

**ANALISIS DAN IMPLEMENTASI SISTEM KEAMANAN DATA
INFORMASI KEUANGAN MENGGUNAKAN ALGORITMA
CAMELLIA PADA SD MUHAMMADIYAH 08 MEDAN**

SKRIPSI

DISUSUN OLEH

ASMA'UL HUSNIAH

2109010105



UMSU
Unggul | Cerdas | Terpercaya

**PROGRAM STUDI SISTEM INFORMASI
FAKULTAS ILMU KOMPUTER DAN TEKNOLOGI INFORMASI
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
MEDAN**

2025

**ANALISIS DAN IMPLEMENTASI SISTEM KEAMANAN DATA
INFORMASI KEUANGAN MENGGUNAKAN ALGORITMA
CAMELLIA PADA SD MUHAMMADIYAH 08 MEDAN**

SKRIPSI

**Diajukan sebagai salah satu syarat untuk memperoleh gelar Sarjana Komputer
(S.Kom) dalam Program Studi Sistem Informasi pada Fakultas Ilmu Komputer
dan Teknologi Informasi, Universitas Muhammadiyah Sumatera Utara**

ASMA'UL HUSNIAH

2109010105

**PROGRAM STUDI SISTEM INFORMASI
FAKULTAS ILMU KOMPUTER DAN TEKNOLOGI INFORMASI
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
MEDAN**

2025

LEMBAR PENGESAHAN

Judul Skripsi : Analisis dan Implementasi Sistem Keamanan Data
Informasi Keuangan Menggunakan Algoritma Camellia
Pada SD Muhammadiyah 08 Medan

Nama Mahasiswa : Asma'ul Husniah

NPM : 2109010105

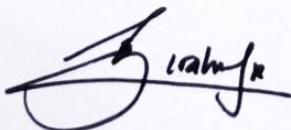
Program Studi : Sistem Informasi

Menyetujui
Komisi Pembimbing



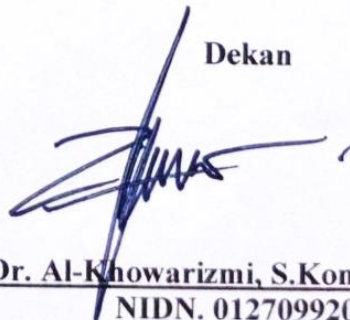
(Ferdy Riza ST, M.Kom)
NIDN. 0103068901

Ketua Program Studi



(Dr. Firahmi Rizky, S.Kom., M.Kom)
NIDN. 0116079201

Dekan



(Dr. Al-Khowarizmi, S.Kom., M.Kom.)
NIDN. 0127099201

PERNYATAAN ORISINALITAS

ANALISIS DAN IMPLEMENTASI SISTEM KEAMANAN DATA INFORMASI KEUANGAN MENGGUNAKAN ALGORITMA CAMELLIA PADA SD MUHAMMADIYAH 08 MEDAN

SKRIPSI

Saya menyatakan bahwa karya tulis ini adalah hasil karya sendiri, kecuali beberapa kutipan dan ringkasan yang masing-masing disebutkan sumbernya.

Medan, 27 Agustus 2025

Yang membuat pernyataan



Asma'ul Husniah

2109010105

**PERNYATAAN PERSETUJUAN PUBLIKASI
KARYA ILMIAH UNTUK KEPENTINGAN
AKADEMIS**

Sebagai sivitas akademika Universitas Muhammadiyah Sumatera Utara, saya bertanda tangan dibawah ini:

Nama	: Asma'ul Husniah
NPM	: 2109010105
Program Studi	: Sistem Informasi
Karya Ilmiah	: Skripsi

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Muhammadiyah Sumatera Utara Hak Bedas Royalti Non-Eksekutif (*Non-Exclusive Royalty free Right*) atas penelitian skripsi saya yang berjudul:

**ANALISIS DAN IMPLEMENTASI SISTEM KEAMANAN DATA
INFORMASI KEUANGAN MENGGUNAKAN ALGORITMA
CAMELLIA PADA SD MUHAMMADIYAH 08 MEDAN**

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Non-Eksekutif ini, Universitas Muhammadiyah Sumatera Utara berhak menyimpan, mengalih media, memformat, mengelola dalam bentuk database, merawat dan mempublikasikan Skripsi saya ini tanpa meminta izin dari saya selama tetap mencantumkan nama saya sebagai penulis dan sebagai pemegang dan atau sebagai pemilik hak cipta.

Demikian pernyataan ini dibuat dengan sebenarnya.

Medan, 27 Agustus 2025

Yang membuat pernyataan



Asma'ul Husniah

NPM. 2109010105

RIWAYAT HIDUP

DATA PRIBADI

Nama Lengkap : Asma'ul Husniah
Tempat dan Tanggal Lahir : Medan, 28 Oktober 2002
Alamat Rumah : Jl. Datuk Kabu, Gang Amal, Pasar 3
Tembung
Telepon/Faks/HP : 081260090974
E-mail : asmaulhusniah28@gmail.com
Instansi Tempat Kerja : -
Alamat Kantor : -

DATA PENDIDIKAN

SD	: SD Muhammadiyah 08 Medan	TAMAT: 2014
SMP	: SMP Negeri 23 Medan	TAMAT: 2017
SMA	: SMK Telkom 2 Medan	TAMAT: 2020

KATA PENGANTAR



Puji syukur penulis panjatkan ke hadirat Allah SWT karena atas rahmat, taufik dan karunianya penulis dapat menyelesaikan skripsi yang berjudul “**Analisis dan Implementasi Sistem Keamanan data Informasi Keuangan Menggunakan Algoritma Camellia Pada SD Muhammadiyah 08 Medan**”. Shalawat serta salam senantiasa tercurah kepada Nabi Muhammad SAW, yang telah membawa kita dari zaman kegelapan menuju zaman yang terang benderang dengan ilmu pengetahuan.

Skripsi ini ditulis dalam rangka memenuhi syarat untuk mencapai gelar Sarjana Komputer pada Program Sistem Informasi Fakultas Ilmu Komputer dan Teknologi Informasi di Universitas Muhammadiyah Sumatera Utara. Penulis menyadari bahwa penyusunan skripsi ini tidak akan terselesaikan tanpa bantuan dan dukungan dari berbagai pihak. Untuk itu penulisan menyampaikan penghargaan dan terima kasih yang tak terhingga kepada:

1. Bapak Prof. Dr. Agussani, M.AP., selaku Rektor Universitas Muhammadiyah Sumatera Utara.
2. Bapak Dr. Al-Khowarizmi, S.Kom., M.Kom., selaku Dekan Fakultas Ilmu Komputer dan Teknologi Informasi (FIKTI) UMSU.
3. Ibu Dr. Firahmi Rizky, S.Kom., M.Kom., selaku Ketua Program Studi Sistem Informasi.
4. Bapak Mahardika Abdi Prawira Tanjung, S.Kom., M.Kom., selaku Sekretaris Program Studi Sistem Informasi.
5. Bapak Ferdy Riza, ST, M.Kom selaku dosen pembimbing yang telah

memberikan arahan dan bimbingan kepada penulis.

6. Kedua orang tua tercinta, yaitu Ibunda Erlinawati dan Ayahanda Jamil, penulis menyampaikan terima kasih yang tak terhingga atas segala kasih sayang yang diberikan dalam membesarkan dan membimbing penulis selama ini. Pengorbanan yang tak kenal lelah, serta memberikan cinta dan doa yang tiada henti dari mereka sangat berarti bagi penulis. Terima kasih juga kepada saudara-saudara penulis yang selalu memberi dukungan serta semangat.
7. Seluruh rekan-rekan seperjuangan selama masa perkuliahan. Terima kasih atas setiap diskusi, kebersamaan, dukungan, semangat, serta kenangan indah yang telah tercipta sepanjang perjalanan perkuliahan ini. Kenangan bersama kalian akan selalu hidup dalam lembaran cerita yang tak tergantikan.
8. Sahabat penulis sejak masa SMK, Mercydita Siburian, terima kasih atas dukungan, motivasi, selalu siap mendengarkan apapun curhatan penulis dan persahabatan yang tetap terjalin hingga saat ini.
9. Ibu Kepala Sekolah, para guru dan staff SD Muhammadiyah yang telah memberikan izin, kesempatan, serta dukungan selama proses pelaksanaan penelitian.
10. Terima kasih yang mendalam kepada diri saya sendiri. Terima kasih telah berjuang sejauh ini, tetap bertahan di saat semangat mulai pudar, tetap percaya ketika ragu dan tidak menyerah walaupun banyak hal terasa sulit. Perjalanan ini tidaklah mudah, namun berkat tekad dan keyakinan, akhirnya semua dapat diselesaikan. Semoga apa yang telah dicapai menjadi langkah

awal menuju masa depan yang lebih baik, serta menjadi pengingat bahwa setiap usaha dan perjuangan diri sendiri adalah hal yang patut dihargai.

Medan, 27 Agustus 2025

Penulis

A handwritten signature in black ink, appearing to be 'Asma'ul Husniah', with a horizontal line underneath.

Asma'ul Husniah

ANALISIS DAN IMPLEMENTASI SISTEM KEAMANAN DATA INFORMASI KEUANGAN MENGGUNAKAN ALGORITMA CAMELLIA PADA SD MUHAMMADIYAH 08 MEDAN

ABSTARK

Keamanan data merupakan salah satu aspek penting dari sebuah informasi dalam sistem pendidikan, terutama pada data keuangan sekolah yang bersifat rahasia dan rentan terjadinya manipulasi data, penyalahgunaan data atau akses tidak sah oleh pihak yang tidak berwenang. Untuk mengatasi permasalahan tersebut, maka diperlukan teknik untuk mengamankan data yang sering disebut dengan kriptografi. Salah satu algoritma kriptografi adalah algoritma kriptografi Camellia. Camellia memiliki putaran kunci untuk proses enkripsi dan dekripsi. Pada penelitian ini dibangun sebuah aplikasi berbasis web memungkinkan pengguna untuk mengunggah data keuangan dalam format excel yang kemudian dienkripsi menggunakan algoritma kriptografi Camellia, data keuangan dapat dienkripsi secara aman sehingga hanya pihak berwenang yang dapat melihat informasi tersebut. Hasil implementasi menunjukkan bahwa sistem mampu mengamankan data keuangan secara efektif dan dapat diakses dengan mudah oleh pengguna. Proses enkripsi berhasil menghasilkan file yang tidak terbaca oleh pihak yang tidak berwenang, sementara proses dekripsi mampu mengembalikan data ke bentuk semula tanpa adanya perubahan isi maupun format. Secara keseluruhan, penerapan algoritma kriptografi Camellia terbukti efektif dalam mengamankan data dan mampu menjaga kerahasiaan sekaligus menjamin integritas data keuangan sekolah.

Kata Kunci: Keamanan Data; Kriptografi Camellia; Enkripsi; Dekripsi.

**ANALYSIS AND IMPLEMENTATION OF A FINANCIAL DATA
SECURITY SYSTEM USING THE CAMELLIA ALGORITHM
AT SD MUHAMMADIYAH 08 MEDAN**

ABSTRACT

Data security is one of the most important aspects of information in the education system, especially financial data, which is confidential and vulnerable to manipulation, misuse, or unauthorized access. To address this problem, a technique called cryptography is required to secure the data. One of the cryptographic algorithms is the Camellia algorithm, which uses key scheduling for the encryption and decryption process. In this research, a web-based application was developed that allows users to upload financial data in Excel format, which is then encrypted using the Camellia algorithm. Financial data can thus be securely encrypted so that only authorized parties are able to access the information. The results of the implementation show that the system is effective in securing financial data and is easily accessible to users. The encryption process successfully produces a file that cannot be read by unauthorized parties, while the decryption process is able to restore the data to its original form without any loss of content or format. Overall, the application of the Camellia cryptographic algorithm has proven to be effective in securing data, maintaining confidentiality, and ensuring the integrity of school financial information.

Keywords: Data Security; Camellia Cryptography; Encryption; Decryption.

DAFTAR ISI

LEMBAR PENGESAHAN	ii
PERNYATAAN ORISINALITAS	iii
PERNYATAAN PERSETUJUAN PUBLIKASI	iv
RIWAYAT HIDUP	v
KATA PENGANTAR.....	vi
ABSTARK	ix
ABSTRACT	x
DAFTAR ISI.....	xi
DAFTAR TABEL	xv
DAFTAR GAMBAR.....	xvi
BAB I PENDAHULUAN.....	1
1.1. Latar Belakang Masalah.....	1
1.2. Rumusan Masalah	4
1.3. Batasan Masalah	4
1.4. Tujuan Penelitian	5
1.5. Manfaat Penelitian	5
BAB II LANDASAN TEORI	6
2.1. Data	6
2.2. Keamanan	6
2.3. Kriptografi.....	7
2.4. Jenis Kriptografi.....	9
2.4.1. Kriptografi Klasik	9
2.4.2. Kriptografi Modern	9
2.5. Algoritma Kriptografi Asimetris.....	10
2.6. Algoritma Kriptografi Simetris	11
2.7. Pengertian Enkripsi	12
2.8. Pengertian Dekripsi.....	12
2.9. Algoritma Kriptografi Camellia.....	12
1. Penjadwalan Kunci (Key Scheduling)	13
2. Proses Enkripsi Algoritma Camellia.....	18
3. Proses Dekripsi Algoritma Camellia.....	22
4. Komponen Penyusunan Algoritma Camellia.....	26
2.10. Sistem Informasi	32
2.11. Website	33

2.12.	HTML	34
2.13.	PHP	34
2.14.	JavaScript.....	35
2.15.	Mysql	36
2.16.	Database	37
2.17.	Pemodelan Beorientasi Objek (UML)	38
1.	<i>Flowchart</i>	38
2.	<i>Use Case Diagrams</i>	41
3.	Diagram Aktivitas (<i>Activity Diagram</i>)	42
4.	Diagram Urutan (<i>Sequence Diagram</i>).....	44
5.	Diagram Kelas (<i>Class Diagram</i>)	46
BAB III	METODOLOGI PENELITIAN	48
3.1.	Tahapan Penelitian	48
3.2.	Metode Pengumpulan Data	50
3.3.	Perancangan Sistem.....	51
3.3.1.	<i>Flowchart</i>	51
1.	<i>Flowchart</i> Alur Program.....	52
2.	<i>Flowchart</i> Proses Pembangkitan Kunci (Generate Key)	53
3.	<i>Flowchart</i> Proses Enkripsi Data	54
4.	<i>Flowchart</i> Proses Dekripsi Data	55
3.3.2.	<i>Use Case Diagram</i>	56
3.3.3.	<i>Class Diagram</i>	57
3.3.4.	<i>Activity Diagram</i>	57
1.	<i>Activity Diagram Login</i>	58
2.	<i>Activity Diagram Menu Dashboard</i>	58
3.	<i>Activity Diagram Menampilkan Daftar File Terenkripsi</i>	59
4.	<i>Activity Diagram Enkripsi Data</i>	60
5.	<i>Activity Diagram Dekripsi Data</i>	61
6.	<i>Activity Diagram Kelola Akun</i>	62
7.	<i>Activity Diagram Logout</i>	63
3.3.5.	<i>Sequence Diagram</i>	63
1.	<i>Sequence Diagram Login</i>	63
2.	<i>Sequence Diagram Menu Dashboard</i>	64
3.	<i>Sequence Diagram Menampilkan Daftar File Terenkripsi</i>	65
4.	<i>Sequence Diagram Enkripsi Data</i>	66
5.	<i>Sequence Diagram Dekripsi Data</i>	66

6.	<i>Sequence</i> Diagram Kelola Akun	67
7.	<i>Sequence</i> Diagram Logout	68
3.4.	Desain <i>Interface</i> Sistem.....	69
3.4.1.	Desain <i>Interface</i> Form <i>Login</i>	69
3.4.2.	Desain <i>Interface</i> Dashboard.....	69
3.4.3.	Desain <i>Interface</i> Data File Terenkripsi.....	70
3.4.4.	Desain <i>Interface</i> Form Upload & Enkripsi	71
3.4.5.	Desain <i>Interface</i> Form Dekripsi.....	71
3.4.6.	Desain <i>Interface</i> Kelola Akun.....	72
BAB IV HASIL DAN UJI COBA.....		73
4.1.	Perhitungan Algoritma Camellia.....	73
1.	Proses Penjadwalan Kunci Algoritma Camellia	73
2.	Proses Enkripsi Algoritma Camellia.....	78
3.	Proses Dekripsi Algoritma Camellia.....	104
4.2.	Hasil.....	132
4.	Tampilan Halaman Form Login.....	133
5.	Tampilan Halaman Dashboard	133
6.	Tampilan Halaman Daftar File Terenkripsi	134
7.	Tampilan Halaman Form Upload dan Enkripsi	135
8.	Tampilan Halaman Form Dekripsi	135
9.	Tampilan Halaman Form Kelola Akun.....	136
4.3.	Pembahasan dan Uji Coba.....	136
4.2.1.	Pembahasan	137
4.2.2.	Uji Coba	138
1.	Uji Coba Form Login Sistem	138
2.	Uji Coba Form Daftar File Terenkripsi.....	139
3.	Uji Coba Form Upload & Enkripsi	139
4.	Uji Coba Form Dekripsi.....	140
5.	Uji Coba Form Kelola Akun	141
6.	Uji Coba Logout Sistem.....	141
4.2.3.	Hasil Pengujian Sistem	142
4.4.	Kelebihan dan Kekurangan Sistem	143
4.3.1.	Kelebihan Sistem	143
4.3.2.	Kekurangan Sistem	144
BAB V KESIMPULAN DAN SARAN		145
5.1.	Kesimpulan	145

5.2. Saran	145
DAFTAR PUSTAKA.....	147
LAMPIRAN.....	152

DAFTAR TABEL

Tabel 2.1. Nilai Konstanta Algoritma Camellia	14
Tabel 2.2. Subkunci untuk kunci rahasia 128 bit.....	15
Tabel 2.3. Subkunci untuk kunci rahasia 192 bit dan 256 bit.....	16
Tabel 2. 4. s-box s1	28
Tabel 2.5. s-box s2	29
Tabel 2.6. s-box s3	29
Tabel 2. 7. s-box s4	29
Tabel 2.8. Simbol Flowchart.....	39
Tabel 2.9. Simbol Use Case Diagram.....	41
Tabel 2.10. Simbol Activity Diagram.....	43
Tabel 2.11. Simbol Sequence Diagram.....	44
Tabel 2.12. Simbol Class Diagram	46
Tabel 4.1. <i>Blackbox Testing</i> Form Login Sistem.....	138
Tabel 4.2. <i>Blackbox Testing</i> Form Daftar File Terenkripsi	139
Tabel 4.3. <i>Blackbox Testing</i> Form Upload & Enkripsi.....	139
Tabel 4.4. <i>Blackbox Testing</i> Form Dekripsi	140
Tabel 4.5. <i>Blackbox Testing</i> Form Kelola Akun.....	141
Tabel 4.6. <i>Blackbox Testing</i> Logout Sistem	141

DAFTAR GAMBAR

Gambar 2.1. Simbol-simbol Algoritma Camellia	13
Gambar 2.2. Pembangkit Kunci Camellia	18
Gambar 2.3. Prosedur Enkripsi Camellia untu panjang kunci 128 bit.....	21
Gambar 2.4. Prosedur Enkripsi Camellia untu panjang kunci 192 bit dan 256 bit	22
Gambar 2.5. Prosedur Dekripsi Camellia untuk panjang kunci 128 bit	25
Gambar 2.6. Prosedur Dekripsi Camellia untuk panjang kunci 192 bit d an 256 bit	26
Gambar 2.7. Fungsi F	27
Gambar 2.8. Fungsi FL	31
Gambar 2.9. Fungsi FL^{-1}	32
Gambar 2.10. Logo PHP	35
Gambar 2.11. Logo MySQL	37
Gambar 3.1. Metodel Waterfall Dalam Perancangan Sistem	48
Gambar 3.2. <i>Flowchart</i> Alur Program	52
Gambar 3.3. Flowchart Proses Generate Key	53
Gambar 3.4. Flowchart Proses Enkripsi Data	54
Gambar 3.5. Flowchart Proses Dekripsi Data.....	55
Gambar 3.6. Use Case Diagram Aplikasi Keamanan Data Keuangan Menggunakan Algoritma Kriptografi Camellia	56
Gambar 3.7. <i>Class</i> Diagram Pada Sistem	57
Gambar 3.8. Activity Diagram Login	58
Gambar 3.9. Activity Diagram Dashboard	59
Gambar 3.10. Activity Diagram Menampilkan Daftar File Terenkripsi.....	60
Gambar 3.11. Activity Diagram Enkripsi Data.....	61
Gambar 3.12. Activity Diagram Dekripsi Data	62
Gambar 3.13. Activity Diagram Kelola Akun	62
Gambar 3.14. Activity Diagram Logout	63
Gambar 3.15. Sequence Diagram Login	64
Gambar 3.16. Sequece Diagram Menampilkan Menu Dashboard.....	65
Gambar 3.17. Sequence Diagram menampililkan daftar data keuangan	65
Gambar 3.18. Sequence Diagram Enkripsi Data	66
Gambar 3.19. Sequence Diagram Dekripsi Data	67
Gambar 3.20. Sequence Diagram Kelola AKun	68
Gambar 3.21. Sequence Diagram Logout.....	68
Gambar 3.22. Desain Interface Form Login	69
Gambar 3.23. Desain Interface Dashboard	70
Gambar 3.24. Desain Interface Data File Terenkripsi	70
Gambar 3.25. Desain Interface Form Upload & Enkripsi	71
Gambar 3.26. Desain Interface Form Dekripsi	72
Gambar 3.27. Desain Interface Profil	72
Gambar 4.1. Tampilan Halaman Form Login.....	133
Gambar 4.2. Tampilan Halaman Dashboard.....	134
Gambar 4.3. Tampilan Halaman Daftar File Terenkripsi	134
Gambar 4.4. Tampilan Halaman Form Upload dan Enkripsi	135
Gambar 4.5. Tampilan Halaman Form Dekripsi	136

Gambar 4.6. Tampilan Halaman Form Kelola Akun.....	136
Gambar 4.7. Contoh Hasil Enkripsi File.....	142

BAB I

PENDAHULUAN

1.1. Latar Belakang Masalah

SD Muhammadiyah 08 Medan adalah salah satu institusi pendidikan dasar yang berbasis islam yang berada di bawah naungan Kementrian Pendidikan dan Kebudayaan. Sekolah ini memiliki visi dan misi untuk membentuk pribadi muslim yang unggul, berakhlak karimah, dan berbudaya melalui pembelajaran efektif, pengembangan ilmu agama dan pembelajaran berbasis IT. Sebagai institusi pendidikan, SD Muhammadiyah 08 Medan telah mengadopsi sistem informasi digital yang digunakan untuk mengelola data-data penting sekolah. Salah satu data yang sangat penting adalah data keuangan, yang memiliki berbagai macam transaksi, seperti penggajian untuk guru, pembayaran uang bulanan bagi siswa, serta pengeluaran dan pemasukan lainnya.

Seiring dengan perkembangan teknologi, muncul permasalahan terkait keamanan data informasi. Pesatnya perkembangan ilmu pengetahuan dan teknologi telah melahirkan teknik-teknik baru, yang dapat disalahgunakan oleh pihak-pihak tertentu yang mengancam keamanan dari sistem informasi tersebut (Hasibuan et al., 2022). Data keuangan menjadi salah satu data yang perlu diamankan, karena sifatnya yang sensitif, sehingga banyak kejahatan yang terjadi. Pencurian data, pelanggaran privasi, dan penyalahgunaan data semakin menjadi risiko nyata yang dapat berdampak serius pada individu, organisasi, dan masyarakat secara keseluruhan (Cristy & Riandari, 2021).

Data keuangan sangat penting bagi sekolah, dikarenakan jika ada kecurangan akan mengalami kerugian yang sangat fatal. Keuangan sekolah perlu dikelola dengan baik. Hal ini penting karena keuangan memberikan gambaran menyeluruh mengenai perencanaan anggaran, pelaksanaan kas, dan pelaporan dalam bentuk akuntansi (Tarigan et al., 2021). Namun, saat ini sekolah masih menggunakan metode penyimpanan secara konvensional atau sistem digital tanpa perlindungan keamanan yang memadai, sehingga mengakibatkan rentan terjadinya kebocoran data, manipulasi, atau penyalahgunaan data atau akses tidak sah oleh pihak yang tidak berwenang. Untuk menjaga keamanan data ini diperlukan sistem yang mampu untuk mengamankan data keuangan, maka penulis berinisiatif untuk memberikan sebuah sistem keamanan data dan sekaligus tempat backup data tersebut.

Salah satu solusi yang ditawarkan adalah menerapkan teknik algoritma kriptografi. Kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan data melalui teknik-teknik pengkodean, sehingga informasi tidak dapat diakses oleh pihak yang tidak berwenang. Dengan cara ini, hanya pengguna yang berhak yang bisa mengakses dan mengelola data dalam bentuk yang dapat dipahami, sehingga keamanan dan integritas data tetap terjaga (Ferdy Riza et al., 2024). Salah satu algoritma kriptografi yang cocok digunakan untuk tujuan ini adalah Algoritma Camellia.

Algoritma Camellia adalah algoritma kriptografi simetris berbasis blok (block cipher) yang menggunakan kunci yang sama untuk proses enkripsi dan dekripsi. Dalam Camellia proses enkripsi dan dekripsi dilakukan pada blok data berukuran 128 bit dengan kunci yang dapat berukuran 128 bit, 192 bit, dan 256 bit. Camellia menggunakan struktur Feistel Cipher yang telah dimodifikasi, di mana

proses enkripsi untuk kunci 128 bit dilakukan sebanyak 18 kali putaran dan untuk panjang kunci 192 bit atau 256 bit dilakukan sebanyak 24 kali putaran. Algoritma Camellia bekerja dengan membagi data menjadi blok berukuran 128 bit, lalu melakukan proses enkripsi melalui beberapa tahapan yang melibatkan operasi XOR, S-Box, rotasi bit, dan transformasi linear, serta dengan fungsi FL dan FL⁻¹ yang meningkatkan kekuatan keamanan (Malau, 2019).

Algoritma Camellia dikenal sangat kuat dalam hal mengenkripsi dan mendekripsi data. Kriptografi Camellia memiliki tingkat keamanan yang tinggi dan efisien dalam performa enkripsi atau dekripsi, sehingga tidak akan memperlambat sistem. Camellia memiliki tingkat keamanan dan performa setara dengan Advanced Encryption Standard (AES), dan telah dipilih sebagai standar internasional oleh ISO/IEC, IETF, dan proyek NESSIE serta CRYPTREC. Camellia juga memiliki struktur algoritma yang fleksibel dan aman, menjadikannya cocok dalam berbagai lingkungan sistem informasi, termasuk pada sistem berbasis web seperti yang akan dibangun pada penelitian ini. Struktur algoritmanya yang kompleks karena melibatkan berbagai transformasi kriptografi dan putaran enkripsi, menciptakan hambatan signifikan bagi pembobolan data oleh pihak yang tidak berwenang. Implementasi Camellia dapat melakukan enkripsi dengan kecepatan jauh lebih tinggi dibandingkan implementasi DES yang dioptimalkan (Aoki et al., 2000).

Berdasarkan solusi yang telah dijelaskan, penulis akan membangun sistem keamanan data informasi keuangan dengan menggunakan algoritma kriptografi Camellia. Metode ini dipilih karena memiliki tingkat keamanan yang tinggi dan kerumitan algoritma yang menyulitkan proses pemecahan kunci oleh pihak yang tidak berwenang. Dengan penerapan algoritma Camellia pada sistem keamanan

data di SD Muhammadiyah 08 Medan diharapkan dapat melindungi data dari akses yang tidak sah. Dengan menggunakan algoritma Camellia, data yang disimpan akan terenkripsi dengan baik, sehingga mengurangi risiko kebocoran data, manipulasi, atau penyalahgunaan data.

1.2. Rumusan Masalah

Berdasarkan latar belakang yang telah dijelaskan, rumusan masalah dalam penelitian ini dapat dirumuskan sebagai berikut:

1. Bagaimana membangun sistem keamanan data keuangan berbasis web yang dapat menjaga keamanan isi data keuangan sekolah?
2. Bagaimana implementasi kriptografi Camellia dalam mengamankan data keuangan yang tersimpan dalam format excel?
3. Bagaimana proses enkripsi dan dekripsi menggunakan algoritma Camellia?

1.3. Batasan Masalah

Penulis membatasi ruang masalah yang akan diteliti. Batasan-batasan masalah yang dipergunakan yaitu:

1. Teknik kriptografi yang akan digunakan dalam proses enkripsi dan dekripsi adalah Algoritma Camellia.
2. Penelitian ini berfokus pada pengamanan data keuangan sekolah dengan format file excel.
3. Penelitian ini berfokus pada merancang program berbasis web yang dibangun menggunakan bahasa program PHP dan menggunakan database MySQL.

1.4. Tujuan Penelitian

Adapun tujuan penelitian adalah sebagai berikut:

1. Mengimplementasikan algoritma Camellia untuk sistem keamanan data.
2. Membangun sistem keamanan data keuangan berbasis web yang dapat menjadi wadah penyimpanan data keuangan sekolah secara aman dari upaya manipulasi data.
3. Mengetahui dan memahami proses enkripsi dan dekripsi menggunakan algoritma Camellia.
4. Untuk merancang sebuah sistem keamanan dalam mengamankan data dengan menggunakan algoritma Camellia.

1.5. Manfaat Penelitian

Adapun beberapa manfaat dari penelitian ini, diantaranya:

1. Dengan adanya sistem keamanan data, informasi penting dapat diamankan dengan lebih baik dan efisien sehingga dapat mencegah kebocoran data, manipulasi data serta akses oleh pihak yang tidak berwenang.
2. Penelitian ini diharapkan dapat memberikan kontribusi terhadap pengembangan ilmu pengetahuan tentang kriptografi. Hasil penelitian dapat memperkaya literatur akademik tentang penerapan algoritma kriptografi dalam perancangan keamanan data informasi keuangan.
3. Penelitian ini memberikan kesempatan bagi penulis untuk menambah pengetahuan tentang keamanan data dan kriptografi serta dapat memberikan kontribusi pada pengetahuan dalam bidang tersebut.

BAB II

LANDASAN TEORI

2.1. Data

Data merupakan sekumpulan fakta, angka atau informasi yang dapat digunakan untuk analisis, pengambilan keputusan, atau penelitian. Data dapat diperoleh dalam bentuk simbol, karakter huruf, angka, gambar, suara, atau sinyal. Data adalah suatu bahan mentah yang jika diolah dengan baik melalui berbagai analisis akan dapat menghasilkan berbagai informasi (Syahrani, 2020). Dalam era digital ini, data menjadi salah satu aset terpenting bagi organisasi dan individu.

Secara umum, data dapat diklasifikasikan menjadi beberapa jenis, yaitu data terstruktur, data tidak terstruktur, dan data semi-terstruktur. Data terstruktur adalah data yang disimpan dalam format yang telah ditentukan seperti tabel, database dan lain sebagainya. Disisi lain, data tidak terstruktur adalah data yang tidak memiliki format yang jelas, seperti teks, gambar, video atau audio. Sementara itu, data semi-terstruktur merupakan data yang memiliki elemen struktural tetapi tidak sepenuhnya terorganisir dalam database, seperti XML atau JSON.

2.2. Keamanan

Keamanan adalah kondisi yang menunjukkan keadaan bebas dari bahaya maupun ancaman. Keamanan merupakan topik yang luas termasuk keamanan nasional terhadap seorang teroris, keamanan komputer terhadap hacker, keamanan rumah terhadap pencurian, hingga keamanan finansial dari risiko kehancuran ekonomi. Komputer yang terhubung ke jaringan (*network*) memiliki ancaman keamanan yang lebih tinggi dibandingkan dengan komputer yang tidak

terhubung kemana-mana. Oleh karena itu, untuk mengurangi risiko tersebut, diperlukan upaya pengendalian terhadap aspek keamanan jaringan (*network security*). Salah satu aspek penting dalam sistem keamanan informasi adalah keamanan data. Keamanan data adalah upaya untuk melindungi data dari akses, modifikasi, atau penghapusan dari akses yang tidak sah, serta memastikan bahwa data tetap tersedia bagi pengguna yang berwenang (Husaini et al., 2022).

Menurut Galih (2020), ada tiga elemen keamanan informasi yaitu kerahasiaan, integritas, dan ketersediaan.

1. Kerahasiaan (*Confidentiality*) merupakan prinsip yang memastikan perlindungan data dan sumber informasi. Hal ini bertujuan untuk memastikan bahwa informasi hanya dapat diakses oleh pihak yang memiliki kewenangan, sehingga keamanan dan kerahasiaan data tersebut tetap terjaga.
2. Integritas (*Integrity*) adalah faktor yang memastikan bahwa data tidak dapat diubah tanpa izin dari pihak yang berwenang, menjaga keakuratannya dan integritas data serta metode pemrosesan yang digunakan untuk memastikan integritas data.
3. Ketersediaan (*Availability*) adalah aspek yang menjamin bahwa data dapat diakses pada saat dibutuhkan dan tepat waktu oleh pihak yang berwenang, serta memastikan penggunaan yang berhak dapat mengakses informasi.

2.3. Kriptografi

Kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti maknanya. Saat

ini, kriptografi lebih dari sekadar menjaga privasi, tetapi juga bertujuan untuk memastikan integritas data, otentikasi entitas, dan non-repudiation (Porman Malau, 2019). Namun seiring perkembangannya definisi terbaru menyatakan bahwa kriptografi adalah ilmu yang mempelajari teknik matematika yang berhubungan dengan keamanan informasi seperti kerahasiaan, keutuhan data dan otentikasi. Jadi pengertian kriptografi modern tidak hanya terbatas dengan menyembunyian pesan, tetapi lebih pada sekumpulan teknik yang bertujuan untuk menjaga keamanan informasi secara menyeluruh (Saragi et al., 2020).

Untuk melaksanakan proses kriptografi, terdapat beberapa elemen utama yang saling berkaitan, yaitu:

1. Plaintext: merupakan pesan awal atau teks asli yang dikirim dalam komunikasi. Teks ini akan melalui proses enkripsi dan dekripsi.
2. Ciphertext: pesan tersembunyi hasil dari proses enkripsi terhadap pesan asli (plaintext). Ciphertext dapat dikembalikan menjadi bentuk aslinya (plaintext) menggunakan kunci (key) yang telah ditentukan.
3. Kunci Kriptografi (*Cryptography Key*): kunci yang digunakan dalam proses enkripsi dan dekripsi. Tanpa kunci yang sesuai, proses enkripsi dan dekripsi tidak dapat dilakukan dengan baik. Kunci ini berperan sebagai pengendali dalam pelaksanaan kriptografi.
4. Algoritma Enkripsi-Dekripsi (*Encryption Decryption Algorithm*): algoritma yang digunakan untuk melakukan enkripsi dan dekripsi, sebagai elemen terakhir yang tak kalah penting dalam prorses kriptografi (Fauzan et al., 2023).

2.4. Jenis Kriptografi

Algoritma kriptografi dapat diklasifikasikan menjadi dua jenis berdasarkan perkembangannya, yaitu:

2.4.1. Kriptografi Klasik

Kriptografi digunakan sebelum era komputerisasi dan umumnya menggunakan teknik kunci simetris. Metode penyembunyian pesan dalam kriptografi klasik dilakukan melalui teknik substitusi atau transposisi, atau dapat menggabungkan keduanya secara bersamaan. Teknik substitusi adalah metode dengan cara mengganti setiap karakter dalam plaintext menjadi karakter lain sehingga menghasilkan ciphertext. Sedangkan teknik transposisi mengubah plaintext menjadi ciphertext dengan cara melakukan permutasi terhadap urutan karakter dalam pesan (Sasono et al., 2023).

Kriptografi klasik masih banyak menggunakan pena dan kertas, terutama dalam pengiriman pesan. Dalam proses penyandian, metode ini berbasis pada pergantian karakter, di mana setiap huruf dalam pesan asli digantikan dengan huruf lain untuk mengelabui pembaca yang tidak berhak. Namun, metode ini tidak disarankan untuk mengamankan informasi penting karena mudah dipecahkan dalam waktu singkat (Murdowo, 2020). Contoh algoritma kriptografi klasik antara lain Caesar Cipher, Vigenere Cipher, dan Hill Cipher.

2.4.2. Kriptografi Modern

Kriptografi Modern memiliki tingkat kesulitan yang lebih kompleks, dengan kekuatan keamanannya yang terletak pada penggunaan kunci. Umumnya, kriptografi modern bekerja dalam mode bit, sehingga semua data dan informasi (baik kunci, plaintext, maupun ciphertext) dalam operasi mode bit

dinyatakan dalam rangkaian string ataupun bit biner, 0 dan 1 (Aryanto et al., 2023).

Kriptografi Modern merupakan penyempurnaan dari teknik-teknik yang digunakan pada kriptografi klasik. Algoritma dalam kriptografi modern menggunakan pengolahan data dalam bentuk simbol biner yang dibentuk dari kode ASCII (*American Standard Code for Information Interchange*), karena seluruh proses berjalan mengikuti operasi komputer digital. Oleh karena itu, pemahaman dasar matematika sangat dibutuhkan untuk menguasai teknik-teknik ini. Algoritma kriptografi modern memiliki tingkat kompleksitas yang tinggi, sehingga pihak yang mencoba memecahkan ciphertext akan sangat kesulitan apabila tidak mengetahui kunci yang digunakan. Jenis kunci dalam kriptografi modern dibagi menjadi tiga, yaitu kunci simetris, kunci asimetris, dan kunci hibrida (Sasono et al., 2023)

2.5. Algoritma Kriptografi Asimetris

Algoritma kriptografi asimetris adalah salah satu jenis kriptografi yang menggunakan dua kunci berbeda namun saling terkait untuk mengamankan informasi, yaitu kunci publik (*public key*) dan kunci privat (*private key*). Kunci publik digunakan untuk mengenkripsi data dan dapat dibagikan kepada pihak lain, sementara kunci privat digunakan untuk mendekripsikan data dan harus dijaga kerahasiannya. Prinsip dasarnya adalah bahwa pesan yang dienkripsi dengan kunci publik hanya dapat didekripsi dengan kunci privat yang sesuai, dan sebaliknya (Ferdy Riza et al., 2024).

Kedua kunci tersebut saling berhubungan satu sama lain. Dengan kunci publik siapa pun dapat mengenkripsi data, tetapi tidak dapat mendekripsinya.

Hanya pemegang kunci privat yang dapat mendekripsi data tersebut. Karena kunci privat bersifat rahasia dan hanya dimiliki oleh satu pihak, sehingga perlindungannya harus ketat. Oleh karena itu, kunci enkripsi tidak boleh sama dengan kunci dekripsi. Jika kunci privat jatuh ke tangan yang tidak berwenang, data yang terenkripsi bisa dibuka dengan mudah, yang berpotensi menyebabkan pelanggaran keamanan yang serius (Putra et al., 2023).

2.6. Algoritma Kriptografi Simetris

Algoritma kriptografi simetris adalah metode enkripsi yang menggunakan satu kunci yang sama untuk proses enkripsi dan dekripsi pesan. Agar penerima dapat membaca pesan yang dikirim, pengirim harus memberitahukan kunci tersebut kepada penerima secara rahasia. Keamanan pesan sangat bergantung pada kerahasiaan kunci, jika kunci diketahui oleh pihak yang tidak berwenang, maka pihak tersebut dapat membaca bahkan memalsukan pesan dengan melakukan enkripsi maupun dekripsi. Oleh karena itu, pengirim dan penerima harus sepakat menggunakan kunci yang sama dan menjaga kerahasiannya agar tidak diketahui oleh pihak tidak berwenang. Karena penggunaan kunci yang sama dan sifat yang rahasia, algoritma ini juga dikenal sebagai algoritma kunci privat atau kunci rahasia (Alfirdaus et al., 2023).

Algoritma kriptografi simetris dapat dikelompokkan menjadi dua kategori, pertama Cipher aliran (Stream Cipher), algoritma kriptografi beroperasi pada plaintext atau ciphertext dalam bentuk bit tunggal yang dalam hal ini rangkaian bit dienkripsi data didekripsikan bit per bit. Cipher aliran mengenkripsi satu bit setiap kali. Kedua Cipher blok (Block Cipher), algoritma kriptografi beroperasi pada plaintext atau ciphertext dalam bentuk blok bit, yang dalam hal ini rangkaian bit

dibagi menjadi blok-blok bit yang panjangnya sudah ditentukan sebelumnya. Cipher blok mengenkripsi satu blok bit setiap kali (Febrianto & Waluyo, 2023).

2.7. Pengertian Enkripsi

Enkripsi adalah proses konversi data asli (plaintext) menjadi format yang tidak dapat dibaca (ciphertext) tanpa kunci deskripsi yang sesuai. Enkripsi adalah teknik yang digunakan untuk mengamankan informasi dengan cara mengubahnya menjadi bentuk yang tidak dapat dibaca atau dimengerti oleh pihak yang tidak berwenang. Dengan enkripsi, meskipun informasi tersebut jatuh ke tangan yang salah, informasi tersebut tidak akan bisa dipahami tanpa kunci yang benar untuk mendekripsi atau mengembalikan ke bentuk aslinya (Pratama et al., 2025).

2.8. Pengertian Dekripsi

Dekripsi merupakan suatu kegiatan yang bertujuan untuk mengembalikan suatu pesan yang telah dikodekan atau dienkripsi ke dalam pesan aslinya atau plaintext. Proses pemulihan isi pesan terenkripsi menggunakan kode tertentu. Deskripsi adalah kebalikan dari enkripsi. Ini adalah proses mengubah pesan asli menjadi pesan terenkripsi atau ciphertext (Pratama et al., 2025).

2.9. Algoritma Kriptografi Camellia

Algoritma Camellia merupakan salah satu algoritma kriptografi modern yang termasuk kedalam kunci simetris dan juga blockcipher dengan jumlah blok 128 bit. Algoritma ini dikembangkan oleh NTT (*Nippon Telegraph and Telephone Corporation*) yang bekerja sama dengan Mitsubishi Corporation pada tahun 2000. Algoritma Camellia ini merupakan salah satu perkembangan dari metode AES (*Advanced Encryption Standard*) (Ani & Nasution, 2020).

Camellia dirancang untuk menyediakan tingkat keamanan yang tinggi serta efisiensi dalam implementasi perangkat keras maupun perangkat lunak. Algoritma Camellia telah terstandarisasi di *International Organization for Standardisation* (ISO) dan *the International Electrotechnics Commission* (IEC), serta telah diakui oleh *Cryptography Research and Evaluation Committee* (CRYPTREC) dan *New European Schemes for Signatures, Integrity, and Encryption* (NESSIE) (Romandhon et al., 2024).

Algoritma Camellia bekerja pada blok data berukuran 128 bit dan mendukung panjang kunci 128 bit, 192 bit, dan 256 bit. Algoritma ini menggunakan struktur Feistel Cipher yang telah dimodifikasi dan terdiri dari beberapa tahap putaran (rounds). Untuk kunci sepanjang 128 bit, proses enkripsi dilakukan sebanyak 18 putaran, sedangkan untuk kunci sepanjang 192 bit atau 256 bit dilakukan sebanyak 24 putaran. Dengan tambahan input output whitening dan fungsi-fungsi logis yang disebut fungsi FL dan FL^{-1} . Fungsi FL dimasukkan disetiap 6 putaran yaitu sebelum dan lanjut putaran ketujuh dan ketigabelas (Ani & Nasution, 2020)

Berikut adalah simbol-simbol yang digunakan dalam proses enkripsi dan dekripsi algoritma Camellia:

$\oplus$	The bitwise exclusive-OR operation.
$\parallel$	The concatenation of the two operands.
$\lll_n$	The left circular rotation of the operand by n bits.
$\cap$	The bitwise AND operation.
$\cup$	The bitwise OR operation.
$\bar{x}$	The bitwise complement of x .

Gambar 2.1. Simbol-simbol Algoritma Camellia
(Sumber: Ani & Nasution, 2020)

1. Penjadwalan Kunci (Key Scheduling)

Penjadwalan kunci merupakan proses awal yang digunakan untuk menghasilkan sub-kunci dari kunci utama. Sub-kunci ini akan digunakan dalam

setiap tahap enkripsi, baik dalam proses whitening, putaran enkripsi, maupun fungsi logis tambahan (FL dan FL^{-1}). Adapun langkah-langkah penjadwalan kunci Algoritma Camellia adalah sebagai berikut:

- a. Kunci utama dibagi menjadi dua bagian, yaitu K_L dan K_R . Masing-masing variabel berukuran 128 bit. Khusus untuk panjang kunci 128 bit, K_R diisi dengan angka 0 karena panjang kunci hanya 128 bit. Untuk panjang kunci 192 bit, K_R sepanjang 64 bit yang kemudian dipadukan dengan padding (pengisian) sepanjang 64 bit. Padding ini diisi dengan invers biner dari K_R , sehingga membentuk total K_R sebesar 128 bit.
- b. Variabel K_L dan K_R di XOR-kan, kemudian dienkripsikan dengan nilai konstanta $\sum_1$ dan $\sum_2$. Hasilnya di XOR-kan dengan K_L kemudian di enkripsi dua tahap lagi menggunakan nilai konstanta $\sum_3$ dan $\sum_4$. Hasil dari enkripsi ini adalah K_A . Kemudian K_A di XOR dengan K_R dan di enkripsi dengan nilai konstanta $\sum_5$ dan $\sum_6$. Hasil dari enkripsi ini adalah K_B . $\sum_i$ didefinisikan sebagai representasi nilai kontinyu dari tempat ke-2 heksadesimal dan tempat ke-17 heksadesimal dari akar kuadrat bilangan prima ke- i . Nilai-nilai konstanta tersebut dapat dilihat pada tabel berikut:

Tabel 2.1. Nilai Konstanta Algoritma Camellia

$\sum_1$	0xA09E6673FBCC908B
$\sum_2$	0xB67AE8584CAA73B2
$\sum_3$	0xC6EF372FE94F82BE
$\sum_4$	0x54FF53A5F1D36F1C
$\sum_5$	0x10E527FADE682D1D
$\sum_6$	0xB05688C2B3E6C1FD

(Sumber: Malau, 2019)

- c. Setelah itu pembangkitan subkunci K_w , k , dan K_l , dibangkitkan dari nilai hasil rotasi penggeseran (bitwise rotation) K_L , K_R , K_A , dan K_B . $\lll n$ merupakan

operasi penggeseran sebanyak n bit. Untuk panjang kunci 128 bit melakukan 18 putaran dan untuk 192 bit atau 256 bit melakukan 24 putaran. Untuk lebih detail dapat dilihat pada gambar berikut:

Tabel 2.2. Subkunci untuk kunci rahasia 128 bit

	Subkunci	Nilai
Preshitening	$Kw_{1(64)}$	$(KL \lll 0)_{L(64)}$
	$Kw_{2(64)}$	$(KL \lll 0)_{R(64)}$
F (Tahap 1)	$k_{1(64)}$	$(KA \lll 0)_{L(64)}$
F (Tahap 2)	$k_{2(64)}$	$(KA \lll 0)_{R(64)}$
F (Tahap 3)	$k_{3(64)}$	$(KL \lll 15)_{L(64)}$
F (Tahap 4)	$k_{4(64)}$	$(KL \lll 15)_{R(64)}$
F (Tahap 5)	$k_{5(64)}$	$(KA \lll 15)_{L(64)}$
F (Tahap 6)	$k_{6(64)}$	$(KA \lll 15)_{R(64)}$
FL	$kl_{1(64)}$	$(KA \lll 30)_{L(64)}$
FL^{-1}	$kl_{2(64)}$	$(KA \lll 30)_{R(64)}$
F (Tahap 7)	$k_{7(64)}$	$(KL \lll 45)_{L(64)}$
F (Tahap 8)	$k_{8(64)}$	$(KL \lll 45)_{R(64)}$
F (Tahap 9)	$k_{9(64)}$	$(KA \lll 45)_{L(64)}$
F (Tahap 10)	$k_{10(64)}$	$(KL \lll 60)_{R(64)}$
F (Tahap 11)	$k_{11(64)}$	$(KA \lll 60)_{L(64)}$
F (Tahap 12)	$k_{12(64)}$	$(KA \lll 60)_{R(64)}$
FL	$kl_{3(64)}$	$(KL \lll 77)_{L(64)}$
FL^{-1}	$kl_{4(64)}$	$(KL \lll 77)_{R(64)}$
F (Tahap 13)	$K_{13(64)}$	$(KL \lll 94)_{L(64)}$

F (Tahap 14)	$K_{14(64)}$	$(KL<<<94)_{R(64)}$
F (Tahap 15)	$K_{15(64)}$	$(KA<<<94)_{L(64)}$
F (Tahap 16)	$k_{16(64)}$	$(KA<<<94)_{R(64)}$
F (Tahap 17)	$k_{17(64)}$	$(KL<<<111)_{L(64)}$
F (Tahap 18)	$k_{18(64)}$	$(KL<<<111)_{R(64)}$
Postwhitening	$Kw_{3(64)}$	$(KA<<<111)_{L(64)}$
	$Kw_{4(64)}$	$(KA<<<111)_{R(64)}$

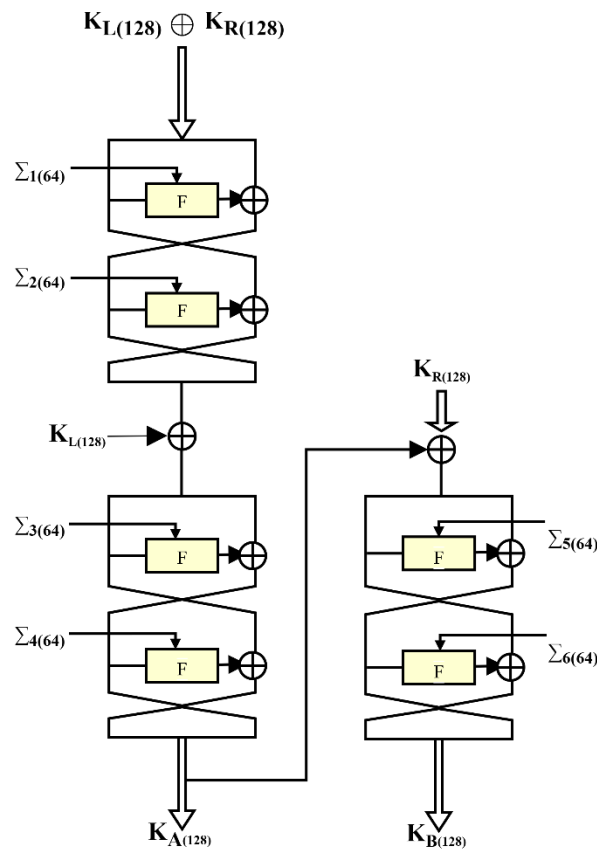
(Sumber: Aoki et al., 2000)

Tabel 2.3. Subkunci untuk kunci rahasia 192 bit dan 256 bit

	Subkunci	Nilai
Prewhitening	$Kw_{1(64)}$	$(KL<<<0)_{L(64)}$
	$Kw_{2(64)}$	$(KL<<<0)_{R(64)}$
F (Tahap 1)	$k_{1(64)}$	$(KB<<<0)_{L(64)}$
F (Tahap 2)	$k_{2(64)}$	$(KB<<<0)_{R(64)}$
F (Tahap 3)	$k_{3(64)}$	$(KR<<<15)_{L(64)}$
F (Tahap 4)	$k_{4(64)}$	$(KR<<<15)_{R(64)}$
F (Tahap 5)	$k_{5(64)}$	$(KA<<<15)_{L(64)}$
F (Tahap 6)	$k_{6(64)}$	$(KA<<<15)_{R(64)}$
FL	$kl_{1(64)}$	$(KR<<<30)_{L(64)}$
FL^{-1}	$kl_{2(64)}$	$(KR<<<30)_{R(64)}$
F (Tahap 7)	$k_{7(64)}$	$(KB<<<30)_{L(64)}$
F (Tahap 8)	$k_{8(64)}$	$(KB<<<30)_{R(64)}$
F (Tahap 9)	$k_{9(64)}$	$(KL<<<45)_{L(64)}$
F (Tahap 10)	$k_{10(64)}$	$(KL<<<45)_{R(64)}$

F (Tahap 11)	$k_{11(64)}$	$(KA<<<45)_{L(64)}$
F (Tahap 12)	$k_{12(64)}$	$(KA<<<45)_{R(64)}$
FL	$kl_{3(64)}$	$(KL<<<60)_{L(64)}$
FL^{-1}	$kl_{4(64)}$	$(KL<<<60)_{R(64)}$
F (Tahap 13)	$k_{13(64)}$	$(KR<<<60)_{L(64)}$
F (Tahap 14)	$k_{14(64)}$	$(KR<<<60)_{R(64)}$
F (Tahap 15)	$k_{15(64)}$	$(KB<<<60)_{L(64)}$
F (Tahap 16)	$k_{16(64)}$	$(KB<<<60)_{R(64)}$
F (Tahap 17)	$k_{17(64)}$	$(KL<<<77)_{L(64)}$
F (Tahap 18)	$k_{18(64)}$	$(KL<<<77)_{R(64)}$
FL	$kl_{5(64)}$	$(KA<<<77)_{L(64)}$
FL^{-1}	$Kl_{6(64)}$	$(KA<<<77)_{R(64)}$
F (Tahap 19)	$k_{19(64)}$	$(KR<<<94)_{L(64)}$
F (Tahap 20)	$k_{20(64)}$	$(KR<<<94)_{R(64)}$
F (Tahap 21)	$k_{21(64)}$	$(KA<<<94)_{L(64)}$
F (Tahap 22)	$k_{22(64)}$	$(KA<<<94)_{R(64)}$
F (Tahap 23)	$k_{23(64)}$	$(KL<<<111)_{L(64)}$
F (Tahap 24)	$k_{24(64)}$	$(KL<<<111)_{R(64)}$
Postwhitening	$Kw_{3(64)}$	$(KB<<<111)_{L(64)}$
	$Kw_{4(64)}$	$(KB<<<111)_{R(64)}$

(Sumber: Aoki et al., 2000)



Gambar 2.2. Pembangkit Kunci Camellia
(Sumber: Aoki et al., 2000)

2. Proses Enkripsi Algoritma Camellia

Proses enkripsi merupakan proses mengubah pesan asli (plaintext) menjadi pesan rahasia (chipertext). Pada algoritma Camellia, proses ini bergantung pada panjang kunci yang digunakan. Proses enkripsi menggunakan kunci 128 bit akan berbeda dengan enkripsi menggunakan kunci 192 bit atau 256 bit.

a. Enkripsi Menggunakan Kunci 128 Bit

Pada enkripsi dengan kunci 128 bit, Camellia menggunakan struktur Feistel Cipher yang terdiri atas 18 putaran dengan 2 lapisan fungsi FL/FL⁻¹ setelah putaran ke-6 dan ke-12. Pertama-tama, blok pertama plaintext $M_{(128)}$ dibagi menjadi dua bagian, kemudian masing-masing di-XOR dengan sub kunci whitening K_{w1} dan K_{w2} , sehingga menghasilkan L_0 dan R_0 .

$$L_0 = M_L \oplus K_{W1} \dots\dots\dots (2.1)$$

$$R_0 = M_R \oplus K_{W2} \dots\dots\dots (2.2)$$

Keterangan:

L_0 dan R_0 : Nilai wal yang akan masuk ke dalam putaran feistel.

M_L : Bagian kanan plaintext 64 bit.

M_R : Bagian kiri plaintext 64 bit.

K_{W1} dan K_{W2} : Subkunci whitening pertama dan kedua.

Operasi $\oplus$ adalah XOR, digunakan untuk menggabungkan data awal dengan kunci sebelum diproses lebih lanjut.

Pada putaran pertama, L_0 dimasukkan ke dalam fungsi F bersama sub kunci k_1 . Hasil dari fungsi tersebut kemudian di-XOR dengan R_0 . Selanjutnya, L_0 menjadi R_1 , dan hasil XOR tadi menjadi L_1 . Pada putaran kedua, L_1 ini kemudian masuk ke dalam fungsi F lagi beserta sub kunci k_2 . Hasilnya kemudian di-XOR dengan R_1 dan L_1 menjadi R_2 . Demikian seterusnya hingga putaran ke-18, kecuali pada putaran ke-6 dan ke-12.

Sebelum putaran ketujuh, L_6 akan memasuki fungsi FL bersama sub kunci kl_1 , dan R_6 akan memasuki fungsi FL^{-1} bersama kl_2 . Setelah itu, hasil masing-masing akan dienkripsi dengan cara seperti tadi selama 6 putaran berikutnya. Kemudian, sebelum putaran ketigabelas, proses FL dan FL^{-1} kembali dilakukan, kali ini dengan sub kunci kl_3 dan kl_4 . Kemudian dienkripsi dengan fungsi F lagi sebanyak 6 putaran, Sehingga total putaran adalah 18.

Jika dirumuskan secara matematis, proses enkripsi Camellia dengan kunci 128 bit adalah sebagai berikut:

$$L_i = R_{i-1} \oplus F(L_{i-1}, k_i) \dots\dots\dots (2.3)$$

$$R_i = L_{i-1} \dots\dots\dots (2.4)$$

Keterangan:

L_i : Perhitungan blok kiri untuk putaran i dalam struktur Feistel

R_i : Perhitungan blok kanan untuk putaran i .

R_{i-1} : Blok kanan dari putaran sebelumnya.

$F(L_{i-1}, k_i)$: Fungsi yang digunakan dalam setiap putaran untuk menghasilkan nilai kompleks dari input dan kunci. Hasil fungsi F dengan input blok kiri putaran sebelumnya (L_{i-1}) dan subkunci putaran ke- i (k_i).

Hasil dari fungsi F kemudian di-XOR dengan R_{i-1} .

Operasi tersebut dilakukan untuk $i=1$ sampai $i=18$, kecuali untuk $i=6$ dan $i=12$, dilakukan operasi sebagai berikut:

$$L'_i = R_{i-1} \oplus F(L_{i-1}, k_i) \dots\dots\dots (2.5)$$

$$R'_i = L_{i-1} \dots\dots\dots (2.6)$$

$$L_i = FL(L'_i, kl_{2i/6-1}) \dots\dots\dots (2.7)$$

$$R_i = FL^{-1}(R'_i, kl_{2i/6}) \dots\dots\dots (2.8)$$

Setelah putaran ke-18 selesai. Terakhir L_{18} akan di-XOR dengan kw_4 dan R_{18} akan di-XOR dengan kw_3 . Kemudian hasilnya digabungkan untuk membentuk ciphertext akhir:

$$C_{(128)} = (R_{18(64)} \parallel L_{18(64)}) \oplus (kw_{3(64)} \parallel kw_{4(64)}) \dots\dots\dots (2.9)$$

Keterangan:

$C_{(128)}$: Pembentukan ciphertext akhir.

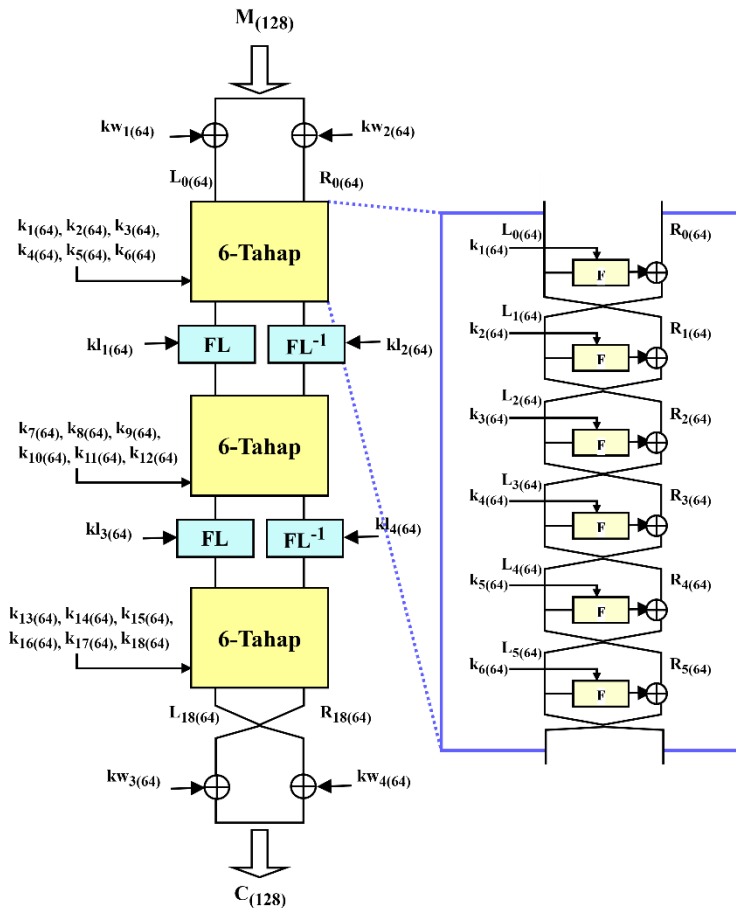
$R_{18(64)}$ dan $L_{18(64)}$: Blok kanan dan kiri setelah 18 putaran.

$\parallel$: Operasi konkatenasi (penggabungan).

kw_3 dan kw_4 : subkunci whitening ketiga dan keempat.

$\oplus$: Operasi XOR antara blok gabungan dan subkunci whitening gabungan.

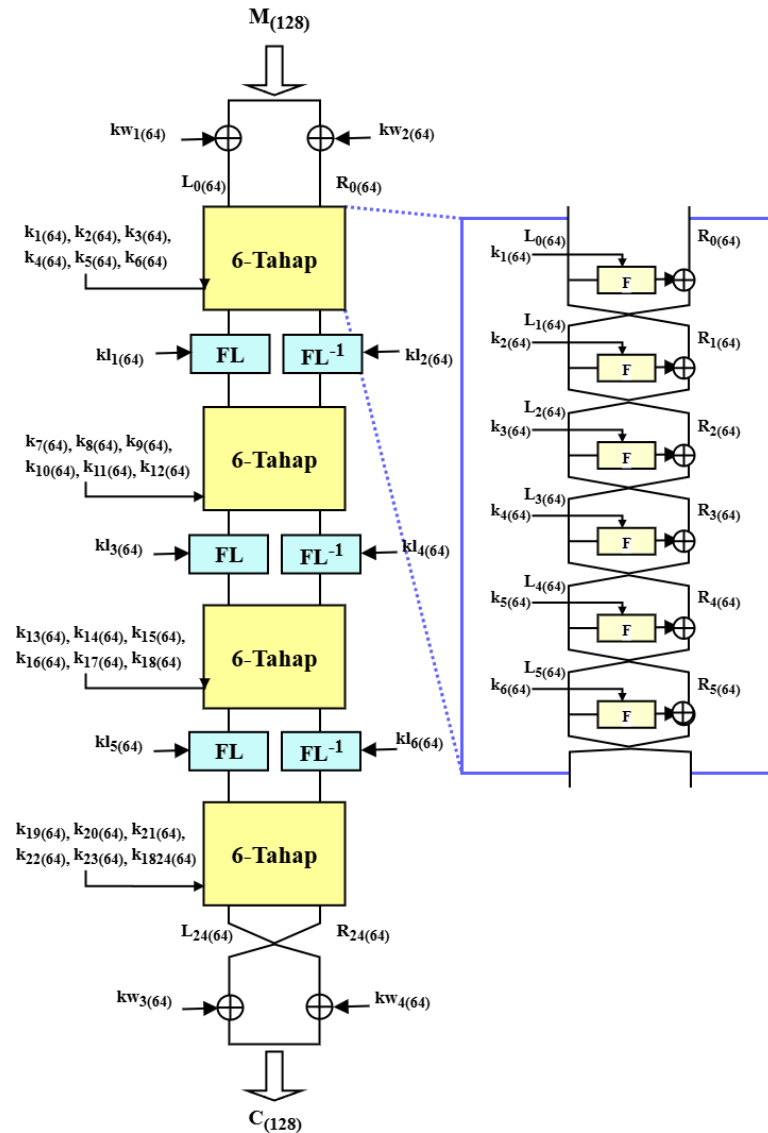
Untuk lebih jelasnya, silahkan lihat gambar berikut yang menggambarkan struktur proses enkripsi Camellia dengan kunci 128 bit:



Gambar 2.3. Prosedur Enkripsi Camellia untuk panjang kunci 128 bit
(Sumber: Aoki et al., 2000)

b. Enkripsi Menggunakan Kunci 192 dan 256 Bit

Enkripsi dengan menggunakan kunci 192 bit dan 256, memiliki jumlah putaran yang lebih banyak, yaitu 24 putaran. Pada enkripsi ini diselipkan 3 buah layer fungsi FL/FL⁻¹ pada putaran ke-6, ke-12, dan ke-18. Tetapi pada proses enkripsi secara umum prosedur sama dengan enkripsi kunci 128 bit. Untuk lebih jelasnya, silahkan lihat gambar berikut yang menggambarkan struktur proses enkripsi Camellia dengan kunci 192 bit dan 256 bit:



Gambar 2.4. Prosedur Enkripsi Camellia untu panjang kunci 192 bit dan 256 bit
(Sumber: Aoki et al., 2000)

3. Proses Dekripsi Algoritma Camellia

Proses dekripsi Camellia dilakukan dengan jalan yang sama dengan proses enkripsi, namun dilakukan dengan urutan subkunci yang dibalik. Sama seperti pada proses enkripsi, prosedur dekripsi juga bergantung pada panjang kunci yang digunakan. Dekripsi dengan kunci 128 bit memiliki struktur berbeda dibandingkan

dengan kunci 192 atau 256 bit, terutama dalam jumlah putaran dan penempatan fungsi FL/FL⁻¹.

a. Dekripsi Menggunakan Kunci 128 Bit

Pada dekripsi dengan kunci 128 bit, pertama-tama blok ciphertext akan dibagi menjadi dua, yaitu L18 dan R18 dengan panjang yang sama. Masing-masing bagian di-XOR dengan subkunci whitening kw3 dan kw4. Hasil dari operasi ini selanjutnya diproses melalui struktur Feistel yang sama seperti pada enkripsi, tetapi dengan penggunaan sub-kunci yang dibalik, yaitu dari k_{18} hingga k_1 . Proses dilakukan secara bertahap, dimulai dari putaran ke-18 hingga putaran ke-1. Seperti halnya pada proses enkripsi, fungsi FL dan FL⁻¹ juga digunakan pada dua titik, yakni sebelum putaran ke-13 dan sebelum putaran ke-7. Hanya saja, sub-kunci yang digunakan juga dibalik, yaitu menggunakan kl_4 dan kl_3 sebelum putaran ke-13, serta kl_2 dan kl_1 sebelum putaran ke-7.

Jika dirumuskan secara matematis, proses dekripsi Camellia dirumuskan sebagai berikut:

$$R_i = L_i \oplus F(R_i, k_i) \dots \dots \dots (2.10)$$

$$L_{i-1} = L_i \dots \dots \dots (2.11)$$

Keterangan:

R_i : Perhitungan blok kanan (R_i) untuk putaran i dalam dekripsi.

L_{i-1} : Perhitungan blok kiri (L_{i-1}) untuk putaran sebelumnya.

L_i : Blok kiri dari putaran saat ini.

$F(R_i, k_i)$: Hasil fungsi F dengan input blok kanan putaran saat ini (R_i) dan subkunci putaran (k_i). Subkunci k_i digunakan secara terbalik dari enkripsi.

Operasi: XOR ($\oplus$) antara L_i dan hasil fungsi F.

Operasi tersebut dilakukan untuk $i=18$ sampai $i=1$, kecuali untuk $i=13$ dan $i=7$, dilakukan operasi sebagai berikut:

$$R'_{i-1} = L_i \oplus F(R_i, k_i) \dots \dots \dots (2.12)$$

$$L'_{i-1} = R_i \dots \dots \dots (2.13)$$

$$R_{i-1} = FL(R'_{i-1}, kl_{2(i-1)/6}) \dots \dots \dots (2.14)$$

$$L_{i-1} = FL^{-1}(L'_{i-1}, kl_{2(i-1)/6-1}) \dots \dots \dots (2.15)$$

Pada tahap terakhir, setelah proses Feistel terbalik selesai, dilakukan operasi XOR antara L_0 dan R_0 dengan subkunci whitening kw_1 dan kw_2 . Hasil penggabungan dua subblok ini merupakan plaintet blok ciphertext.

$$M_{(128)} = (L_{0(64)} \parallel R_{0(64)}) \oplus (kw_{1(64)} \parallel kw_{2(64)}) \dots \dots \dots (2.16)$$

Keterangan:

$M_{(128)}$: Pembentukan plaintext akhir.

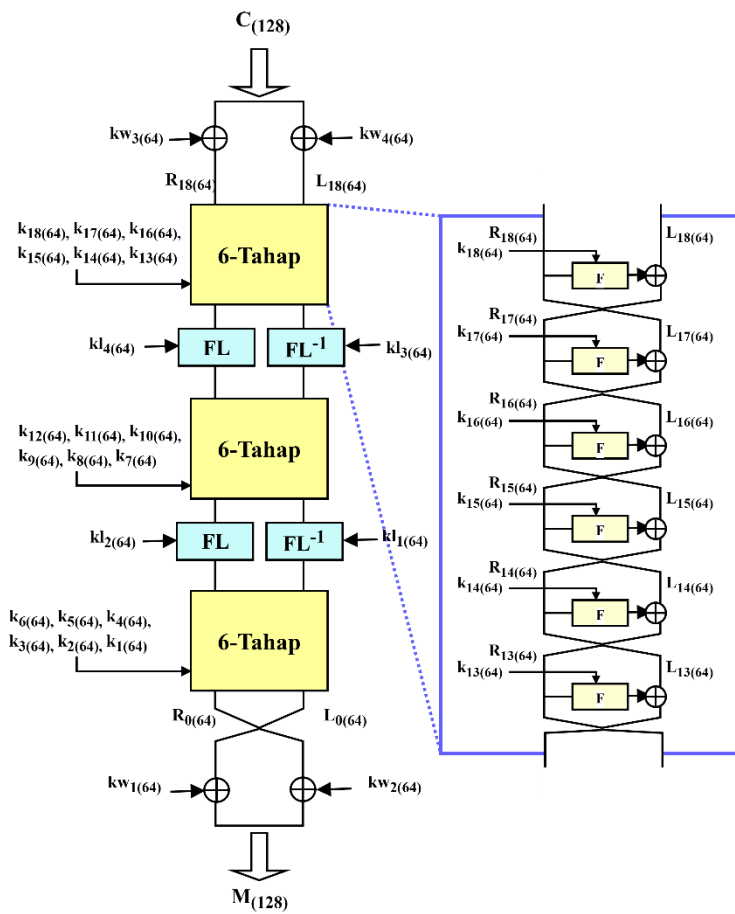
$L_{0(64)}$ dan $R_{0(64)}$: Blok kanan dan kiri setelah putaran dekripsi.

$\parallel$: Operasi konkatenasi (penggabungan).

kw_1 dan kw_2 : subkunci whitening pertama dan kedua.

$\oplus$: Operasi XOR antara blok gabungan dan subkunci whitening gabungan

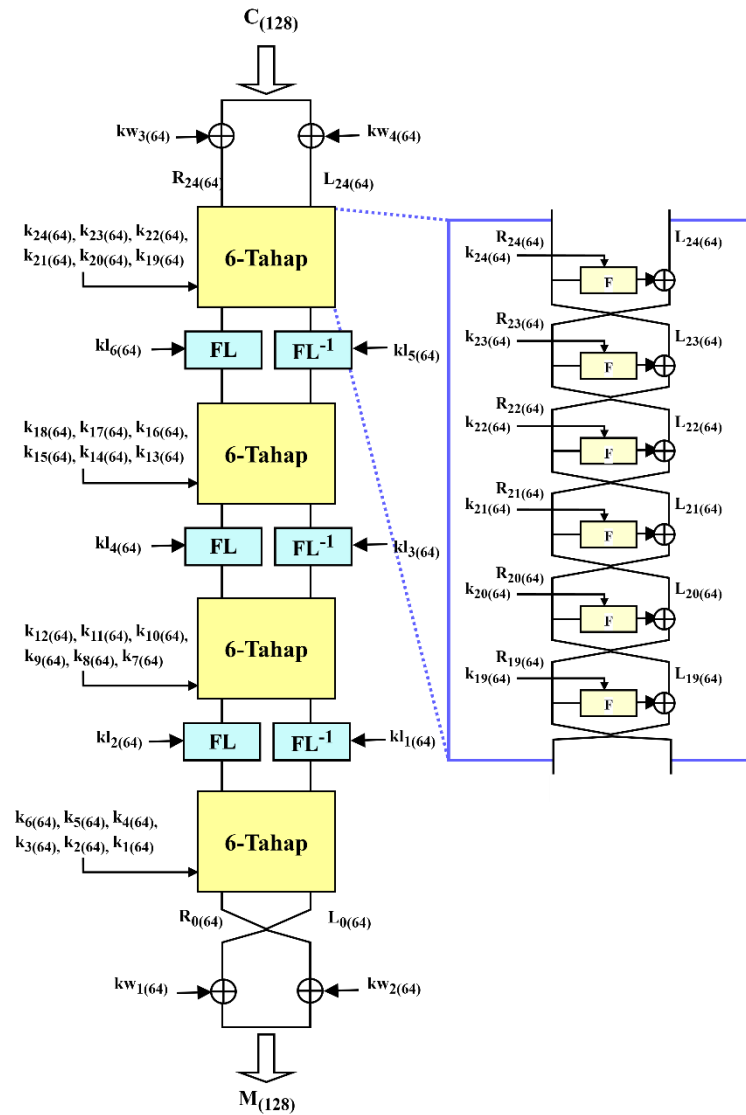
Untuk lebih jelasnya, silahkan lihat gambar berikut yang menggambarkan struktur proses dekripsi Camellia dengan kunci 128 bit:



Gambar 2.5. Prosedur Dekripsi Camellia untuk panjang kunci 128 bit
(Sumber: Aoki et al., 2000)

b. Dekripsi Menggunakan Kunci 192 Bit dan 256 Bit

Proses dekripsi untuk kunci 192 bit atau 256 bit, memiliki struktur 24 putaran feistel dengan 3 lapisan fungsi FL/FL-1 sebelum putaran ke-19, ke-13 dan putaran ke-7. Sama seperti proses dekripsi pada algoritma Camellia dengan kunci 128 bit, proses dekripsi juga menggunakan proses yang sama seperti enkripsi algoritma Camellia dengan kunci 192 bit atau 256 bit, namun dengan urutan penggunaan subkunci yang berkebalikan. Untuk lebih jelasnya, silahkan lihat gambar berikut yang menggambarkan struktur proses dekripsi Camellia dengan kunci 192 bit dan 256 bit:



Gambar 2.6. Prosedur Dekripsi Camellia untuk panjang kunci 192 bit dan 256 bit

(Sumber: Aoki et al., 2000)

4. Komponen Penyusunan Algoritma Camellia

Pada Algoritma Camellia terdapat beberapa fungsi internal, yaitu fungsi F, fungsi FL, fungsi FL-1, fungsi S, dan fungsi P.

a. Fungsi F (F-Fuction)

Fungsi F diperlihatkan pada gambar dibawah ini, yang didefnisikan sebagai berikut:

$$F: L \times L \rightarrow L$$

$$(X_{(64)}, k_{(64)}) \rightarrow Y_{(64)} = (P(S(X_{(64)} \oplus k_{(64)}))) \dots \dots \dots (2.18)$$

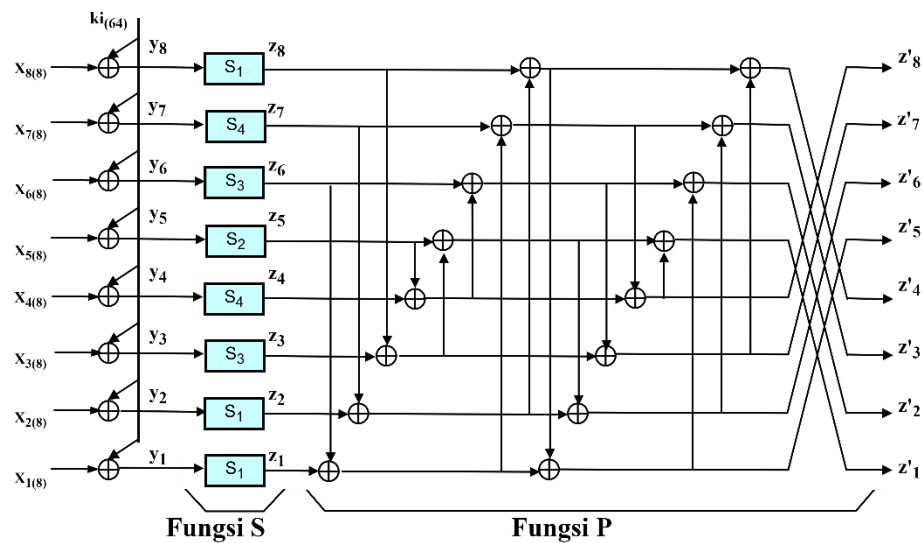
Keterangan:

$X_{(64)}$: Input data 64 bit

$K_{(64)}$: Subkunci 64 bit

S: Fungsi substitusi non-linear menggunakan S-Box

P: Fungsi permutasi linier untuk menyebarkan bit



Gambar 2.7. Fungsi F
(Sumber: Aoki et al., 2000)

Artinya, input 64-bit X akan dioperasikan dengan kunci k (64-bit) menggunakan XOR, kemudian hasilnya masuk ke dalam dua tahap penting Fungsi S (S-Function) dan Fungsi P (P-Function). Output akhir dari Fungsi P adalah $Y_{(64)}$, yang merupakan hasil dari Fungsi F. Output akhir dari Fungsi F adalah blok 64-bit yang disebut Z' (Z aksen), yang akan di-XOR dengan sisi kiri blok dalam proses Feistel untuk menghasilkan nilai baru dalam putaran tersebut.

b. Fungsi S

Fungsi S merupakan fungsi yang menggunakan empat buah S-box. Masing-masing S-box ini menerima input 8 bit dan menghasilkan keluaran 8 bit. Fungsi S

merupakan salah satu bagian dari fungsi F, yang didefinisikan sebagai berikut:

$$S: L \rightarrow L$$

$$l'_{1(8)} = s1(l_{1(8)}),$$

$$l'_{2(8)} = s2(l_{2(8)}),$$

$$l'_{3(8)} = s3(l_{3(8)}),$$

$$l'_{4(8)} = s4(l_{4(8)}),$$

$$l'_{5(8)} = s2(l_{5(8)}),$$

$$l'_{6(8)} = s3(l_{6(8)}),$$

$$l'_{7(8)} = s4(l_{7(8)}),$$

$$l'_{8(8)} = s1(l_{8(8)}), \dots \dots \dots (2.19)$$

Keterangan:

l_1 hingga l_8 : Input 8-bit dari pembagian 64 bit.

$s1$ sampai $s4$: S-box non-linear ukuran 16x16.

S-box yang digunakan ialah berukuran 16*16. Empat buah S-box yang digunakan yaitu $s1$, $s2$, $s3$ dan $s4$ dapat dilihat pada tabel berikut:

Tabel 2. 4. s-box s1

Tabel dibaca sebagai berikut: $s1(0) = 112, s1(1) = 130, \dots, s1(255) = 158$.

112	130	44	236	179	39	192	229	228	133	87	53	234	12	174	65
35	239	107	147	69	25	165	33	237	14	79	78	29	101	146	189
134	184	175	143	124	235	31	206	62	48	220	95	94	197	11	26
166	225	57	202	213	71	93	61	217	1	90	214	81	86	108	77
139	13	154	102	251	204	176	45	116	18	43	32	240	177	132	153
223	76	203	194	52	126	118	5	109	183	169	49	209	23	4	215
20	88	58	97	222	27	17	28	50	15	156	22	83	24	242	34
254	68	207	178	195	181	122	145	36	8	232	168	96	252	105	80
170	208	160	125	161	137	98	151	84	91	30	149	224	255	100	210
16	196	0	72	163	247	117	219	138	3	230	218	9	63	221	148
135	92	131	2	205	74	144	51	115	103	246	243	157	127	191	226
82	155	216	38	200	55	198	59	129	150	111	75	19	190	99	46
233	121	167	140	159	110	188	142	41	245	249	182	47	253	180	89
120	152	6	106	231	70	113	186	212	37	171	66	136	162	141	250
114	7	185	85	248	238	172	10	54	73	42	104	60	56	241	164
64	40	211	123	187	201	67	193	21	227	173	244	119	199	128	158

(Sumber: Aoki et al., 2000)

Tabel 2.5. s-box s2

224	5	88	217	103	78	129	203	201	11	174	106	213	24	93	130
70	223	214	39	138	50	75	66	219	28	158	156	58	202	37	123
13	113	95	31	248	215	62	157	124	96	185	190	188	139	22	52
77	195	114	149	171	142	186	122	179	2	180	173	162	172	216	154
23	26	53	204	247	153	97	90	232	36	86	64	225	99	9	51
191	152	151	133	104	252	236	10	218	111	83	98	163	46	8	175
40	176	116	194	189	54	34	56	100	30	57	44	166	48	229	68
253	136	159	101	135	107	244	35	72	16	209	81	192	249	210	160
85	161	65	250	67	19	196	47	168	182	60	43	193	255	200	165
32	137	0	144	71	239	234	183	21	6	205	181	18	126	187	41
15	184	7	4	155	148	33	102	230	206	237	231	59	254	127	197
164	55	177	76	145	110	141	118	3	45	222	150	38	125	198	92
211	242	79	25	63	220	121	29	82	235	243	109	94	251	105	178
240	49	12	212	207	140	226	117	169	74	87	132	17	69	27	245
228	14	115	170	241	221	89	20	108	146	84	208	120	112	227	73
128	80	167	246	119	147	134	131	42	199	91	233	238	143	1	61

(Sumber: Aoki et al., 2000)

Tabel 2.6. s-box s3

56	65	22	118	217	147	96	242	114	194	171	154	117	6	87	160
145	247	181	201	162	140	210	144	246	7	167	39	142	178	73	222
67	92	215	199	62	245	143	103	31	24	110	175	47	226	133	13
83	240	156	101	234	163	174	158	236	128	45	107	168	43	54	166
197	134	77	51	253	102	88	150	58	9	149	16	120	216	66	204
239	38	229	97	26	63	59	130	182	219	212	152	232	139	2	235
10	44	29	176	111	141	136	14	25	135	78	11	169	12	121	17
127	34	231	89	225	218	61	200	18	4	116	84	48	126	180	40
85	104	80	190	208	196	49	203	42	173	15	202	112	255	50	105
8	98	0	36	209	251	186	237	69	129	115	109	132	159	238	74
195	46	193	1	230	37	72	153	185	179	123	249	206	191	223	113
41	205	108	19	100	155	99	157	192	75	183	165	137	95	177	23
244	188	211	70	207	55	94	71	148	250	252	91	151	254	90	172
60	76	3	53	243	35	184	93	106	146	213	33	68	81	198	125
57	131	220	170	124	119	86	5	27	164	21	52	30	28	248	82
32	20	233	189	221	228	161	224	138	241	214	122	187	227	64	79

(Sumber: Aoki et al., 2000)

Tabel 2. 7. s-box s4

112	44	179	192	228	87	234	174	35	107	69	165	237	79	29	146
134	175	124	31	62	220	94	11	166	57	213	93	217	90	81	108
139	154	251	176	116	43	240	132	223	203	52	118	109	169	209	4
20	58	222	17	50	156	83	242	254	207	195	122	36	232	96	105
170	160	161	98	84	30	224	100	16	0	163	117	138	230	9	221
135	131	205	144	115	246	157	191	82	216	200	198	129	111	19	99
233	167	159	188	41	249	47	180	120	6	231	113	212	171	136	141
114	185	248	172	54	42	60	241	64	211	187	67	21	173	119	128
130	236	39	229	133	53	12	65	239	147	25	33	14	78	101	189
184	143	235	206	48	95	197	26	225	202	71	61	1	214	86	77
13	102	204	45	18	32	177	153	76	194	126	5	183	49	23	215
88	97	27	28	15	22	24	34	68	178	181	145	8	168	252	80
208	125	137	151	91	149	255	210	196	72	247	219	3	218	63	148
92	2	74	51	103	243	127	226	155	38	55	59	150	75	190	46
121	140	110	142	245	182	253	89	152	106	70	186	37	66	162	250
7	85	238	10	73	104	56	164	40	123	201	193	227	244	199	158

(Sumber: Aoki et al., 2000)

c. Fungsi P

Fungsi P adalah transformasi linier yang juga merupakan bagian dari fungsi F. Fungsi ini menerima hasil dari fungsi S dalam bentuk 8 blok data 8 bit (z_1 sampai z_8) dan menghasilkan 8 blok data baru (z'_1 hingga z'_8) yang merupakan hasil permutasi dengan operasi XOR, yang didefinisikan sebagai berikut:

$$P: L \rightarrow L$$

$$z'_1 = z_1 \oplus z_3 \oplus z_4 \oplus z_6 \oplus z_7 \oplus z_8$$

$$z'_2 = z_1 \oplus z_2 \oplus z_4 \oplus z_5 \oplus z_7 \oplus z_8$$

$$z'_3 = z_1 \oplus z_2 \oplus z_3 \oplus z_5 \oplus z_6 \oplus z_8$$

$$z'_4 = z_2 \oplus z_3 \oplus z_4 \oplus z_5 \oplus z_6 \oplus z_7$$

$$z'_5 = z_1 \oplus z_2 \oplus z_6 \oplus z_7 \oplus z_8$$

$$z'_6 = z_2 \oplus z_3 \oplus z_5 \oplus z_7 \oplus z_8$$

$$z'_7 = z_3 \oplus z_4 \oplus z_5 \oplus z_6 \oplus z_8$$

$$z'_8 = z_1 \oplus z_4 \oplus z_5 \oplus z_6 \oplus z_7 \dots\dots\dots (2.20)$$

Keterangan:

z_1 hingga z_8 : Hasil dari fungsi S.

z'_1 hingga z'_8 : Hasil akhir dari fungsi P setelah permutasi XOR.

d. Fungsi FL

Fungsi FL didefinisikan sebagai berikut:

$$F: L \times L \rightarrow L$$

$$(X_{L(32)} \parallel X_{L(32)}, kl_{L(32)} \parallel kl_{R(32)}) \rightarrow Y_{L(32)} \parallel Y_{R(32)}$$

Dengan perhitungan:

$$Y_{R(32)} = ((X_{L(32)} \cap kl_{L(32)}) \lll 1) \oplus X_{R(32)}$$

$$Y_{L(32)} = (Y_{R(32)} \cup kl_{R(32)}) \oplus X_{L(32)} \dots\dots\dots (2.21)$$

Keterangan:

X_L dan X_R : Input data kiri dan kanan, masing-masing 32 bit.

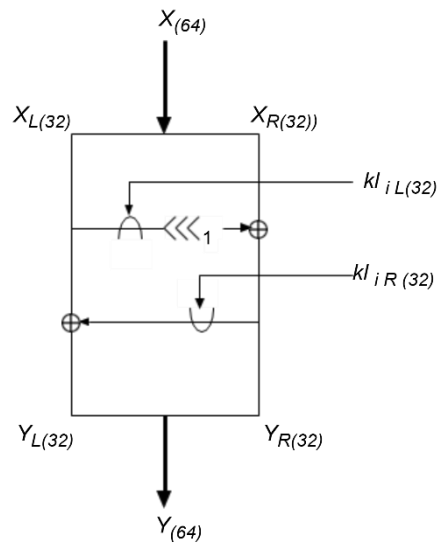
kl_L dan kl_R : Subkunci FL bagian kiri dan kanan.

$\lll 1$: Rotasi bit kiri sebanyak 1 posisi (left circular shift).

$\cap$ dan $\cup$: Operasi AND dan OR logika bit per bit.

Y_R dan Y_L : Output hasil fungsi FL, masing-masing 32 bit.

Fungsi FL diperlihatkan pada gambar berikut:



Gambar 2.8. Fungsi FL
(Sumber: Aoki et al., 2000)

e. Fungsi FL^{-1}

Fungsi FL^{-1} didefinisikan sebagai berikut:

$$FL^{-1}: L \times L \rightarrow L$$

$$(Y_{L(32)} \parallel Y_{R(32)}, kl_{L(32)} \parallel kl_{R(32)}) \rightarrow X_{L(32)} \parallel X_{R(32)}$$

Dimana:

$$X_{L(32)} = (Y_{R(32)} \cup kl_{R(32)}) \oplus Y_{L(32)}$$

$$X_{R(32)} = ((X_{L(32)} \cap kl_{L(32)}) \lll 1) \oplus Y_{R(32)} \dots \dots \dots (2.22)$$

Keterangan:

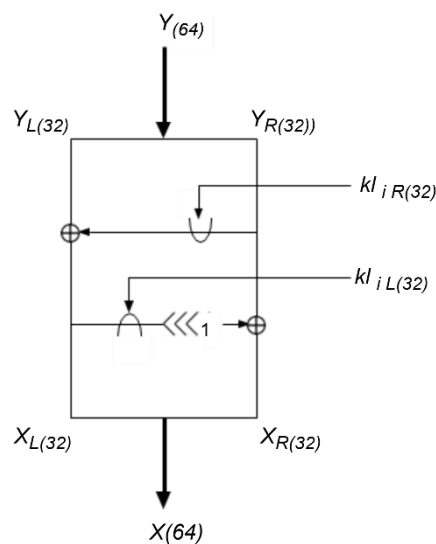
Y_L dan Y_R : Input hasil dari proses FL.

X_L dan X_R : Hasil setelah proses FL^{-1} .

Subkunci kl_L dan kl_R tetap sama seperti pada fungsi FL.

Operasi yang digunakan tetap melibatkan logika OR, AND, XOR, dan rotasi kiri sebanyak 1 bit.

Fungsi FL^{-1} ini diperlihatkan pada gambar berikut:



Gambar 2.9. Fungsi FL^{-1}
(Sumber: Aoki et al., 2000)

Jadi, sebenarnya fungsi FL dan FL^{-1} merupakan fungsi yang saling berkebalikan.

2.10. Sistem Informasi

Sistem informasi merupakan salah satu teknologi yang dibutuhkan untuk memudahkan dalam menemukan informasi yang dibutuhkan dan mengelola data dengan lebih efektif dan efisien. Sistem informasi memegang peran penting, semakin cepat perkembangan teknologi suatu perusahaan atau organisasi maka

semakin penting pula peran sistem informasi tersebut. Saat ini, sistem informasi berbasis web menjadi salah satu sumber informasi yang banyak digunakan. Aplikasi web ini dirancang untuk mempermudah pengguna dalam berinteraksi melalui internet (Arief & Sugiarti, 2022).

Sistem informasi adalah kombinasi terorganisir dari manusia, perangkat keras (hardware), perangkat lunak (software), jaringan komunikasi, dan sumber daya data yang digunakan untuk mengintegrasikan, merubah, dan menyebarkan informasi dalam sebuah perusahaan. Sistem informasi menggunakan manusia sebagai sumber, hardware, software, data, dan jaringan untuk melakukan input, output, proses, penyimpanan, dan pengendalian yang mengubah data menjadi informasi (Arief & Sugiarti, 2022).

2.11. Website

Website adalah suatu sistem yang berkaitan dengan dokumen yang digunakan untuk sebagai media menampilkan teks, gambar, multimedia dan lainnya pada jaringan internet. Website atau situs diartikan sebagai kumpulan halaman yang menampilkan informasi data teks, data gambar diam atau gerak, data animasi, suara, video atau gabungan dari semuanya, baik yang bersifat statis maupun dinamis yang membentuk satu rangkaian bangunan yang saling terkait dimana masing-masing dihubungkan dengan jaringan-jaringan halaman (hyperlink). Bersifat statis apabila isi informasi website tetap, jarang berubah, dan isi informasinya searah hanya dari pemilik website. Bersifat dinamis apabila isi informasinya interaktif dua arah berasal dari pemilik serta pengguna website (Jamaludin & Romindo, 2019).

Dokumen pada website disebut web page (halaman web) dan link dalam website memungkinkan pengguna bisa berpindah dari satu halaman web kehalaman

web lain(hypertext), baik antara server yang sama maupun server diseluruh dunia. Halaman website biasanya berupa dokumen yang ditulis dalam format Hyper Text Markup Language (HTML), yang bisa diakses melalui HTTP. Skrip HTML ini akan diterjemahkan oleh web browser sehingga dapat ditampilkan dalam bentuk informasi yang dapat dibaca oleh semua orang (Permatasari & Suhendi, 2020).

2.12. HTML

HTML merupakan singkatan dari *Hypertext Markup Language* yaitu bahasa standar web yang dikelola penggunaannya oleh W3C (*World Wide Web Consortium*) berupa tag-tag yang menyusun setiap elemen dari website. HTML berperan sebagai penyusun struktur halaman website yang menempatkan setiap elemen website layout yang diinginkan (Permatasari & Suhendi, 2020).

Dalam dunia pemrograman berbasis website, HTML menjadi pondasi dasar pada halaman website. HTML merupakan bahasa pemrograman standar yang digunakan untuk membuat sebuah halaman web, yang kemudian dapat diakses untuk menampilkan berbagai informasi didalam sebuah penjelajah web internet. Fungsi HTML adalah untuk mengelola serangkaian data dan informasi sehingga suatu dokumen dapat diakses dan ditampilkan di internet melalui layanan web (Lengkong et al., 2019).

2.13. PHP

PHP (*Hypertext Preprocessor*) adalah bahasa pemrograman yang digunakan untuk membuat website dinamis dan interaktif. Dinamis artinya, website tersebut bisa berubah-ubah tampilan dan kontennya sesuai kondisi tertentu. PHP merupakan bahasa pemrograman berjenis server-side, yang berarti proses eksekusi kode dilakukan di server yang hasil olahannya akan dikirim kembali ke browser.

Oleh karena itu, salah satu tool yang harus tersedia sebelum memulai pemrograman PHP adalah server. PHP bersifat opensource yang berarti dapat digunakan oleh siapa aja secara gratis (Sulistiati et al., 2020).

Kode PHP dapat disisipkan ke dalam script HTML atau sebaliknya, karena PHP dirancang untuk diterjemahkan oleh komputer dan dijalankan di sisi server. PHP dikhususkan untuk pengembangan web dinamis. Tujuan dari bahasa ini adalah membantu para pengembangan web untuk membuat web dinamis dengan cepat. Agar dapat menjalankan PHP harus menyediakan perangkat lunak berikut web server (Apache, IIS, personal web server/PWS), PHP server dan database server (MySQL, Iterbase, MSSQL) (Damanik, 2021).



Gambar 2.10. Logo PHP
(Sumber: <https://id.wikipedia.org>)

2.14. JavaScript

JavaScript merupakan salah satu bahasa pemrograman tingkat tinggi yang banyak digunakan dalam pengembangan aplikasi berbasis web. Bahasa ini berbentuk kumpulan skrip yang berjalan di dalam dokumen HTML, dan memiliki peran penting dalam menyempurnakan tampilan serta fungsionalitas dari halaman web (Mariko, 2019).

JavaScript merupakan bahasa pemrograman web yang pemrosesannya dilakukan di sisi client (client-side). Karena berjalan di sisi client, JavaScript dapat dijalankan hanya dengan menggunakan browser. Berbeda dengan PHP yang

bekerja di sisi server, untuk menjalankan skrip Java Script tidak memerlukan refresh pada browser. JavaScript biasanya dijalankan ketika ada event tertentu yang terjadi pada halaman web, baik yang dipicu oleh tindakan pengguna seperti klik, input data, atau pergerakan mouse, maupun yang terjadi secara otomatis akibat perubahan pada konten halaman web itu sendiri (Damanik, 2021).

2.15. Mysql

MySQL adalah sebuah perangkat lunak yang terdapat didalam sistem manajemen basis data SQL (database management system) atau yang biasa disebut DBMS yang bersifat multithread dan multi-user. MySQL merupakan sebuah implementasi dari sistem manajemen basis data relasional (RDBMS) yang didistribusikan secara gratis dibawah lisensi GPL (General Public License). Hal ini memungkinkan pengguna untuk memanfaatkan MySQL secara gratis, dengan syarat bahwa perangkat lunak tersebut tidak dijadikan produk turunan yang bersifat komersial. MySQL merupakan sistem database yang banyak digunakan untuk pengembangan aplikasi web dan tergolong sebagai perangkat lunak database server, namun MySQL bukan termasuk bahasa pemrograman (Hidayah & Yani, 2019).

MySQL merupakan server yang melayani database. Untuk membuat dan mengolah database, kita dapat mempelajari pemrograman khusus yang disebut query (perintah) SQL. SQL merupakan konsep dari pengoperasian database, terutama untuk pemilihan atau menyeleksi dan memasukkan data, yang kemungkinan pengoperasian data dikerjakan dengan sangat mudah secara otomatis. Keunggulan MySQL terletak pada kemampuannya dalam menangani banyak permintaan sekaligus dalam satu waktu atau yang disebut Multi-Threading, serta

kemampuannya berfungsi ganda sebagai server maupun client, sehingga sering disebut sebagai sistem client/server database (Damanik, 2021).



Gambar 2.11. Logo MySQL
(Sumber: <https://id.wikipedia.org>)

2.16. Database

Database adalah sebuah kumpulan data yang saling berhubungan secara logis, dan merupakan sebuah penjelasan dari data tersebut, yang didesain untuk menemukan data yang dibutuhkan oleh sebuah organisasi. Di dalam basis data, semua data diintegrasikan dengan menghindari duplikasi data. Basis data dapat digunakan oleh banyak departemen dan pemakai (Sulistiati et al., 2020).

Sistem basis data adalah terkomputerisasi yang tujuan utamanya untuk memelihara data yang telah diolah menjadi informasi dan membuat informasi tersedia saat dibutuhkan. Secara umum, basis data merupakan media penyimpanan data agar dapat diakses dengan mudah dan cepat. Informasi dalam basis data disimpan secara sistematis di dalam komputer, sehingga dapat diperiksa dan diolah menggunakan suatu program komputer untuk menghasilkan keluaran informasi yang berguna. Database adalah tempat penyimpanan suatu kumpulan data yang terkait secara teknis dan dapat membuat sebuah program berisikan table, field, dan record. Database merupakan tempat penyimpanan data berupa kumpulan dari file atau table yang bisa dikelola dan saling terhubung (Damanik, 2021).

2.17. Pemodelan Beorientasi Objek (UML)

UML (Unified Modeling Language) adalah suatu metode dalam pemodelan secara visual yang digunakan sebagai sarana perancangan sistem berorientasi objek. UML merupakan bahasa standar yang digunakan untuk mendokumentasikan, merancang, dan membangun perangkat lunak. Dengan menggunakan UML memungkinkan para pengembang untuk menjabarkan kebutuhan sistem, melakukan analisis dan desain sistem, serta memvisualisasikan arsitektur sistem dalam konteks pemrograman berorientasi objek. UML berperan sebagai metodologi dalam pengembangan sistem berorientasi objek, sekaligus alat bantu untuk mendukung proses pengembangan tersebut. Saat ini, UML telah menjadi bahasa standar dalam pembuatan rancangan awal (blueprint) perangkat lunak (Ratu et al., 2024).

Alat bantu yang digunakan dalam perancangan berorientasi objek berbasis UML adalah:

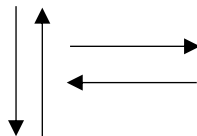
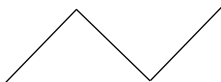
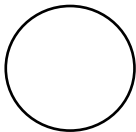
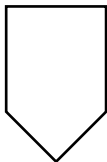
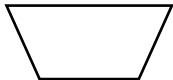
1. *Flowchart*

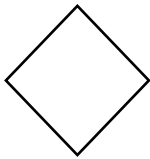
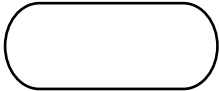
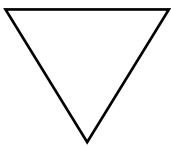
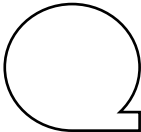
Flowchart atau sering disebut dengan diagram alir merupakan suatu jenis diagram yang merepresentasikan algoritma atau langkah-langkah instruksi yang berurutan dalam sistem. Seorang analis sistem menggunakan *flowchart* sebagai bukti dokumentasi untuk menjelaskan gambaran logis sebuah sistem yang akan dibangun kepada programmer. Dengan begitu, *flowchart* dapat membantu untuk memberikan solusi terhadap masalah yang bisa saja terjadi dalam membangun sistem. *Flowchart* digambarkan dengan menggunakan simbol-simbol. Setiap simbol mewakili suatu proses tertentu. Sedangkan untuk menghubungkan satu

proses ke proses selanjutnya digambarkan dengan menggunakan garis penghubung (Rosaly & Prasetyo, 2019).

Berikut ini adalah simbol-simbol *flowchart*, seperti yang terlihat pada tabel dibawah ini:

Tabel 2.8. Simbol *Flowchart*

Simbol	Nama	Fungsi
	Flow Direction Symbol/ Connecting Line	Berfungsi untuk menghubungkan simbol yang satu dengan yang lainnya, menyatakan arus suatu proses.
	Communication Link	Berfungsi untuk transmisi data dari satu lokasi ke lokasi lain.
	Connector	Digunakan untuk meyatakan sambungan dari proses yang satu ke proses berikutnya di halaman yang sama.
	Offline Connector	Digunakan untuk menyatakan sambungan dari proses yang satu ke proses berikutnya di halaman yang berbeda.
	Processing	Digunakan untuk menunjukkan pengolahan yang akan dilakukan dalam komputer.
	Manual Operation	Digunakan untuk menunjukkan pengolaha yang tidak dilakukan oleh komputer.

	Decision	Digunakan untuk memilih proses yang akan dilakukan berdasarkan kondisi tertentu.
	Predefined Process	Digunakan untuk mempersiapkan penyimpanan yang sedang/akan digunakan dengan memberikan harga awal.
	Terminal	Digunakan untuk memulai atau mengakhiri program.
	Offline Storage	Berfungsi untuk menunjukkan bahwa data akan disimpan ke media tertentu.
	Manual Input Symbol	Digunakan untuk menginputkan data secara manual dengan keyboard.
	Input/Output	Digunakan untuk menyatakan input dan output tanpa melihat jenisnya.
	Punched Card	Digunakan untuk menyatakan masukan dan keluaran yang berasal dari card.
	Disk Storage	Digunakan untuk menyatakan masukan dan keluaran yang berasal dari disk.
	Magnetic Tape	Digunakan untuk menyatakan masukan dan keluaran yang berasal dari pita magnetis.

	Document	Digunakan untuk menyatakan masukan dan keluaran yang berasal dari dokumen.
	Display	Digunakan untuk menyatakan keluaran melalui layar monitor.

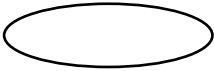
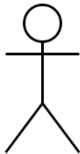
(Sumber: Rosaly & Prasetyo, 2019)

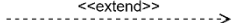
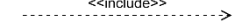
2. Use Case Diagrams

Diagram *Use Case* merupakan pemodelan untuk kelakuan sistem informasi yang akan dibangun. *Use Case* mendeskripsikan sebuah interaksi antara satu atau lebih aktor dengan sistem informasi yang akan dibangun. *Use Case* digunakan untuk mengetahui fungsi apa saja yang ada pada sebuah sistem informasi dan siapa saja yang berhak menggunakan fungsi-fungsi tersebut (Hutabri & Putri, 2019).

Berikut ini adalah simbol-simbol diagram *use case*, seperti yang terlihat pada tabel dibawah ini:

Tabel 2.9. Simbol Use Case Diagram

Simbol	Nama	Deskripsi
	<i>Use Case</i>	Deskripsikan dari urutan aksi-aksi yang ditampilkan sistem yang menghasilkan suatu hasil yang terukur bagi suatu aktor.
 Actor	Aktor / Actor	Aktor adalah abstraction dari orang atau sistem yang lain yang mengaktifkan fungsi dari target sistem. Untuk mengidentifikasikan aktor, harus ditentukan pembagian tenaga kerja dan

		tugas-tugas yang berkaitan dengan peran pada konteks target sistem. Orang atau sistem bisa muncul dalam beberapa peran.
	Association	Komunikasi antara aktor dan <i>use case</i> yang berpartisipasi pada <i>use case</i> atau <i>use case</i> memiliki interaksi dengan aktor
	Extend	Menspesifikasikan bahwa <i>use case</i> target memperluas perilaku dari <i>use case</i> sumber pada suatu titik yang diberikan.
	Generalization	Hubungan generalisasi dan spesialisasi (umum – khusus) antara dua buah <i>use case</i> dimana fungsi yang satu adalah fungsi yang lebih umum dari lainnya.
	Uses atau Include	Merupakan relasi dua <i>use case</i> , <i>use case</i> yang ditambahkan dengan <i>use case</i> tambahan. <i>Use case</i> yang ditambahkan memerlukan <i>use case</i> tambahan untuk menjalankan kegunaan atau fungsi sebagai syarat menjalankan <i>use case</i> .

(Sumber: Hutabri & Putri, 2019)

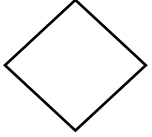
3. Diagram Aktivitas (*Activity Diagram*)

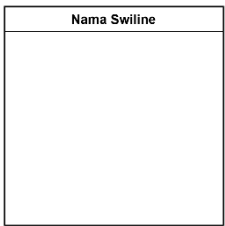
Diagram aktivitas (*activity diagram*) mendeskripsikan aliran kerja (*workflow*) atau aktivitas sistem atau proses bisnis atau menu yang terdapat di dalam sistem

atau perangkat lunak. Penekanan pada diagram aktivitas adalah menggambarkan aktivitas sistem atau aktivitas yang dapat dilakukan oleh sistem atau aktivitas yang dapat dilakukan oleh sistem, bukan apa yang dilakukan aktor (Hutabri & Putri, 2019).

Berikut ini adalah simbol-simbol *activity* diagram, seperti yang terlihat pada tabel dibawah ini:

Tabel 2.10. Simbol *Activity* Diagram

Simbol	Nama	Deskripsi
	Status Awal	Merupakan status awal keadaan dari sistem, setiap diagram memiliki satu status awal.
	Status Akhir	Merupakan status akhiri keadaan dari sistem, setiap diagram memiliki satu status akhir.
	Aktivitas	Merupakan kegiatan yang dilakukan sistem, sering dimulai dengan kata kerja.
	Decision (Percabangan)	Merupakan hubungan percabangan untuk keputusan aktivitas yang memiliki lebih dari satu pilihan.
	Join (Penggabungan)	Merupakan hubungan penggabunga jika satu atau lebih aktivitas menjadi satu.

	Swimlane	Merupakan yang memisahkan organisasi bisnis. Memiliki tanggung jawab aktivitas yang terjadi.
---	----------	--

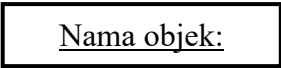
(Sumber: Hutabri & Putri, 2019)

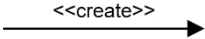
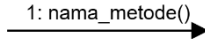
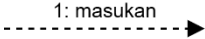
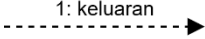
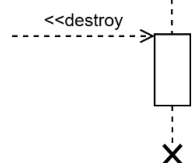
4. Diagram Urutan (*Sequence Diagram*)

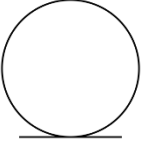
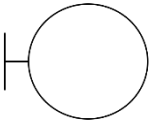
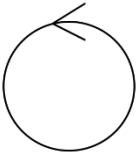
Diagram Urutan (*Sequence Diagram*) mendeskripsikan perilaku objek pada *use case* dengan menjelaskan alur waktu hidup dari objek dan pesan atau message yang diterima dan dikirim antar objek (Hutabri & Putri, 2019).

Berikut ini adalah simbol-simbol *sequence* diagram, seperti yang terlihat pada tabel dibawah ini:

Tabel 2.11. Simbol *Sequence Diagram*

Simbol	Nama	Deskripsi
	Aktor	Merupakan orang atau sistem lain atau proses diluar sistem yang dibuat, yang berhubungan dengan sistem yang dibuat. Aktor belum tentu orang, walaupun memiliki simbol bergambar orang.
	Lifeline (Garis Hidup)	Merupakan garis hidup objek yang menerangkan kehidupan objek.
	Objek	Merupakan objek yang melakukan interaksi pesan.

	Waktu Aktif	Merupakan simbol yang menyatakan bahwa objek dalam keadaan berinteraksi dan keadaan aktif, dan semua yang berhubungan dengan waktu aktif merupakan tahapan yang dilakukan selama dalam keadaan aktif.
	Pesan Tipe Create	Merupakan pernyataan satu objek membuat objek lain.
	Pesan Tipe Call	Merupakan pernyataan satu objek memanggil metode atau operasi pada objek lain atau diri sendiri
	Pesan Tipe Send	Merupakan pernyataan bahwa objek mengirimkan informasi atau masukan atau data ke objek lain.
	Pesan Tipe Return	Merupakan pernyataan bahwa objek menjalankan metode atau operasi yang memberi hasil suatu pengembalian atau keluaran ke objek tertentu.
	Pesan Tipe Destory	Merupakan pernyataan bahwa satu objek mengakhiri hidup dari objek lain, arah panah yang mengarah

		pada objek yang diakhiri. jika ada creat maka ada destory.
	Entity Class	Gambaran sistem sebagai landasan dalam menyusun basis data
	Boundary Class	Menangani komunikasi antar lingkungan sistem
	Control Class	Bertanggung jawab terhadap kelas-kelas terhadap objek yang berisi logika.

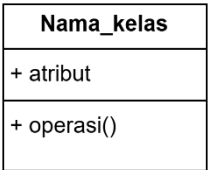
(Sumber: Hutabri & Putri, 2019)

5. Diagram Kelas (Class Diagram)

Class Diagram atau Diagram kelas digunakan untuk membuat sistem dengan mendeskripsikan struktur sistem dari sisi pendefinisian kelas yang dibuat. Kelas memiliki variabel-variabel yang dimiliki oleh kelas (atribut) dan fungsi-fungsi yang dipunyai oleh kelas (metode atau operasi) (Hutabri & Putri, 2019).

Berikut ini adalah simbol-simbol class diagram, seperti yang terlihat pada tabel dibawah ini:

Tabel 2.12. Simbol Class Diagram

Simbol	Nama	Deskripsi
	Class (Kelas)	Merupakan kelas yang ada pada struktur sistem. Memiliki atribut dan operasi dalam kelas.

	<i>Interface</i> (antarmuka)	Merupakan kemiripan dengan kelas tetapi memiliki metode yang di deklarasikan tanpa isi dan tanpa atribut kelas.
	Association (Asosiasi)	Merupakan relasi antarkelas (umum), biasanya dilengkapi dengan multiplicity.
	Directed Association (Asosiasi berarah)	Merupakan relasi antara kelas bermakna satu kelas digunakan oleh kelas yang lain, biasanya dilengkapi dengan multiplicity.
	Generalisasi	Merupakan relasi antara kelas bermakna generalisasi-spesialisasi (umum ke khusus).
	Dependency (Kebergantungan)	Merupakan relasi kebergantungan (dependency) antara kelas.
	Aggregation (Agregasi)	Merupakan relasi antara kelas bermakna semua-bagian (whole-part)

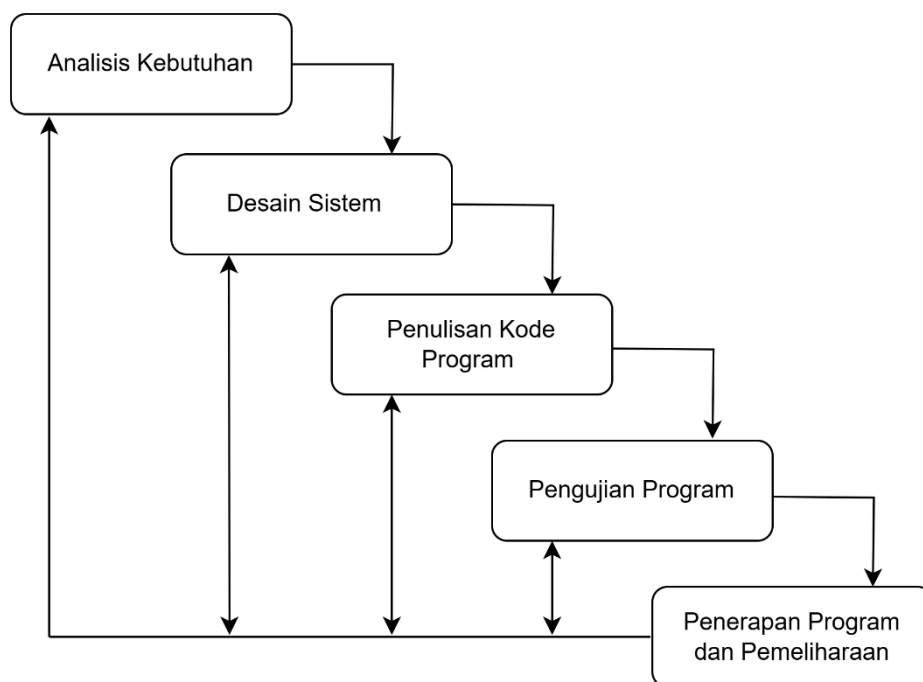
(Sumber: Hutabri & Putri, 2019)

BAB III

METODOLOGI PENELITIAN

3.1. Tahapan Penelitian

Pada penelitian ini, metode perancangan sistem yang digunakan adalah waterfall. Metode waterfall adalah pengerjaan dari suatu sistem dilakukan secara berurutan atau secara linear. Tahapan dalam model waterfal yaitu analisis, desain, penulisan, pengujian dan penerapan serta pemeliharaan. Berikut adalah gambar model waterfall:



Gambar 3.1. Metodel Waterfall Dalam Perancangan Sistem

1. Analisis Kebutuhan

Tahap awal dalam metode ini adalah melakukan analisis terhadap kebutuhan yang diperlukan untuk mencapai tujuan penelitian yang dilakukan. Pada tahap ini, dilakukan identifikasi dan mengumpulkan semua informasi yang

diperlukan, yang akan digunakan sebagai dasar dalam perancangan program yang akan dibangun.

2. Desain Sistem

Setelah kebutuhan sistem diperoleh, tahap selanjutnya adalah mendesain sistem. Pada tahap ini dilakukan perancangan sistem baik dari sisi tampilan, basis data, maupun proses enkripsi dan dekripsi data. Desain sistem menggunakan pemodelan UML yaitu perancangan *flowchart*, *use case diagram*, *class diagram*, *activity diagram*, *sequence diagram* dan *user interface*. Tujuan dari tahap ini adalah untuk memberikan gambaran teknis secara keseluruhan sebelum implementasi dimulai.

3. Penulisan Kode Program

Pada tahap ini desain sistem diimplementasikan ke dalam kode program menggunakan bahasa pemrograman. Proses ini diawali dengan perancangan desain antarmuka pengguna (*user interface*) menggunakan sintak HTML dan CSS. Selanjutnya, logika program sistem dikembangkan menggunakan bahasa pemrograman PHP dan Javascript, serta pengolahan data dilakukan pada database MySQL.

4. Pengujian Program

Tahap pengujian bertujuan untuk memastikan bahwa sistem berjalan sesuai dengan fungsinya dan bebas dari kesalahan. Proses Pengujian ini dilakukan untuk memastikan data dapat dienkripsi dan dekripsi menggunakan algoritma camellia dapat bekerja dengan baik dan menghasilkan output yang sesuai. Selain itu, pengujian ini juga bertujuan untuk memastikan desain antarmuka

pengguna telah sesuai dengan alur logika dan struktru sistem yang telah dirancang.

5. Penerapan Program dan Pemeliharaan

Pada tahap ini merupakan langkah terakhir dalam perancangan sistem, setelah program dinyatakan berjalan dengan baik, sistem kemudian diterapkan di lingkungan yang sebenarnya. Pada tahap ini dilakukan juga pemeliharaan berkelanjutan untuk memperbaiki bug, melakukan peningkatan, dan memastikan sistem tetap berfungsi dengan baik seiring waktu.

3.2. Metode Pengumpulan Data

Dalam penelitian ini, data yang digunakan diperoleh melalui beberapa metode pengumpulan data yang dilakukan untuk menunjang proses perancangan dan pembangunan sistem. Adapun metode yang digunakan adalah sebagai berikut:

1. Pengamatan (Observation)

Metode pengumpulan data yang dilakukan dengan cara mengamati secara langsung ke lokasi penelitian pada SD Muhammadiyah 08 Medan. Tujuan dari metode ini adalah untuk memperoleh data faktual yang sesuai dengan keadaan di lapangan. Melalui observasi ini, penulis mengamati proses pengelolaan dan penyimpanan data yang masih dilakukan secara konvensional atau sistem digital, namun belum didukung oleh sistem pengamanan data yang memadai.

2. Wawancara (Interview)

Metode data yang dilakukan melalui sesi tanya jawab secara langsung kepada responden untuk mendapatkan informasi yang lebih mendalam. Dalam penelitian ini, penulis melakukan sesi tanya jawab dengan Kepala Sekolah dan Bendahara SD Muhammadiyah 08 Medan.

3. Studi Pustaka

Penulis mengumpulkan dan mempelajari berbagai referensi dan teori yang berkaitan dengan topik penelitian, seperti artikel ilmiah, jurnal, buku dan penelitian terdahulu yang serupa.

3.3. Perancangan Sistem

Dalam perancangan sistem pada penelitian ini, penulis menggunakan pemodelan UML (Unified Modeling Language) untuk menggambarkan proses dan struktur sistem. UML digunakan untuk memodelkan interaksi antar pengguna dan sistem, alur data, dan komponen internal sistem. Pemodelan ini mencakup *flowchart*, *use case diagram*, *class diagram*, *activity diagram*, dan *sequence diagram*.

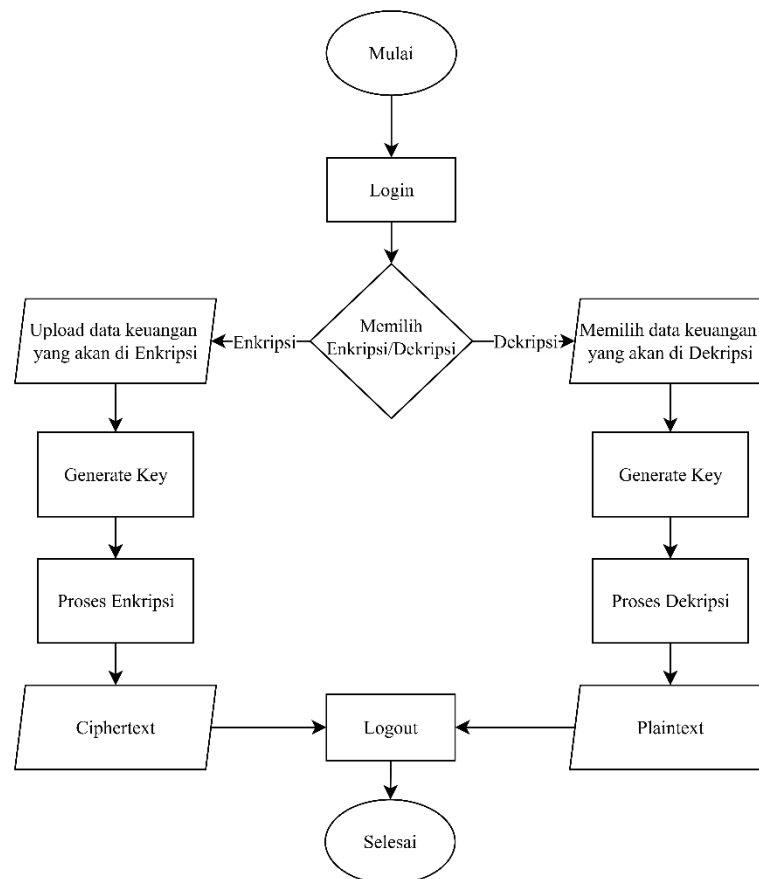
Pada penelitian ini, implementasi algoritma kriptografi Camellia penulis menggunakan panjang kunci 128 bit. Pemilihan panjang kunci ini dilakukan untuk menyederhanakan proses perancangan dan pengujian sistem, sekaligus karena kunci 128 bit sudah dianggap aman untuk kebutuhan pengamanan data. Oleh karena itu, seluruh proses sistem, diagram, serta logika enkripsi dan dekripsi yang ditampilkan dalam penelitian ini berfokus pada struktur algoritma Camellia dengan 18 putaran enkripsi, yang sesuai dengan standar penggunaan panjang kunci 128 bit.

3.3.1. *Flowchart*

Flowchart digunakan untuk menggambarkan alur kerja sistem secara lebih detail. *Flowchart* dibawah ini menggambarkan urutan langkah-langkah dari proses utama yang mencakup alur program secara keseluruhan, proses pembangkitan kunci (generate key), proses enkripsi data, dan proses dekripsi data.

1. *Flowchart* Alur Program

Flowchart ini menunjukkan alur kerja utama dari sistem mulai dari pengguna *login*, pemilihan menu enkripsi atau dekripsi, hingga *logout*. Jika pengguna memilih enkripsi, maka sistem akan menjalankan proses unggah data, generate key, dan enkripsi. Sedangkan jika memilih dekripsi, pengguna akan memilih file yang akan di dekripsi, generate key, dan menjalankan proses dekripsi. Setelah proses selesai sistem menampilkan hasil, dan pengguna dapat keluar dari sistem. *Flowchart* alur program sistem dapat dilihat pada *flowchart* dibawah ini:



Gambar 3.2. *Flowchart* Alur Program

2. *Flowchart* Proses Pembangkitan Kunci (Generate Key)

Flowchart ini menggambarkan proses pembangkitan kunci pada algoritma Camellia dengan panjang kunci 128 bit. Pada *flowchart* menunjukkan tahapan-tahapan mulai dari input kunci, pemrosesan dengan nilai konstanta, hingga pembangkitan subkey yang akan digunakan pada proses enkripsi dan dekripsi.

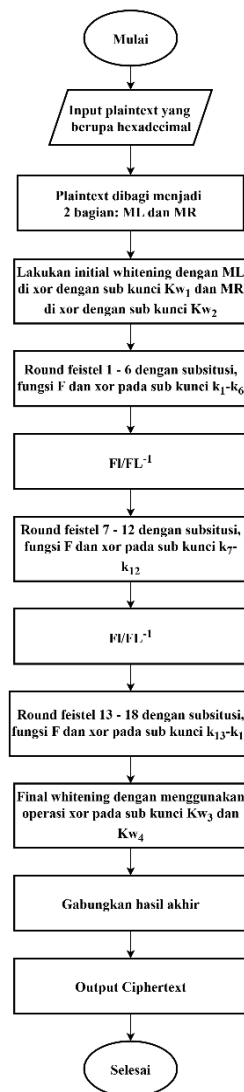
Flowchart proses pembangkitan kunci (generate key) pada algoritma kriptografi Camellia dengan panjang kunci 128 bit dapat dilihat pada *flowchart* dibawah ini:



Gambar 3.3. *Flowchart* Proses Generate Key

3. *Flowchart* Proses Enkripsi Data

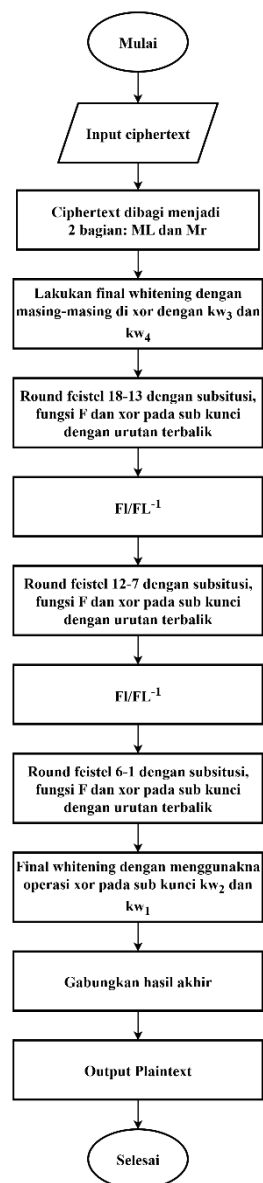
Flowchart proses enkripsi data menggambarkan langkah-langkah yang diambil untuk mengenkripsi data menggunakan algoritma Camellia. Proses dimulai dengan user mengunggah data yang ingin dienkripsi, memasukkan kunci yang akan digunakan dalam proses enkripsi. Setelah kunci dihasilkan, sistem akan melakukan proses enkripsi, yang mengubah data asli menjadi *ciphertext*. *Flowchart* proses enkripsi pada algoritma kriptografi Camellia dengan panjang kunci 128 bit dapat dilihat pada *flowchart* dibawah ini:



Gambar 3.4. *Flowchart* Proses Enkripsi Data

4. *Flowchart* Proses Dekripsi Data

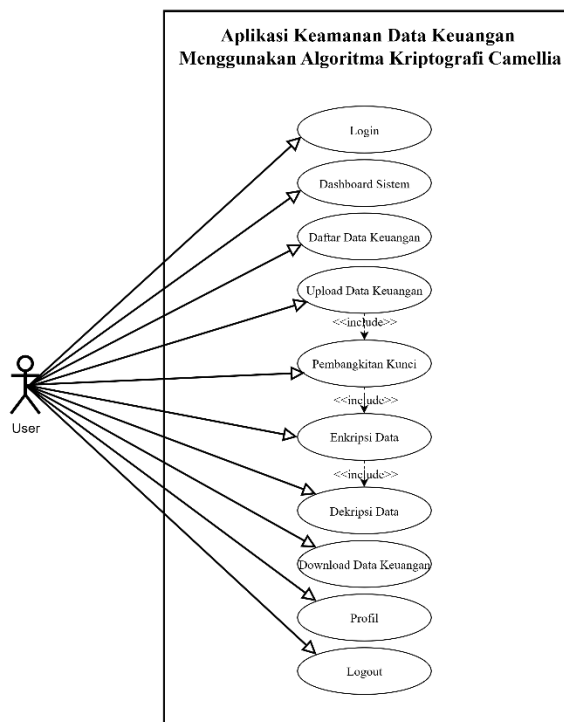
Flowchart proses dekripsi data menggambarkan langkah-langkah yang diambil untuk mengembalikan data yang telah dienkripsi ke bentuk aslinya (*plaintext*). Proses ini dimulai dengan pengguna memilih file terenkripsi dan memasukkan kunci yang sama seperti saat proses enkripsi. *Flowchart* proses dekripsi pada algoritma kriptografi Camellia dengan panjang kunci 128 bit dapat dilihat pada *flowchart* dibawah ini:



Gambar 3.5. *Flowchart* Proses Dekripsi Data

3.3.2. Use Case Diagram

Dalam penyusunan suatu program diperlukan suatu model data yang berbentuk diagram yang dapat menjelaskan suatu alur proses sistem yang akan dibangun. Dalam penulisan skripsi ini penulis menggunakan metode UML (Unified Modeling Language), salah satu adalah *use case* diagram. *Use case* diagram mendeskripsikan interaksi antara pengguna (aktor) dengan sistem yang akan dibangun, serta fungsionalitas yang diharapkan dari sebuah sistem. Adapun rancangan sistem berdasarkan *use case* diagram dapat dilihat pada gambar dibawah ini:



Gambar 3.6. Use Case Diagram Aplikasi Keamanan Data Keuangan Menggunakan Algoritma Kriptografi Camellia

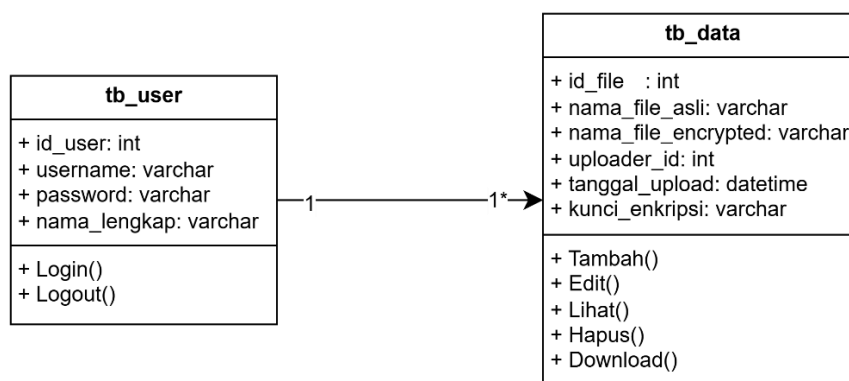
Penjelasan:

Pada gambar 3.6 terdapat use case diagram aplikasi keamanan data keuangan menggunakan algoritma Camellia. Use case tersebut menggambarkan

interaksi antara bendahara SD Muhammadiyah 08 medan sebagai aktor utama dengan sistem. Bendahara dapat mengelola data keuangan serta menjaga keamanan data. Beberapa aktivitas utama yang dilakukan dalam sistem ini meliputi proses login ke dalam sistem, menampilkan halaman dashboard, melihat daftar data keuangan, serta melakukan enkripsi dan dekripsi data, dengan cara mengunggah file yang ingin dilindungi dan memasukkan kunci. Selanjutnya, sistem akan membangkitkan kunci enkripsi dan menerapkan algoritma Camellia untuk mengamankan data tersebut Hasil dari proses enkripsi maupun dekripsi dapat diunduh oleh pengguna. Setelah selesai, pengguna dapat logout dari sistem untuk memastikan bahwa tidak ada akses tidak sah ke informasi mereka.

3.3.3. Class Diagram

Class diagram digunakan untuk menggambarkan struktur sistem secara logis, dengan mendefinisikan kelas, atribut, metode serta hubungan antar kelas dalam sistem. Adapun rancangan kelas-kelas yang akan digunakan pada sistem yang akan dirancang dapat dilihat pada gambar dibawah ini:



Gambar 3.7. Class Diagram Pada Sistem

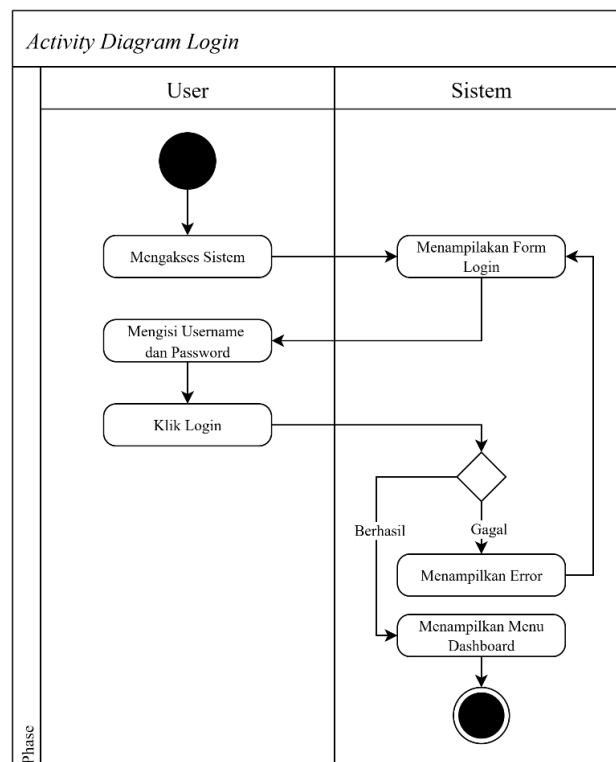
3.3.4. Activity Diagram

Activity Diagram mendeskripsikan aliran kerja (workflow) atau aktivitas sistem yang terdapat di dalam sistem secara rinci. Diagram ini menunjukkan

proses langkah demi langkah, dari awal hingga akhir aktivitas, sehingga memudahkan dalam memahami logika kerja sistem. Adapun rancangan activity diagram adalah sebagai berikut:

1. *Activity Diagram Login*

Diagram ini menggambarkan alur pengguna saat melakukan proses *login* ke sistem. Pengguna diminta untuk memasukkan username dan password yang valid pada form login. Rancangan *Activity Diagram Login* dapat dilihat pada gambar dibawah ini:

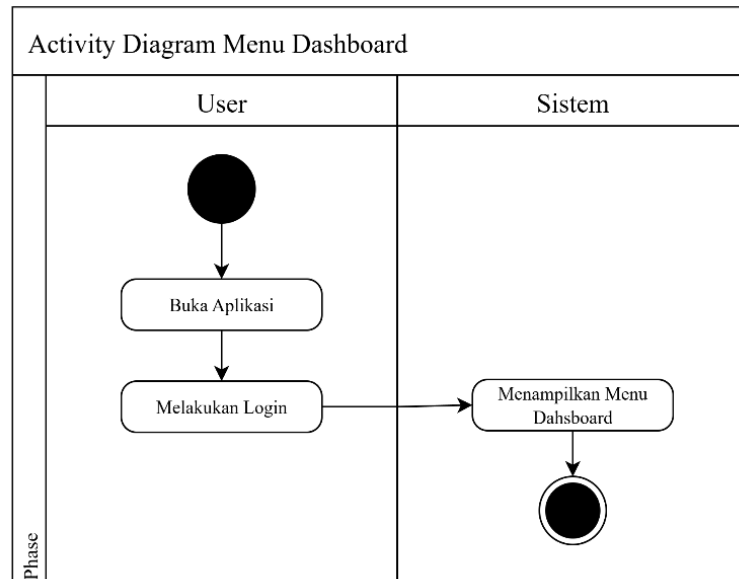


Gambar 3.8. Activity Diagram Login

2. *Activity Diagram Menu Dashboard*

Diagram ini menampilkan alur pengguna setelah berhasil *login*. Pada halaman dashboard, terdapat beberapa navigasi yaitu daftar file terenkripsi,

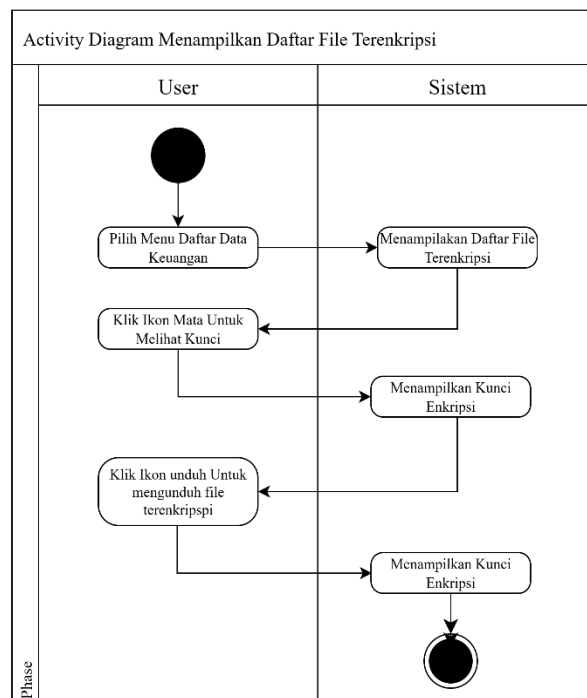
melakukan proses enkripsi, dekripsi, melihat profil, dan logout. Rancangan *Activity Diagram* Menu Dashboard dapat dilihat pada gambar dibawah ini:



Gambar 3.9. Activity Diagram Dashboard

3. Activity Diagram Menampilkan Daftar File Terenkripsi

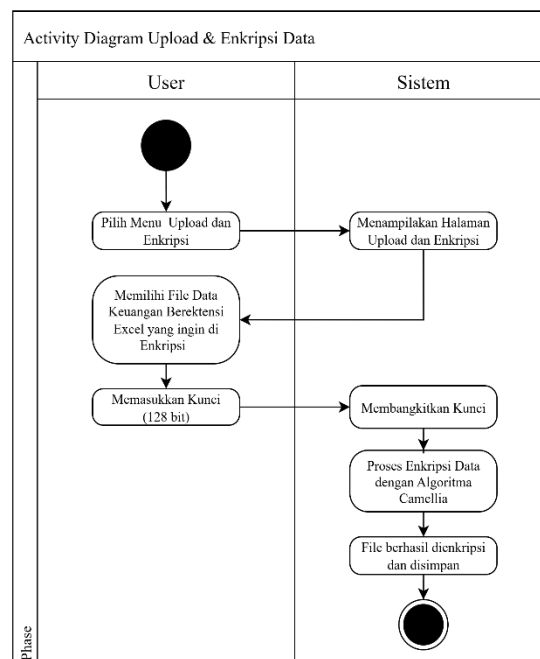
Diagram ini menampilkan daftar data keuangan yang telah tersimpan oleh pengguna setelah melalui proses enkripsi. Pada halaman Daftar File Terenkripsi, pengguna sistem menyediakan fitur bagi pengguna untuk melihat kunci enkripsi, melakukan dekripsi file dan mengunduh file yang telah terenkripsi. Rancangan *Activity Diagram* Menampilkan Daftar File Terenkripsi dapat dilihat pada gambar dibawah ini:



Gambar 3.10. Activity Diagram Menampilkan Daftar File Terenkripsi

4. Activity Diagram Enkripsi Data

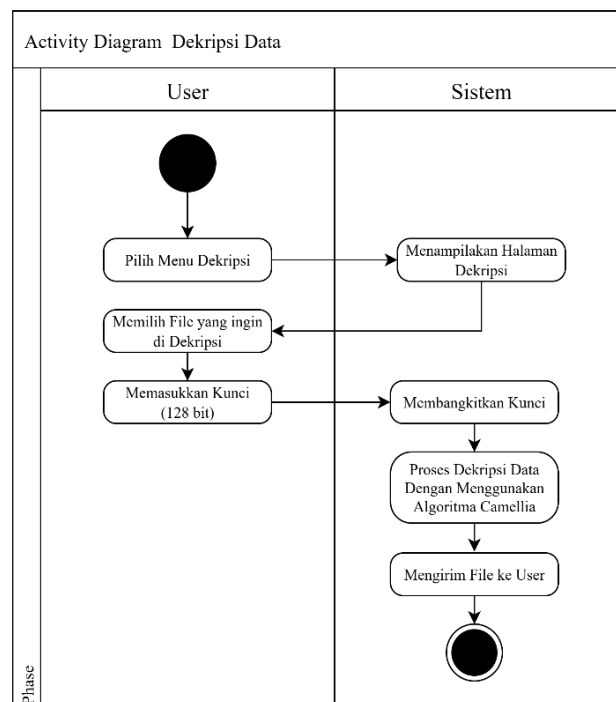
Diagram ini menampilkan aktivitas pengguna dalam melakukan enkripsi file data keuangan. Proses dimulai dari pemilihan file, input kunci enkripsi, hingga sistem membangkitkan sub-kunci dan menerapkan algoritma Camellia. Hasil enkripsi disimpan dalam database dan pengguna dapat mengunduh file terenkripsi pada menu Daftar File Terenkripsi. Rancangan *Activity Diagram* Enkripsi Data dapat dilihat pada gambar dibawah ini:



Gambar 3.11. Activity Diagram Enkripsi Data

5. Activity Diagram Dekripsi Data

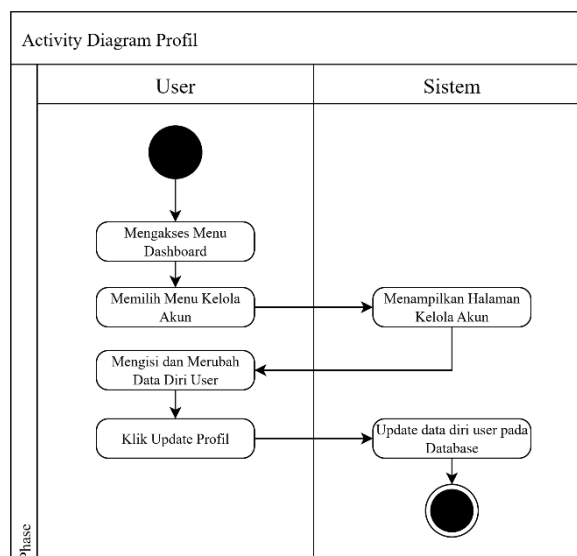
Diagram ini menampilkan aktivitas pengguna dalam melakukan dekripsi data yang sebelumnya telah dienkripsi. Pengguna memilih file terenkripsi, memasukkan kunci yang sesuai, dan sistem akan memproses dekripsi dengan algoritma camellia. Rancangan *Activity Diagram Dekripsi Data* dapat dilihat pada gambar dibawah ini:



Gambar 3.12. Activity Diagram Dekripsi Data

6. Activity Diagram Kelola Akun

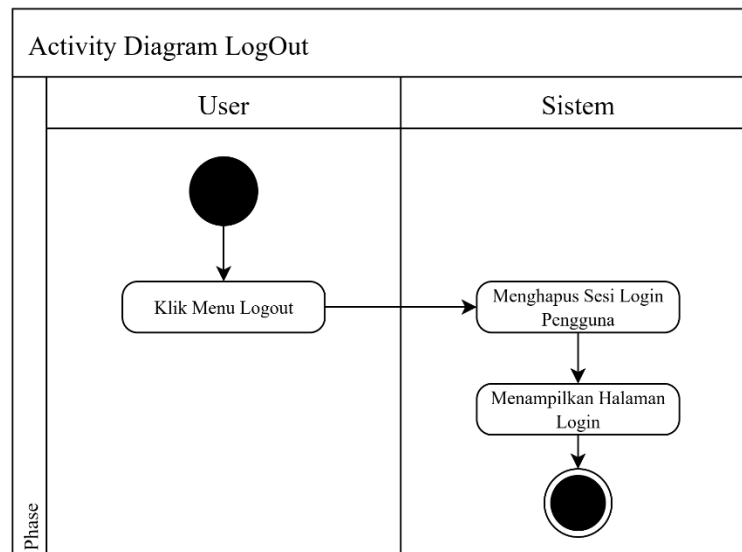
Diagram ini menggambarkan aktivitas pengguna ketika mengakses halaman Kelola Akun. Pengguna dapat melihat dan melakukan mengubah Username dan Password. Rancangan Activity Diagram Profil dapat dilihat pada gambar dibawah ini:



Gambar 3.13. Activity Diagram Kelola Akun

7. Activity Diagram Logout

Diagram ini menggambarkan alur ketika pengguna saat melakukan proses logout dari sistem. Proses ini akan menghapus sesi *login* pengguna dan mengarahkan kembali ke halaman login. Rancangan *Activity Diagram Logout* dapat dilihat pada gambar dibawah ini:



Gambar 3.14. Activity Diagram Logout

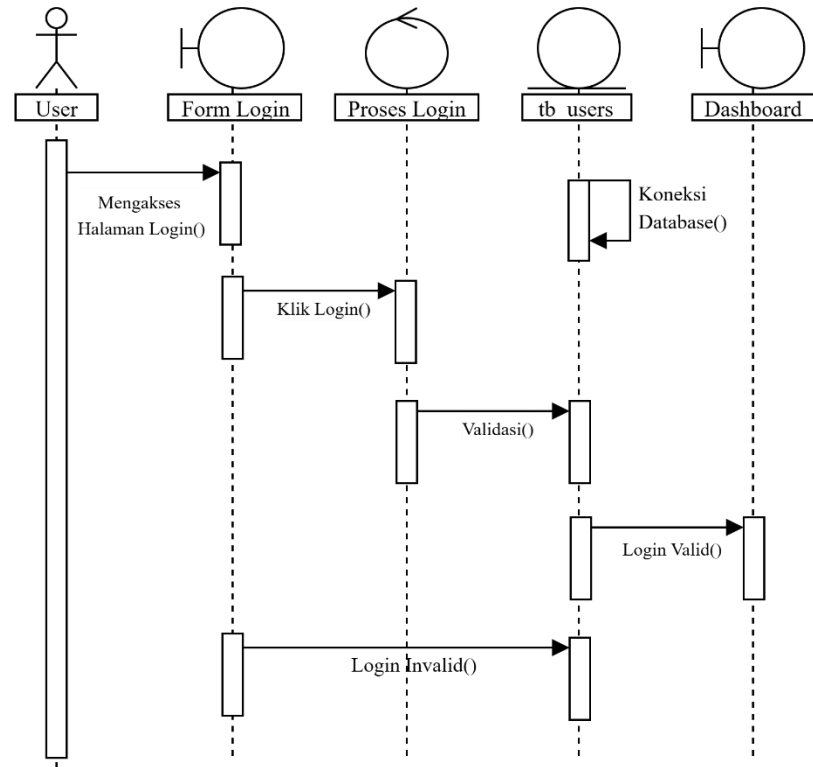
3.3.5. Sequence Diagram

Sequence Diagram adalah diagram yang digunakan untuk menggambarkan perilaku antar objek dalam sistem, dengan menunjukkan urutan pesan yang dikirim dan diterima antar objek sesuai dengan alur waktu dari atas ke bawah.

1. Sequence Diagram Login

Diagram ini menggambarkan interaksi antara pengguna dan sistem saat melakukan proses *login*. Dimulai dari pengguna mengisi username dan password, kemudian sistem memverifikasi data tersebut dengan data pada database. Jika sesuai, sistem akan memberikan akses ke halaman dashboard.

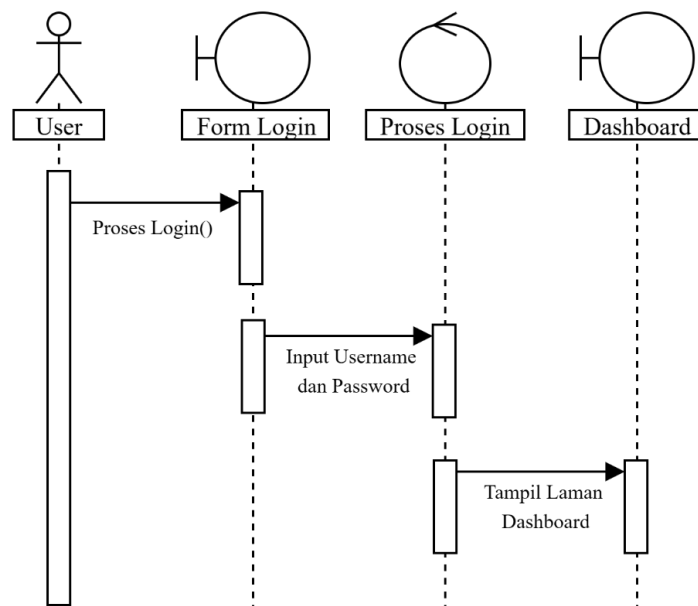
Jika tidak sesuai, sistem menampilkan pesan kesalahan. *Sequence Diagram Login* dapat dilihat pada gambar dibawah ini:



Gambar 3.15. Sequence Diagram Login

2. Sequence Diagram Menu Dashboard

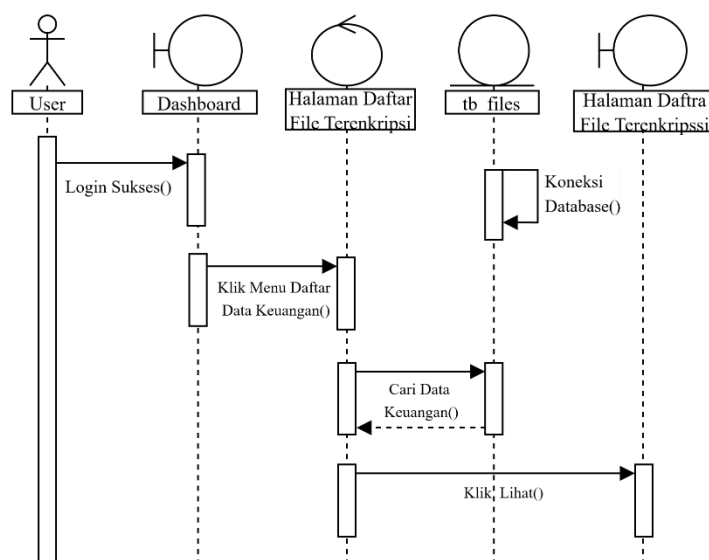
Diagram ini menampilkan alur interaksi pengguna setelah berhasil login dan mengakses dashboard. Pada tahap ini, pengguna dapat memilih navigasi yang tersedia yaitu, melihat daftar file terenkripsi, enkripsi data, dekripsi data, melihat profil atau keluar dari sistem. *Sequence Diagram tampilan menu dashboard sistem* dapat dilihat pada gambar dibawah ini:



Gambar 3.16. Sequece Diagram Menampilkan Menu Dashboard

3. *Sequence Diagram Menampilkan Daftar File Terenkripsi*

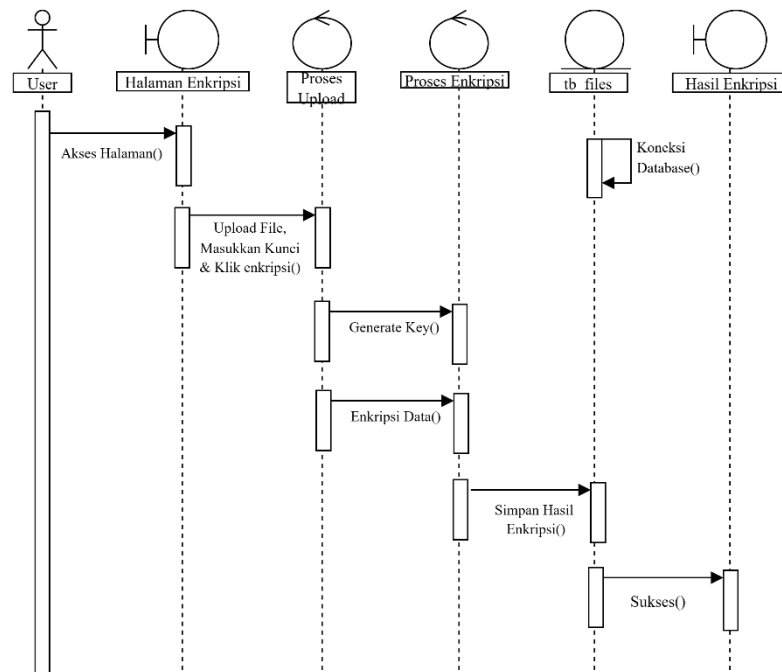
Diagram ini menunjukkan proses ketika pengguna memilih untuk melihat daftar file terenkripsi. Sistem mengambil data dari database dan menampilkannya dalam bentuk tabel. Data yang ditampilkan mencakup file yang sudah melalui proses enkripsi. Sequence Diagram menampilkan daftar file dapat dilihat pada gambar dibawah ini:



Gambar 3.17. Sequence Diagram menampilkan daftar data keuangan

4. Sequence Diagram Enkripsi Data

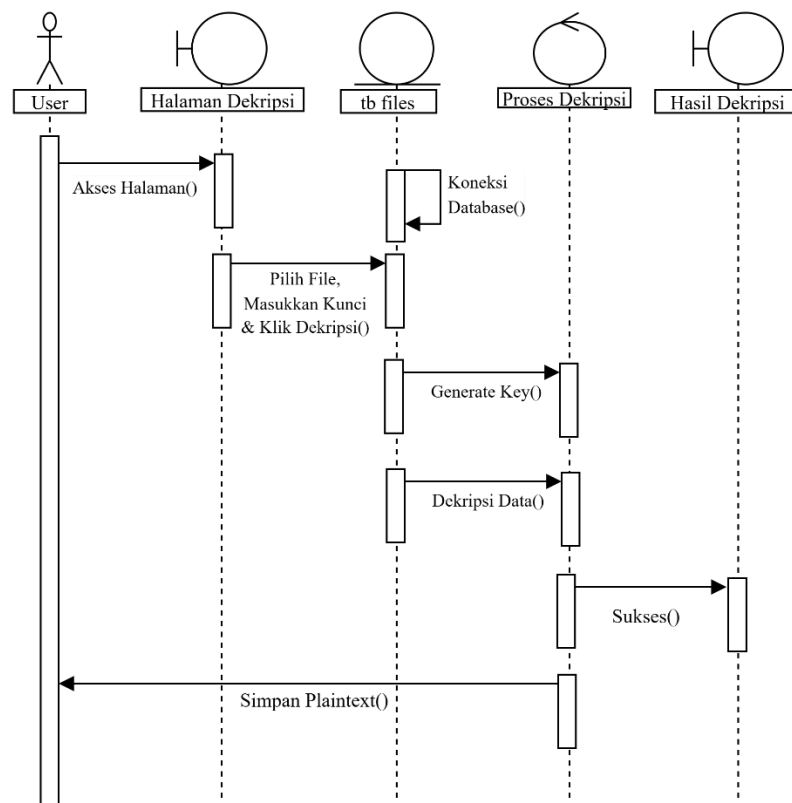
Diagram ini menggambarkan alur pengguna saat melakukan enkripsi data. Pengguna mengunggah file dan memasukkan kunci, kemudian sistem melakukan proses pembangkitan sub kunci dan enkripsi dengan algoritma Camellia. Hasil file yang terenkripsi disimpan ke database. *Sequence Diagram* proses enkripsi data keuangan dapat dilihat pada gambar dibawah ini:



Gambar 3.18. Sequence Diagram Enkripsi Data

5. Sequence Diagram Dekripsi Data

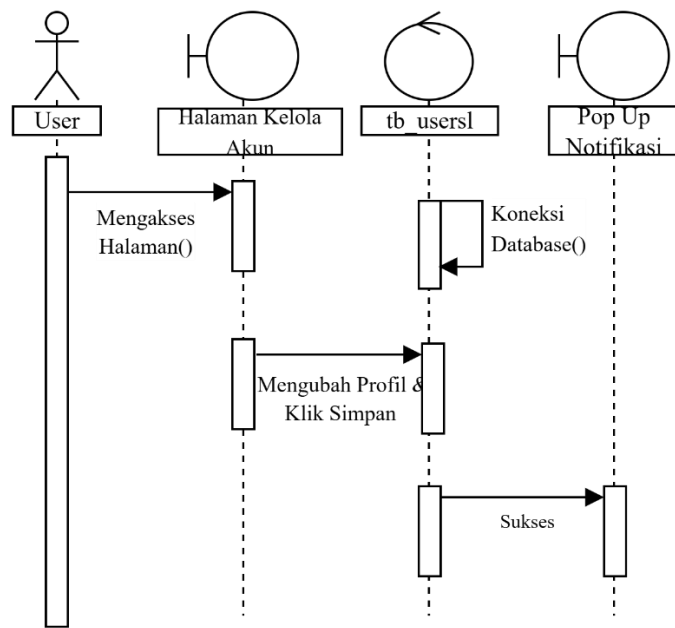
Diagram ini menjelaskan proses saat pengguna ingin mengembalikan file terenkripsi ke bentuk semula. Pengguna memilih file terenkripsi dan memasukkan kunci. Sistem melakukan proses dekripsi dengan kunci yang sama, lalu sistem akan mengunduh file. *Sequence Diagram* proses dekripsi data keuangan dapat dilihat pada gambar dibawah ini:



Gambar 3.19. Sequence Diagram Dekripsi Data

6. Sequence Diagram Kelola Akun

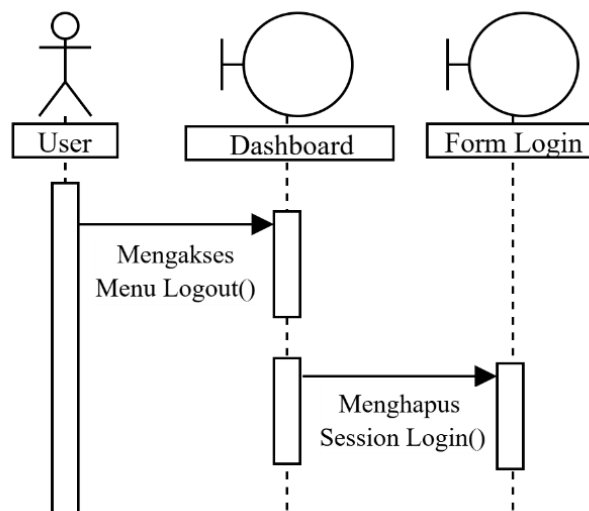
Diagram ini memperlihatkan alur ketika pengguna mengakses halaman kelola akun. Sistem mengambil data pengguna dari database dan menampilkannya di antarmuka. Pengguna juga dapat mengedit informasi akun pada tahap ini. *Sequence Diagram* kelola akun dapat dilihat pada gambar dibawah ini:



Gambar 3.20. Sequence Diagram Kelola AKun

7. Sequence Diagram Logout

Diagram ini menggambarkan proses logout dari sistem. Pengguna memilih tombol logout, lalu sistem mengakhiri sesi login dan mengarahkan pengguna kembali ke halaman login awal. *Sequence Diagram Logout* keuangan dapat dilihat pada gambar dibawah ini:

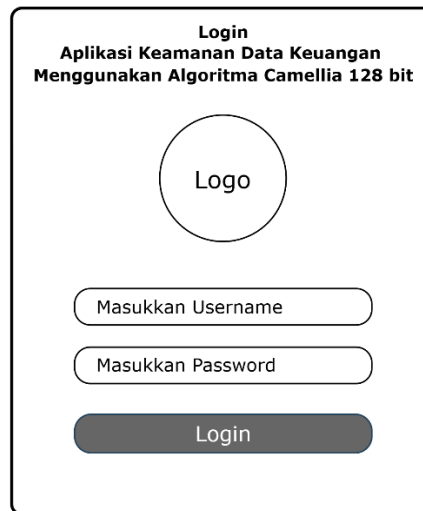


Gambar 3.21. Sequence Diagram Logout

3.4. Desain *Interface* Sistem

3.4.1. Desain *Interface* Form *Login*

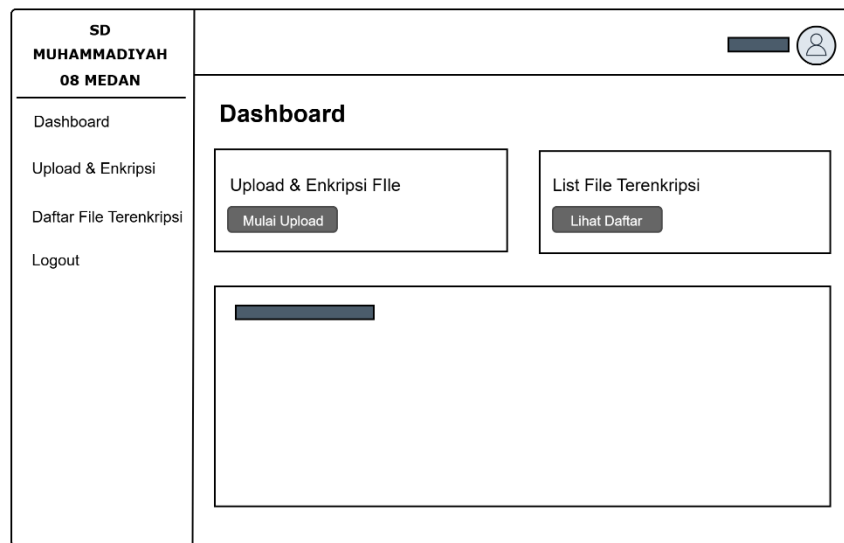
Desain tampilan form *login* merupakan tampilan awal yang digunakan oleh pengguna untuk mengakses sistem. Adapun rancangan antarmuka form *login* dapat dilihat pada gambar dibawah ini:

The image shows a login form interface within a rounded rectangular border. At the top, the text 'Login' is centered, followed by 'Aplikasi Keamanan Data Keuangan' and 'Menggunakan Algoritma Camellia 128 bit'. Below this is a circular placeholder labeled 'Logo'. Underneath the logo are two input fields: 'Masukkan Username' and 'Masukkan Password'. At the bottom is a dark gray button labeled 'Login'.

Gambar 3.22. Desain *Interface* Form *Login*

3.4.2. Desain *Interface* Dashboard

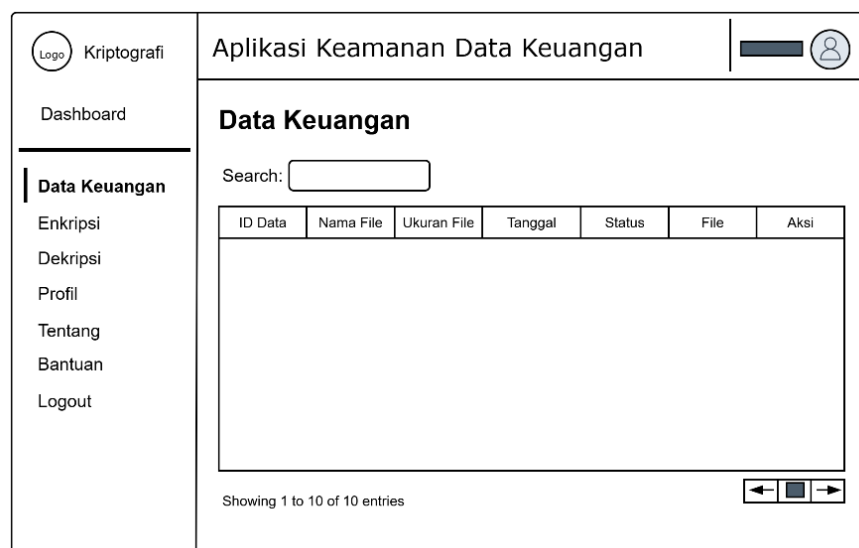
Desain halaman dashboard merupakan halaman utama yang ditampilkan setelah pengguna berhasil *login*. Pada halaman ini tersedia berbagai menu navigasi yang mengarahkan pengguna ke fitur utama sistem yaitu lihat file terenkripsi, enkripsi data, dan dekripsi data. Adapun rancangan antarmuka halaman dashboard dapat dilihat pada gambar dibawah ini:



Gambar 3.23. Desain *Interface* Dashboard

3.4.3. Desain *Interface* Data File Terenkripsi

Desain halaman data file terenkripsi berfungsi untuk menampilkan daftar file data keuangan yang telah diunggah oleh user. Pada halaman ini, user dapat melihat informasi data seperti nama file, tanggal unggah, serta kunci enkripsi. Adapun rancangan antarmuka halaman data keuangan dapat dilihat pada gambar dibawah ini:



Gambar 3.24. Desain *Interface* Data File Terenkripsi

3.4.4. Desain *Interface* Form Upload & Enkripsi

Desain form enkripsi digunakan untuk melakukan proses enkripsi data keuangan menggunakan algoritma Camellia. User dapat memilih file yang ingin dienkripsi, memasukkan kunci, lalu klik button enkripsi file untuk memulai proses enkripsi. Adapun rancangan antarmuka form enkripsi dapat dilihat pada gambar dibawah ini:

Gambar 3.25. Desain *Interface* Form Upload & Enkripsi

3.4.5. Desain *Interface* Form Dekripsi

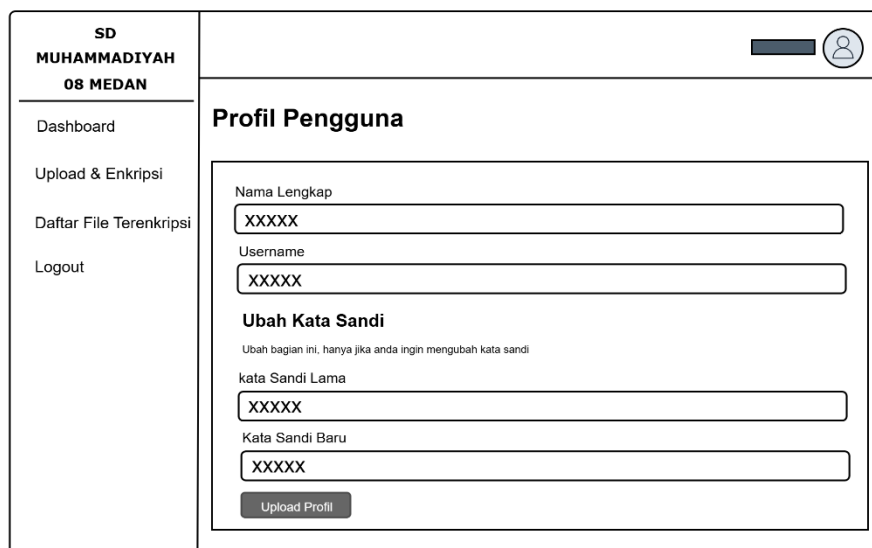
Desain form enkripsi berfungsi untuk menampilkan halaman yang digunakan user untuk melakukan proses dekripsi file yang sebelum telah dienkripsi. User dapat memilih file yang terenkripsi dan memasukkan kunci yang sesuai. Adapun rancangan antarmuka form dekripsi dapat dilihat pada gambar dibawah ini:



Gambar 3.26. Desain *Interface* Form Dekripsi

3.4.6. Desain *Interface* Kelola Akun

Desain halaman profil menampilkan informasi akun pengguna. Halaman ini memungkinkan pengguna untuk melihat atau memperbarui data pribadinya. Adapun rancangan antarmuka halaman profil dapat dilihat pada gambar dibawah ini:



Gambar 3.27. Desain *Interface* Profil

BAB IV

HASIL DAN UJI COBA

4.1. Perhitungan Algoritma Camellia

Pada tahap ini membahas pengujian proses pembangkitan kunci, enkripsi dan dekripsi menggunakan algoritma kriptografi Camellia pada sistem yang dikembangkan. Pengujian dilakukan untuk memastikan bahwa algoritma kriptografi Camellia telah bekerja dengan benar dalam mengamankan data. Pada pengujian sistem ini, penulis menggunakan 1 file data keuangan sekolah sebagai objek uji.

Sampel yang digunakan untuk proses perhitungan enkripsi dan dekripsi Camellia diambil baris pertama file, yaitu sebanyak 16 karakter awal yang berisi teks **“Laporan Keuangan”** pada file data keuangan sekolah. Pada proses ini, penulis menggunakan panjang kunci 128bit dengan rincian sebagai berikut:

Plaintext : Laporan Keuangan

Kunci : SKRIPSI2024HUSNI

1. Proses Penjadwalan Kunci Algoritma Camellia

Penjadwalan kunci adalah proses awal yang digunakan untuk menghasilkan sub kunci dari kunci utama. Sub kunci ini akan digunakan dalam setiap tahap putaran proses enkripsi dan dekripsi. Kunci utama terlebih dahulu dibagi menjadi dua bagian, kemudian diproses dengan nilai konstanta $\sum_1, \sum_2, \sum_3, \sum_4$ untuk menghasilkan nilai K_A . Setelah itu sub kunci K_w, k dan k_l dibangkitkan dari nilai hasil rotasi penggeseran bit dari K_L, K_R , dan K_A .

Σ_1	0xA09E6673FBCC908B
Σ_2	0xB67AE8584CAA73B2
Σ_3	0xC6EF372FE94F82BE
Σ_4	0x54FF53A5F1D36F1C
Σ_5	0x10E527FADE682D1D
Σ_6	0xB05688C2B3E6C1FD

Kunci = SKRIPSI2024HUSNI

= 534B 5249 5053 4932 3032 3448 3553 4E49

a. KL = 534B 5249 5053 4932 3032 3448 5553 4E49

KL_L = 534B 5249 5053 4932

KL_R = 3032 3448 5553 4E49

b. Misalkan $P(S(KL_L \oplus \Sigma_1)) = A$

$A \oplus KL_R = A'$

$P(S(A' \oplus \Sigma_2)) = B$

$B \oplus KL_L = B'$

$P(S(B \oplus \Sigma_3)) = C$

$C \oplus A = C'$

$P(S(C' \oplus \Sigma_4)) = D$

$D \oplus B = D'$

$D' \parallel C' = K_A$

$A = KL_L \oplus \Sigma_1$

= 534B 5249 5053 4932 $\oplus$ A09E 6673 FBCC 908B

= F3D5 343A AB9F D9B9

$P(S(A_{8(8)})) = F3 = S_1(243) = 123 = 7B$

$P(S(A_{7(8)})) = D5 = S_4(213) = 255 = FF$

$P(S(A_{6(8)})) = 34 = S_3(52) = 534 = EA$

$$P(S(A_{5(8)})) = 3A = S_2(58) = 180 = B4$$

$$P(S(A_{4(8)})) = AB = S_4(171) = 5 = 05$$

$$P(S(A_{3(8)})) = 9F = S_3(159) = 74 = 4A$$

$$P(S(A_{2(8)})) = D9 = S_2(217) = 74 = 4A$$

$$P(S(A_{1(8)})) = B9 = S_1(185) = 150 = 96$$

$$A = 7BFF\ EAB4\ 054A\ 4A96$$

$$A' = A \oplus KL_R$$

$$= 7BFF\ EAB4\ 054A\ 4A96 \oplus 3032\ 3448\ 5553\ 4E49$$

$$= 4BCD\ DEFC\ 5019\ 04DF$$

$$B = A' \oplus \sum_2$$

$$= 4BCD\ DEFC\ 5019\ 04DF \oplus B67A\ E858\ 4CAA\ 73B2$$

$$= FDB7\ 36A4\ 1CB3\ 776D$$

$$P(S(B_{8(8)})) = FD = S_1(253) = 199 = C7$$

$$P(S(B_{7(8)})) = B7 = S_4(183) = 34 = 22$$

$$P(S(B_{6(8)})) = 36 = S_3(54) = 174 = AE$$

$$P(S(B_{5(8)})) = A4 = S_2(164) = 155 = 9B$$

$$P(S(B_{4(8)})) = 1C = S_4(28) = 217 = D9$$

$$P(S(B_{3(8)})) = B3 = S_3(179) = 19 = 13$$

$$P(S(B_{2(8)})) = 77 = S_2(119) = 35 = 23$$

$$P(S(B_{1(8)})) = 6D = S_1(109) = 24 = 18$$

$$B = C722\ AE9B\ D913\ 2318$$

$$B' = B \oplus KL_L$$

$$= C722\ AE9B\ D913\ 2318 \oplus 534B\ 5249\ 5053\ 4932$$

$$= 9469\ FCD2\ 8940\ 6A2A$$

$$B' \oplus KL_L = B$$

$$A' \oplus KL_R = A$$

$$\begin{aligned} C &= P(S(B \oplus \Sigma_3)) \\ &= C722 \text{ AE9B D913 2318} \oplus C6EF \text{ 372F E94F 82BE} \\ &= 01CD \text{ 99B4 305C A1A6} \end{aligned}$$

$$P(S(C_{8(8)})) = 01 = S_1(1) = 130 = 82$$

$$P(S(C_{7(8)})) = CD = S_4(205) = 218 = DA$$

$$P(S(C_{6(8)})) = 99 = S_3(153) = 129 = 81$$

$$P(S(C_{5(8)})) = BA = S_2(186) = 222 = DE$$

$$P(S(C_{4(8)})) = 30 = S_4(48) = 20 = 14$$

$$P(S(C_{3(8)})) = 5C = S_3(92) = 232 = E8$$

$$P(S(C_{2(8)})) = A1 = S_2(161) = 184 = B8$$

$$P(S(C_{1(8)})) = A6 = S_1(166) = 144 = 90$$

$$C = 82DA \text{ 81DE 14E8 B890}$$

$$\begin{aligned} C' &= C \oplus A \\ &= 82DA \text{ 81DE 14E8 B890} \oplus 7BFF \text{ EAB4 054A 4A96} \\ &= F925 \text{ 6B6A 11A2 F206} \end{aligned}$$

$$\begin{aligned} D &= P(S(C' \oplus \Sigma_4)) \\ &= F925 \text{ 6B6A 11A2 F206} \oplus 54FF \text{ 53A5 F1D3 6F1C} \\ &= ADDA \text{ 38CF E071 9D1A} \end{aligned}$$

$$P(S(D_{8(8)})) = AD = S_1(173) = 127 = 75$$

$$P(S(D_{7(8)})) = DA = S_4(218) = 55 = 37$$

$$P(S(D_{6(8)})) = 38 = S_3(56) = 236 = EC$$

$$P(S(D_{5(8)})) = CF = S_2(207) = 44 = 2C$$

$$P(S(D_{4(8)})) = E0 = S_4(224) = 121 = 79$$

$$P(S(D_{3(8)})) = 71 = S_3(113) = 34 = 22$$

$$P(S(D_{2(8)})) = 9D = S_2(157) = 126 = 7E$$

$$P(S(D_{1(8)})) = 1A = S_1(26) = 79 = 4F$$

$$D = 7537 \text{ EC2C } 7922 \text{ 7E4F}$$

$$D' = D \oplus B$$

$$= 7537 \text{ EC2C } 7922 \text{ 7E4F} \oplus C722 \text{ AE9B } D913 \text{ 2318}$$

$$= C722 \text{ AE9B } D913 \text{ 2318}$$

$$K_A = D' \parallel C'$$

$$= F925 \text{ 6B6A } 11A2 \text{ F206 } C722 \text{ AE9B } D913 \text{ 2318}$$

Berdasarkan tabel 2.2 subkunci untuk kunci 128 bit, maka didapatkan 24 subkunci yang akan digunakan untuk proses enkripsi dan dekripsi, yaitu:

$$K_{W1(64)} = (KL \lll 0)_{L(64)} = 534B \text{ 5249 } 5053 \text{ 4932}$$

$$K_{W2(64)} = (KL \lll 0)_{R(64)} = 3032 \text{ 3448 } 5553 \text{ 4E49}$$

$$k_{1(64)} = (KA \lll 0)_{L(64)} = F925 \text{ 6B6A } 11A2 \text{ F206}$$

$$k_{2(64)} = (KA \lll 0)_{R(64)} = C722 \text{ AE9B } D913 \text{ 2318}$$

$$k_{3(64)} = (KL \lll 15)_{L(64)} = A924 \text{ A829 } A499 \text{ 29A5}$$

$$k_{4(64)} = (KL \lll 15)_{R(64)} = 1A24 \text{ 2AA9 } A724 \text{ 9819}$$

$$k_{5(64)} = (KA \lll 15)_{L(64)} = B5B5 \text{ 08D1 } 7903 \text{ 7C92}$$

$$k_{6(64)} = (KA \lll 15)_{R(64)} = 574D \text{ EC89 } 918C \text{ 6391}$$

$$kl_{1(64)} = (KA \lll 30)_{L(64)} = 8468 \text{ BC81 } BE49 \text{ 5ADA}$$

$$kl_{2(64)} = (KA \lll 30)_{R(64)} = F644 \text{ C8C6 } 31C8 \text{ ABA6}$$

$$k_{7(64)} = (KL \lll 45)_{L(64)} = 6926 \text{ 4A69 } 6A49 \text{ 2A0A}$$

$$k_{8(64)} = (KL \lll 45)_{R(64)} = 69C9 \text{ 2606 } 4689 \text{ 0AAA}$$

$$\begin{aligned}
k_{9(64)} &= (KA<<<45)_{L(64)} = 5E40\ DF24\ AD6D\ 4234 \\
k_{10(64)} &= (KL<<<60)_{R(64)} = 9303\ 2344\ 8555\ 34E4 \\
k_{11(64)} &= (KA<<<60)_{L(64)} = 6F92\ 56B6\ A11A\ 2F20 \\
k_{12(64)} &= (KA<<<60)_{R(64)} = 8C72\ 2AE9\ BD91\ 3231 \\
k_{13(64)} &= (KL<<<77)_{L(64)} = 6A49\ 2A0A\ 6926\ 4A69 \\
k_{14(64)} &= (KL<<<77)_{R(64)} = 4689\ 0AAA\ 69C9\ 2606 \\
K_{13(64)} &= (KL<<<94)_{L(64)} = 5414\ D24C\ 94D2\ D492 \\
K_{14(64)} &= (KL<<<94)_{R(64)} = 1554\ D392\ 4C0C\ 8D12 \\
K_{15(64)} &= (KA<<<94)_{L(64)} = 8468\ BC81\ BE49\ 5ADA \\
k_{16(64)} &= (KA<<<94)_{R(64)} = F644\ C8C6\ 31C8\ ABA6 \\
k_{17(64)} &= (KL<<<111)_{L(64)} = A499\ 29A5\ A924\ A829 \\
k_{18(64)} &= (KL<<<111)_{R(64)} = A724\ 9819\ 1A24\ 2AA9 \\
Kw_{3(64)} &= (KA<<<111)_{L(64)} = 7903\ 7C92\ B5B5\ 08D1 \\
Kw_{4(64)} &= (KA<<<111)_{R(64)} = 918C\ 6391\ 574D\ EC89
\end{aligned}$$

2. Proses Enkripsi Algoritma Camellia

Sample *plaintext* = Laporan Keuangan

$$M_{(128)} = 4C61\ 706F\ 7261\ 6E20\ 4B65\ 7561\ 6E67\ 616E$$

$$M_{L(64)} = 4C61\ 706F\ 7261\ 6E20$$

$$M_{R(64)} = 4B65\ 7561\ 6E67\ 616E$$

$$\begin{aligned}
L_0 &= M_{L(64)} \oplus Kw_1 \\
&= 4C61\ 706F\ 7261\ 6E20 \oplus 534B\ 5249\ 5053\ 4932 \\
&= 1F2A\ 2226\ 2232\ 2712
\end{aligned}$$

$$\begin{aligned}
R_0 &= M_{R(64)} \oplus Kw_2 \\
&= 4B65\ 7561\ 6E67\ 616E \oplus 3032\ 3448\ 5553\ 4E49
\end{aligned}$$

$$= 7B57\ 4129\ 3B34\ 2F27$$

a. Round $\rightarrow 1$

$$L_1 = R_0 \oplus F(L_0, k_1)$$

$$R_1 = L_0$$

$$L_1 = R_0 \oplus F(L_0, k_1)$$

$$= 7B57\ 4129\ 3B34\ 2F27 \oplus F(L_0, k_1)$$

$$R_1 = 1F2A\ 2226\ 2232\ 2712$$

$$k_1 = F925\ 6B6A\ 11A2\ F206$$

$$(X_{(64)}, k_{(64)}) \rightarrow Y_{(64)} = (P(S(X_{(64)}, k_{(64)})))$$

$$(P(S(X_{8(64)}, k_{(64)}))) = 1F \oplus F9 = E6 = P(S_1(230)) = Y(172)$$

$$(P(S(X_{7(64)}, k_{(64)}))) = 2A \oplus 25 = 0F = P(S_4(15)) = Y(146)$$

$$(P(S(X_{6(64)}, k_{(64)}))) = 22 \oplus 6B = 49 = P(S_3(73)) = Y(9)$$

$$(P(S(X_{5(64)}, k_{(64)}))) = 26 \oplus 6A = 4C = P(S_2(76)) = Y(225)$$

$$(P(S(X_{4(64)}, k_{(64)}))) = 22 \oplus 11 = 33 = P(S_4(51)) = Y(17)$$

$$(P(S(X_{3(64)}, k_{(64)}))) = 32 \oplus A2 = 90 = P(S_3(144)) = Y(8)$$

$$(P(S(X_{2(64)}, k_{(64)}))) = 27 \oplus F2 = D5 = P(S_2(213)) = Y(140)$$

$$(P(S(X_{1(64)}, k_{(64)}))) = 12 \oplus 06 = 14 = P(S_1(20)) = Y(69)$$

$$z'_1 = z1 \oplus z3 \oplus z4 \oplus z6 \oplus z7 \oplus z8 = 69 \oplus 8 \oplus 17 \oplus 9 \oplus 146 \oplus 172 = 107$$

$$z'_2 = z1 \oplus z2 \oplus z4 \oplus z5 \oplus z7 \oplus z8 = 69 \oplus 140 \oplus 17 \oplus 225 \oplus 146 \oplus 172 = 7$$

$$z'_3 = z1 \oplus z2 \oplus z3 \oplus z5 \oplus z6 \oplus z8 = 69 \oplus 140 \oplus 8 \oplus 225 \oplus 9 \oplus 172 = 133$$

$$z'_4 = z2 \oplus z3 \oplus z4 \oplus z5 \oplus z6 \oplus z7 = 140 \oplus 8 \oplus 17 \oplus 225 \oplus 9 \oplus 146 = 239$$

$$z'_5 = z1 \oplus z2 \oplus z6 \oplus z7 \oplus z8 = 69 \oplus 140 \oplus 9 \oplus 146 \oplus 172 = 254$$

$$z'_6 = z2 \oplus z3 \oplus z5 \oplus z7 \oplus z8 = 140 \oplus 8 \oplus 225 \oplus 146 \oplus 172 = 91$$

$$z'_7 = z3 \oplus z4 \oplus z5 \oplus z6 \oplus z8 = 8 \oplus 17 \oplus 225 \oplus 9 \oplus 172 = 93$$

$$z'_8 = z1 \oplus z4 \oplus z5 \oplus z6 \oplus z7 = 69 \oplus 17 \oplus 225 \oplus 9 \oplus 146 = 46$$

$$z'_{(64)} = 6B07\ 85EF\ FE5B\ 5D2E$$

$$\begin{aligned} L_1 &= R_0 \oplus F(L_0, k_1) \\ &= 7B57\ 4129\ 3B34\ 2F27 \oplus 6B07\ 85EF\ FE5B\ 5D2E \\ &= 1050\ C4C6\ C56F\ 7209 \end{aligned}$$

$$R_1 = 1F2A\ 2226\ 2232\ 2712$$

b. Round $\rightarrow 2$

$$L_2 = R_1 \oplus F(L_1, k_2)$$

$$R_2 = L_1$$

$$\begin{aligned} L_2 &= R_1 \oplus F(L_1, k_2) \\ &= 1F2A\ 2226\ 2232\ 2712 \oplus F(L_1, k_2) \end{aligned}$$

$$R_2 = 1050\ C4C6\ C56F\ 7209$$

$$k_2 = C722\ AE9B\ D913\ 2318$$

$$(X_{(64)}, k_{(64)}) \rightarrow Y_{(64)} = (P(S(X_{(64)}, k_{(64)}))$$

$$(P(S(X_{8(64)}, k_{(64)}))) = 10 \oplus C7 = D7 = P(S_1(215)) = Y(186)$$

$$(P(S(X_{7(64)}, k_{(64)}))) = 50 \oplus 22 = 72 = P(S_4(114)) = Y(248)$$

$$(P(S(X_{6(64)}, k_{(64)}))) = C4 \oplus AE = 6A = P(S_3(106)) = Y(78)$$

$$(P(S(X_{5(64)}, k_{(64)}))) = C6 \oplus 9B = 5D = P(S_2(93)) = Y(46)$$

$$(P(S(X_{4(64)}, k_{(64)}))) = C5 \oplus D9 = 1C = P(S_4(28)) = Y(217)$$

$$(P(S(X_{3(64)}, k_{(64)}))) = 6F \oplus 13 = 7C = P(S_3(124)) = Y(48)$$

$$(P(S(X_{2(64)}, k_{(64)}))) = 72 \oplus 23 = 51 = P(S_2(81)) = Y(176)$$

$$(P(S(X_{1(64)}, k_{(64)}))) = 09 \oplus 18 = 11 = P(S_1(17)) = Y(239)$$

$$z'_1 = z1 \oplus z3 \oplus z4 \oplus z6 \oplus z7 \oplus z8 = 239 \oplus 48 \oplus 217 \oplus 78 \oplus 248 \oplus 186 = 10$$

$$z'_2 = z1 \oplus z2 \oplus z4 \oplus z5 \oplus z7 \oplus z8 = 239 \oplus 176 \oplus 217 \oplus 46 \oplus 248 \oplus 186 = 234$$

$$z'_3 = z1 \oplus z2 \oplus z3 \oplus z5 \oplus z6 \oplus z8 = 239 \oplus 176 \oplus 48 \oplus 46 \oplus 78 \oplus 186 = 181$$

$$z'_4 = z2 \oplus z3 \oplus z4 \oplus z5 \oplus z6 \oplus z7 = 176 \oplus 48 \oplus 217 \oplus 46 \oplus 78 \oplus 248 = 193$$

$$z'_5 = z1 \oplus z2 \oplus z6 \oplus z7 \oplus z8 = 239 \oplus 176 \oplus 78 \oplus 248 \oplus 186 = 83$$

$$z'_6 = z2 \oplus z3 \oplus z5 \oplus z7 \oplus z8 = 176 \oplus 48 \oplus 46 \oplus 248 \oplus 186 = 236$$

$$z'_7 = z3 \oplus z4 \oplus z5 \oplus z6 \oplus z8 = 48 \oplus 217 \oplus 46 \oplus 78 \oplus 186 = 51$$

$$z'_8 = z1 \oplus z4 \oplus z5 \oplus z6 \oplus z7 = 239 \oplus 217 \oplus 46 \oplus 78 \oplus 248 = 174$$

$$z'_{(64)} = 0AEA\ B5C1\ 53EC\ 33AE$$

$$L_2 = R_1 \oplus F(L_1, k_2)$$

$$= 1F2A\ 2226\ 2232\ 2712 \oplus 0AEA\ B5C1\ 53EC\ 33AE$$

$$= 15C0\ 97E7\ 71DE\ 14BC$$

$$R_2 = 1050\ C4C6\ C56F\ 7209$$

c. Round $\rightarrow 3$

$$L_3 = R_2 \oplus F(L_2, k_3)$$

$$R_3 = L_2$$

$$L_3 = R_2 \oplus F(L_2, k_3)$$

$$= 1050\ C4C6\ C56F\ 7209 \oplus F(L_2, k_3)$$

$$R_3 = 15C0\ 97E7\ 71DE\ 14BC$$

$$k_3 = A924\ A829\ A499\ 29A5$$

$$(X_{(64)}, k_{(64)}) \rightarrow Y_{(64)} = (P(S(X_{(64)}, k_{(64)}))$$

$$(P(S(X_{8(64)}, k_{(64)}))) = 15 \oplus A9 = BC = P(S_1(188)) = Y(19)$$

$$(P(S(X_{7(64)}, k_{(64)}))) = C0 \oplus 24 = E4 = P(S_4(228)) = Y(245)$$

$$(P(S(X_{6(64)}, k_{(64)}))) = 97 \oplus A8 = 3F = P(S_3(63)) = Y(166)$$

$$(P(S(X_{5(64)}, k_{(64)}))) = E7 \oplus 29 = CE = P(S_2(206)) = Y(105)$$

$$(P(S(X_{4(64)}, k_{(64)}))) = 71 \oplus A4 = D5 = P(S_4(213)) = Y(185)$$

$$(P(S(X_{3(64)}, k_{(64)}))) = DE \oplus 99 = 47 = P(S_3(71)) = Y (150)$$

$$(P(S(X_{2(64)}, k_{(64)}))) = 14 \oplus 29 = 3D = P(S_2(61)) = Y (172)$$

$$(P(S(X_{1(64)}, k_{(64)}))) = BC \oplus A5 = 19 = P(S_1(25)) = Y (14)$$

$$z'_1 = z1 \oplus z3 \oplus z4 \oplus z6 \oplus z7 \oplus z8 = 14 \oplus 150 \oplus 185 \oplus 166 \oplus 145 \oplus 19 = 05$$

$$z'_2 = z1 \oplus z2 \oplus z4 \oplus z5 \oplus z7 \oplus z8 = 14 \oplus 172 \oplus 185 \oplus 105 \oplus 245 \oplus 19 = 148$$

$$z'_3 = z1 \oplus z2 \oplus z3 \oplus z5 \oplus z6 \oplus z8 = 14 \oplus 172 \oplus 150 \oplus 105 \oplus 166 \oplus 19 = 232$$

$$z'_4 = z2 \oplus z3 \oplus z4 \oplus z5 \oplus z6 \oplus z7 = 172 \oplus 150 \oplus 185 \oplus 105 \oplus 166 \oplus 245 = 185$$

$$z'_5 = z1 \oplus z2 \oplus z6 \oplus z7 \oplus z8 = 14 \oplus 172 \oplus 166 \oplus 245 \oplus 19 = 226$$

$$z'_6 = z2 \oplus z3 \oplus z5 \oplus z7 \oplus z8 = 172 \oplus 150 \oplus 105 \oplus 245 \oplus 19 = 181$$

$$z'_7 = z3 \oplus z4 \oplus z5 \oplus z6 \oplus z8 = 150 \oplus 185 \oplus 105 \oplus 166 \oplus 245 = 21$$

$$z'_8 = z1 \oplus z4 \oplus z5 \oplus z6 \oplus z7 = 14 \oplus 185 \oplus 105 \oplus 166 \oplus 245 = 141$$

$$Z'_{(64)} = 0594 \text{ E8B9 E2B5 158D}$$

$$L_3 = R_2 \oplus F(L_2, k_3)$$

$$= 1050 \text{ C4C6 C56F 7209} \oplus 0594 \text{ E8B9 E2B5 158D}$$

$$= 15C4 \text{ 2C7F 27DA 6784}$$

$$R_3 = 15C0 \text{ 97E7 71DE 14BC}$$

d. Round $\rightarrow 4$

$$L_4 = R_3 \oplus F(L_3, k_4)$$

$$R_4 = L_3$$

$$L_4 = R_3 \oplus F(L_3, k_4)$$

$$= 15C0 \text{ 97E7 71DE 14BC} \oplus F(L_3, k_4)$$

$$R_4 = 15C4 \text{ 2C7F 27DA 6784}$$

$$k_4 = 1A24 \text{ 2AA9 A724 9819}$$

$$(X_{(64)}, k_{(64)}) \rightarrow Y_{(64)} = (P(S(X_{(64)}, k_{(64)})))$$

$$(P(S(X_{8(64)}, k_{(64)}))) = 15 \oplus 1A = 0F = P(S_1(15)) = Y(65)$$

$$(P(S(X_{7(64)}, k_{(64)}))) = C4 \oplus 24 = E0 = P(S_4(224)) = Y(121)$$

$$(P(S(X_{6(64)}, k_{(64)}))) = C7 \oplus 2A = 06 = P(S_3(6)) = Y(96)$$

$$(P(S(X_{5(64)}, k_{(64)}))) = F2 \oplus 29 = D6 = P(S_2(214)) = Y(226)$$

$$(P(S(X_{4(64)}, k_{(64)}))) = 27 \oplus A7 = 80 = P(S_4(128)) = Y(130)$$

$$(P(S(X_{3(64)}, k_{(64)}))) = DA \oplus 24 = FE = P(S_3(254)) = Y(64)$$

$$(P(S(X_{2(64)}, k_{(64)}))) = 67 \oplus 98 = FF = P(S_2(255)) = Y(61)$$

$$(P(S(X_{1(64)}, k_{(64)}))) = 84 \oplus 19 = 9D = P(S_1(157)) = Y(63)$$

$$z'_1 = z1 \oplus z3 \oplus z4 \oplus z6 \oplus z7 \oplus z8 = 63 \oplus 64 \oplus 130 \oplus 96 \oplus 121 \oplus 65 = 165$$

$$z'_2 = z1 \oplus z2 \oplus z4 \oplus z5 \oplus z7 \oplus z8 = 63 \oplus 61 \oplus 130 \oplus 226 \oplus 121 \oplus 65 = 90$$

$$z'_3 = z1 \oplus z2 \oplus z3 \oplus z5 \oplus z6 \oplus z8 = 63 \oplus 61 \oplus 64 \oplus 226 \oplus 96 \oplus 65 = 129$$

$$z'_4 = z2 \oplus z3 \oplus z4 \oplus z5 \oplus z6 \oplus z7 = 61 \oplus 64 \oplus 130 \oplus 226 \oplus 96 \oplus 121 = 04$$

$$z'_5 = z1 \oplus z2 \oplus z6 \oplus z7 \oplus z8 = 63 \oplus 61 \oplus 96 \oplus 121 \oplus 65 = 90$$

$$z'_6 = z2 \oplus z3 \oplus z5 \oplus z7 \oplus z8 = 61 \oplus 64 \oplus 226 \oplus 121 \oplus 65 = 167$$

$$z'_7 = z3 \oplus z4 \oplus z5 \oplus z6 \oplus z8 = 64 \oplus 130 \oplus 226 \oplus 96 \oplus 65 = 01$$

$$z'_8 = z1 \oplus z4 \oplus z5 \oplus z6 \oplus z7 = 63 \oplus 130 \oplus 226 \oplus 96 \oplus 121 = 70$$

$$z'_{(64)} = A55A\ 8104\ 5AA7\ 0146$$

$$L_4 = R_3 \oplus F(L_3, k_4)$$

$$= 15C0\ 97E7\ 71DE\ 14BC \oplus A55A\ 8104\ 5AA7\ 0146$$

$$= B09A\ 16E3\ 2B79\ 15FA$$

$$R_4 = 15C4\ 2C7F\ 27DA\ 6784$$

e. Round $\rightarrow$ 5

$$L_5 = R_4 \oplus F(L_4, k_5)$$

$$R_5 = L_4$$

$$L_5 = R_4 \oplus F(L_4, k_5)$$

$$= 15C4\ 2C7F\ 27DA\ 6784 \oplus F(L_4, k_5)$$

$$R_5 = B09A\ 16E3\ 2B79\ 15FA$$

$$k_5 = B5B5\ 08D1\ 7903\ 7C92$$

$$(X_{(64)}, k_{(64)}) \rightarrow Y_{(64)} = (P(S(X_{(64)}, k_{(64)})))$$

$$(P(S(X_{8(64)}, k_{(64)}))) = B0 \oplus B5 = 05 = P(S_1(5)) = Y(39)$$

$$(P(S(X_{7(64)}, k_{(64)}))) = 9A \oplus B5 = 2F = P(S_4(47)) = Y(4)$$

$$(P(S(X_{6(64)}, k_{(64)}))) = 16 \oplus 08 = 1E = P(S_3(30)) = Y(73)$$

$$(P(S(X_{5(64)}, k_{(64)}))) = E3 \oplus D1 = 32 = P(S_2(50)) = Y(114)$$

$$(P(S(X_{4(64)}, k_{(64)}))) = 2B \oplus 79 = 52 = P(S_4(82)) = Y(205)$$

$$(P(S(X_{3(64)}, k_{(64)}))) = 79 \oplus 03 = 7A = P(S_3(122)) = Y(116)$$

$$(P(S(X_{2(64)}, k_{(64)}))) = 15 \oplus 7C = 69 = P(S_2(105)) = Y(30)$$

$$(P(S(X_{1(64)}, k_{(64)}))) = FA \oplus 92 = 68 = P(S_1(104)) = Y(50)$$

$$z'_1 = z1 \oplus z3 \oplus z4 \oplus z6 \oplus z7 \oplus z8 = 50 \oplus 116 \oplus 205 \oplus 73 \oplus 4 \oplus 39 = 225$$

$$z'_2 = z1 \oplus z2 \oplus z4 \oplus z5 \oplus z7 \oplus z8 = 50 \oplus 30 \oplus 205 \oplus 114 \oplus 4 \oplus 39 = 176$$

$$z'_3 = z1 \oplus z2 \oplus z3 \oplus z5 \oplus z6 \oplus z8 = 50 \oplus 30 \oplus 116 \oplus 114 \oplus 73 \oplus 39 = 68$$

$$z'_4 = z2 \oplus z3 \oplus z4 \oplus z5 \oplus z6 \oplus z7 = 30 \oplus 116 \oplus 205 \oplus 114 \oplus 73 \oplus 4 = 152$$

$$z'_5 = z1 \oplus z2 \oplus z6 \oplus z7 \oplus z8 = 50 \oplus 30 \oplus 73 \oplus 4 \oplus 39 = 70$$

$$z'_6 = z2 \oplus z3 \oplus z5 \oplus z7 \oplus z8 = 30 \oplus 116 \oplus 114 \oplus 4 \oplus 39 = 59$$

$$z'_7 = z3 \oplus z4 \oplus z5 \oplus z6 \oplus z8 = 116 \oplus 205 \oplus 114 \oplus 73 \oplus 39 = 165$$

$$z'_8 = z1 \oplus z4 \oplus z5 \oplus z6 \oplus z7 = 50 \oplus 205 \oplus 114 \oplus 73 \oplus 4 = 192$$

$$z'_{(64)} = E1B0\ 4498\ 463B\ A5C0$$

$$L_5 = R_4 \oplus F(L_4, k_5)$$

$$= 15C4\ 2C7F\ 27DA\ 6784 \oplus E1B0\ 4498\ 463B\ A5C0$$

$$= \text{F474 68E7 61E1 C244}$$

$$R_5 = \text{B09A 16E3 2B79 15FA}$$

f. Round $\rightarrow$ 6

$$L'_6 = R_5 \oplus F(L_5, k_6)$$

$$R'_6 = L_5$$

$$L_6 = FL(L'_6, kl_1)$$

$$R_6 = FL^{-1}(R'_6, kl_2)$$

$$L'_6 = R_5 \oplus F(L_5, k_6)$$

$$= \text{B09A 16E3 2B79 15FA} \oplus F(L_5, k_6)$$

$$R'_6 = \text{F474 68E7 61E1 C244}$$

$$k_6 = \text{574D EC89 918C 6391}$$

$$(X_{(64)}, k_{(64)}) \rightarrow Y_{(64)} = (P(S(X_{(64)}, k_{(64)})))$$

$$(P(S(X_{8(64)}, k_{(64)}))) = \text{F4} \oplus 57 = \text{A3} = P(S_1(163)) = Y(2)$$

$$(P(S(X_{7(64)}, k_{(64)}))) = 74 \oplus 4D = 39 = P(S_4(57)) = Y(207)$$

$$(P(S(X_{6(64)}, k_{(64)}))) = 68 \oplus EC = 84 = P(S_3(132)) = Y(208)$$

$$(P(S(X_{5(64)}, k_{(64)}))) = E7 \oplus 89 = 6E = P(S_2(110)) = Y(229)$$

$$(P(S(X_{4(64)}, k_{(64)}))) = 61 \oplus 91 = F0 = P(S_4(240)) = Y(7)$$

$$(P(S(X_{3(64)}, k_{(64)}))) = E1 \oplus 8C = 6D = P(S_3(109)) = Y(12)$$

$$(P(S(X_{2(64)}, k_{(64)}))) = C2 \oplus 63 = A1 = P(S_2(161)) = Y(184)$$

$$(P(S(X_{1(64)}, k_{(64)}))) = 44 \oplus 91 = D5 = P(S_1(213)) = Y(70)$$

$$z'_1 = z1 \oplus z3 \oplus z4 \oplus z6 \oplus z7 \oplus z8 = 70 \oplus 12 \oplus 7 \oplus 208 \oplus 207 \oplus 2 = 80$$

$$z'_2 = z1 \oplus z2 \oplus z4 \oplus z5 \oplus z7 \oplus z8 = 70 \oplus 184 \oplus 7 \oplus 229 \oplus 207 \oplus 2 = 209$$

$$z'_3 = z1 \oplus z2 \oplus z3 \oplus z5 \oplus z6 \oplus z8 = 70 \oplus 184 \oplus 12 \oplus 229 \oplus 208 \oplus 2 = 197$$

$$z'_4 = z2 \oplus z3 \oplus z4 \oplus z5 \oplus z6 \oplus z7 = 184 \oplus 12 \oplus 7 \oplus 229 \oplus 208 \oplus 207 = 73$$

$$z'_5 = z1 \oplus z2 \oplus z6 \oplus z7 \oplus z8 = 70 \oplus 184 \oplus 208 \oplus 207 \oplus 2 = 227$$

$$z'_6 = z2 \oplus z3 \oplus z5 \oplus z7 \oplus z8 = 184 \oplus 12 \oplus 229 \oplus 207 \oplus 2 = 156$$

$$z'_7 = z3 \oplus z4 \oplus z5 \oplus z6 \oplus z8 = 12 \oplus 7 \oplus 229 \oplus 208 \oplus 2 = 60$$

$$z'_8 = z1 \oplus z4 \oplus z5 \oplus z6 \oplus z7 = 70 \oplus 7 \oplus 229 \oplus 208 \oplus 207 = 187$$

$$z'_{(64)} = 50D1 \ C549 \ E39C \ 3CBB$$

$$L'_6 = R_5 \oplus F(L_5, k_6)$$

$$= B09A \ 16E3 \ 2B79 \ 15FA \oplus 50D1 \ C549 \ E39C \ 3CBB$$

$$= E04B \ D3AA \ C8E5 \ 2941$$

$$R'_6 = F474 \ 68E7 \ 61E1 \ C244$$

Menerapkan fungsi FL pada L'_6 dengan kl_1 , untuk mendapatkan L_6

Definisi FL:

$$L_6 = FL(L'_6, kl_1)$$

$$\text{Jika input } (X_{L(32)} \parallel X_{R(32)}, kl_{L(32)} \parallel kl_{R(32)}) \rightarrow Y_{L(32)} \parallel Y_{R(32)}$$

Maka:

$$Y_{R(32)} = ((X_{L(32)} \cap kl_{L(32)}) \lll 1) \oplus X_{R(32)}$$

$$Y_{L(32)} = (Y_{R(32)} \cup kl_{R(32)}) \oplus X_{L(32)}$$

$$\text{Output } Y = Y_L \parallel Y_R$$

Ambil nilai:

$$X = L'_6 = E04B \ D3AA \ C8E5 \ 2941 \rightarrow X_L = E04B \ D3AA, X_R = C8E5 \ 2941$$

$$kl_1 = 8468 \ BC81 \ BE49 \ 5ADA \rightarrow kl_{1L} = 8468 \ BC81, kl_{1R} = BE49 \ 5ADA$$

$$Y_{R(32)} = ((X_{L(32)} \cap kl_{L(32)}) \lll 1) \oplus X_{R(32)}$$

$$= ((E04B \ D3AA \cap 8468 \ BC81) \lll 1) \oplus C8E5 \ 2941$$

$$= (8048 \ 9080 \lll 1) \oplus C8E5 \ 2941$$

$$Y_R = 0091 \ 2101 \oplus C8E5 \ 2941 = C874 \ 0840$$

$$Y_{L(32)} = (Y_{R(32)} \cup kl_{R(32)}) \oplus X_{L(32)}$$

$$= (C874\ 0840 \cup BE49\ 5ADA) \oplus E04B\ D3AA$$

$$Y_L = FE7D\ 5ADA \oplus E04B\ D3AA = 1E36\ 8970$$

$$L_6 = FL(L'_6, kl_1) = Y_L \parallel Y_R = 1E36\ 8970 \parallel C874\ 0840$$

$$L_6 = 1E36\ 8970\ C874\ 0840$$

Menerapkan FL^{-1} pada R'_6 dengan kl_2 untuk mendapatkan R_6

$$R_6 = FL^{-1}(R'_6, kl_2)$$

Definisi FL^{-1} :

Jika input $(Y_{L(32)} \parallel Y_{R(32)}, kl_{L(32)} \parallel kl_{R(32)}) \rightarrow X_{L(32)} \parallel X_{R(32)}$:

Maka:

$$X_{L(32)} = (Y_{R(32)} \cup kl_{R(32)}) \oplus Y_{L(32)}$$

$$X_{R(32)} = ((X_{L(32)} \cap kl_{L(32)}) \lll 1) \oplus Y_{R(32)}$$

$$\text{Output } X = X_{L(32)} \parallel X_{R(32)}$$

Ambil nilai:

$$Y = R'_6 = F474\ 68E7\ 61E1\ C244 \rightarrow Y_L = F474\ 68E7, Y_R = 61E1\ C244$$

$$kl_2 = F644\ C8C6\ 31C8\ ABA6 \rightarrow kl_{2L} = F644\ C8C6, kl_{2R} = 31C8\ ABA6$$

$$X_{L(32)} = (Y_{R(32)} \cup kl_{2R(32)}) \oplus Y_{L(32)}$$

$$= (61E1\ C244 \cup 31C8\ ABA6) \oplus F474\ 68E7$$

$$X_L = 71E9\ EBE6 \oplus F474\ 68E7 = 859D\ 8301$$

$$X_{R(32)} = ((X_{L(32)} \cap kl_{2L(32)}) \lll 1) \oplus Y_{R(32)}$$

$$= ((859D\ 8301 \cap F644\ C8C6) \lll 1) \oplus 61E1\ C244$$

$$= (8404\ 8000 \lll 1) \oplus 61E1\ C244$$

$$X_R = 0809\ 0001 \oplus 61E1\ C244 = 69E8\ C245$$

$$R_6 = FL^{-1}(R'_6, kl_2) = X_L \parallel X_R = 859D\ 8301 \parallel 69E8\ C245$$

$$R_6 = 859D\ 8301\ 69E8\ C245$$

Hasil akhir Round 6:

$$L'_6 = E04B\ D3AA\ C8E5\ 2941 \text{ setelah FL: } L_6 = 1E36\ 8970\ C874\ 0840$$

$$R'_6 = F474\ 68E7\ 61E1\ C244 \text{ setelah FL}^{-1}: R_6 = 859D\ 8301\ 69E8\ C245$$

g. Round $\rightarrow 7$

$$L_7 = R_6 \oplus F(L_6, k_7)$$

$$R_7 = L_6$$

$$L_7 = R_6 \oplus F(L_6, k_7)$$

$$= 859D\ 8301\ 69E8\ C245 \oplus F(L_6, k_7)$$

$$R_7 = 1E36\ 8970\ C874\ 0840$$

$$k_7 = 6926\ 4A69\ 6A49\ 2A0A$$

$$(X_{(64)}, k_{(64)}) \rightarrow Y_{(64)} = (P(S(X_{(64)}, k_{(64)})))$$

$$(P(S(X_{8(64)}, k_{(64)}))) = 1E \oplus 69 = 77 = P(S_1(119)) = Y(145)$$

$$(P(S(X_{7(64)}, k_{(64)}))) = 36 \oplus 26 = 10 = P(S_4(16)) = Y(134)$$

$$(P(S(X_{6(64)}, k_{(64)}))) = 89 \oplus 4A = C3 = P(S_3(195)) = Y(70)$$

$$(P(S(X_{5(64)}, k_{(64)}))) = 70 \oplus 69 = 19 = P(S_2(25)) = Y(28)$$

$$(P(S(X_{4(64)}, k_{(64)}))) = C8 \oplus 6A = A2 = P(S_4(162)) = Y(204)$$

$$(P(S(X_{3(64)}, k_{(64)}))) = 74 \oplus 49 = 3D = P(S_3(61)) = Y(43)$$

$$(P(S(X_{2(64)}, k_{(64)}))) = 08 \oplus 2A = 22 = P(S_2(34)) = Y(95)$$

$$(P(S(X_{1(64)}, k_{(64)}))) = 40 \oplus 0A = 4A = P(S_1(74)) = Y(43)$$

$$z'_1 = z1 \oplus z3 \oplus z4 \oplus z6 \oplus z7 \oplus z8 = 43 \oplus 43 \oplus 204 \oplus 70 \oplus 234 \oplus 245 = 149$$

$$z'_2 = z1 \oplus z2 \oplus z4 \oplus z5 \oplus z7 \oplus z8 = 43 \oplus 95 \oplus 204 \oplus 28 \oplus 134 \oplus 145 = 179$$

$$z'_3 = z1 \oplus z2 \oplus z3 \oplus z5 \oplus z6 \oplus z8 = 43 \oplus 95 \oplus 43 \oplus 28 \oplus 70 \oplus 145 = 148$$

$$z'_4 = z2 \oplus z3 \oplus z4 \oplus z5 \oplus z6 \oplus z7 = 92 \oplus 43 \oplus 204 \oplus 28 \oplus 70 \oplus 134 = 103$$

$$z'_5 = z1 \oplus z2 \oplus z6 \oplus z7 \oplus z8 = 43 \oplus 95 \oplus 70 \oplus 134 \oplus 145 = 37$$

$$z'_6 = z2 \oplus z3 \oplus z5 \oplus z7 \oplus z8 = 95 \oplus 43 \oplus 28 \oplus 134 \oplus 145 = 127$$

$$z'_7 = z3 \oplus z4 \oplus z5 \oplus z6 \oplus z8 = 43 \oplus 204 \oplus 28 \oplus 70 \oplus 145 = 44$$

$$z'_8 = z1 \oplus z4 \oplus z5 \oplus z6 \oplus z7 = 43 \oplus 204 \oplus 28 \oplus 70 \oplus 134 = 59$$

$$z'_{(64)} = 95B3\ 9467\ 257F\ 2C3B$$

$$\begin{aligned} L_7 &= R_6 \oplus F(L_6, k_7) \\ &= 859D\ 8301\ 69E8\ C245 \oplus 95B3\ 9467\ 257F\ 2C3B \\ &= 102E\ 1766\ 4C97\ EE7E \end{aligned}$$

$$R_7 = 1E36\ 8970\ C874\ 0840$$

h. Round $\rightarrow 8$

$$L_8 = R_7 \oplus F(L_7, k_8)$$

$$R_8 = L_7$$

$$\begin{aligned} L_8 &= R_7 \oplus F(L_7, k_8) \\ &= 1E36\ 8970\ C874\ 0840 \oplus F(L_7, k_8) \end{aligned}$$

$$R_8 = 102E\ 1766\ 4C97\ EE7E$$

$$k_8 = 69C9\ 2606\ 4689\ 0AAA$$

$$(X_{(64)}, k_{(64)}) \rightarrow Y_{(64)} = (P(S(X_{(64)}, k_{(64)}))$$

$$(P(S(X_{8(64)}, k_{(64)}))) = 10 \oplus 69 = 79 = P(S_1(121)) = Y(8)$$

$$(P(S(X_{7(64)}, k_{(64)}))) = 2E \oplus C9 = E7 = P(S_4(231)) = Y(89)$$

$$(P(S(X_{6(64)}, k_{(64)}))) = 17 \oplus 26 = 31 = P(S_3(49)) = Y(240)$$

$$(P(S(X_{5(64)}, k_{(64)}))) = 66 \oplus 06 = 60 = P(S_2(96)) = Y(40)$$

$$(P(S(X_{4(64)}, k_{(64)}))) = 4C \oplus 46 = 0A = P(S_4(10)) = Y(69)$$

$$(P(S(X_{3(64)}, k_{(64)}))) = 97 \oplus 89 = 1E = P(S_3(30)) = Y(73)$$

$$(P(S(X_{2(64)}, k_{(64)}))) = EE \oplus 0A = E4 = P(S_2(228)) = Y(241)$$

$$(P(S(X_{1(64)}, k_{(64)}))) = 7E \oplus AA = D4 = P(S_1(212)) = Y(231)$$

$$z'_1 = z1 \oplus z3 \oplus z4 \oplus z6 \oplus z7 \oplus z8 = 231 \oplus 73 \oplus 69 \oplus 240 \oplus 89 \oplus 8 = 74$$

$$z'_2 = z1 \oplus z2 \oplus z4 \oplus z5 \oplus z7 \oplus z8 = 231 \oplus 241 \oplus 69 \oplus 40 \oplus 89 \oplus 8 = 42$$

$$z'_3 = z1 \oplus z2 \oplus z3 \oplus z5 \oplus z6 \oplus z8 = 231 \oplus 241 \oplus 73 \oplus 40 \oplus 240 \oplus 8 = 143$$

$$z'_4 = z2 \oplus z3 \oplus z4 \oplus z5 \oplus z6 \oplus z7 = 241 \oplus 73 \oplus 69 \oplus 40 \oplus 240 \oplus 89 = 124$$

$$z'_5 = z1 \oplus z2 \oplus z6 \oplus z7 \oplus z8 = 231 \oplus 241 \oplus 240 \oplus 89 \oplus 8 = 183$$

$$z'_6 = z2 \oplus z3 \oplus z5 \oplus z7 \oplus z8 = 241 \oplus 73 \oplus 40 \oplus 89 \oplus 8 = 193$$

$$z'_7 = z3 \oplus z4 \oplus z5 \oplus z6 \oplus z8 = 73 \oplus 69 \oplus 40 \oplus 240 \oplus 8 = 220$$

$$z'_8 = z1 \oplus z4 \oplus z5 \oplus z6 \oplus z7 = 231 \oplus 69 \oplus 40 \oplus 240 \oplus 89 = 35$$

$$z'_{(64)} = 4A2A\ 8F7C\ B7C1\ DC23$$

$$L_8 = R_7 \oplus F(L_7, k_8)$$

$$= 1E36\ 8970\ C874\ 0840 \oplus 4A2A\ 8F7C\ B7C1\ DC23$$

$$= 541C\ 060C\ 7FB5\ D463$$

$$R_8 = 102E\ 1766\ 4C97\ EE7E$$

i. Round $\rightarrow 9$

$$L_9 = R_8 \oplus F(L_8, k_9)$$

$$R_9 = L_8$$

$$L_9 = R_8 \oplus F(L_8, k_9)$$

$$= 102E\ 1766\ 4C97\ EE7E \oplus F(L_8, k_9)$$

$$R_9 = 541C\ 060C\ 7FB5\ D463$$

$$k_9 = 5E40\ DF24\ AD6D\ 4234$$

$$(X_{(64)}, k_{(64)}) \rightarrow Y_{(64)} = (P(S(X_{(64)}, k_{(64)})))$$

$$(P(S(X_{8(64)}, k_{(64)}))) = 54 \oplus 5E = 0A = P(S_1(10)) = Y(87)$$

$$(P(S(X_{7(64)}, k_{(64)}))) = 1C \oplus 40 = 5C = P(S_4(92)) = Y(129)$$

$$(P(S(X_{6(64)}, k_{(64)}))) = 06 \oplus DF = D9 = P(S_3(217)) = Y(146)$$

$$(P(S(X_{5(64)}, k_{(64)}))) = 0C \oplus 24 = 28 = P(S_2(40)) = Y(124)$$

$$(P(S(X_{4(64)}, k_{(64)}))) = 7F \oplus AD = D2 = P(S_4(210)) = Y(74)$$

$$(P(S(X_{3(64)}, k_{(64)}))) = B5 \oplus 6D = D8 = P(S_3(216)) = Y(106)$$

$$(P(S(X_{2(64)}, k_{(64)}))) = D4 \oplus 42 = 96 = P(S_2(150)) = Y(234)$$

$$(P(S(X_{1(64)}, k_{(64)}))) = 63 \oplus 34 = 57 = P(S_1(87)) = Y(5)$$

$$z'_1 = z1 \oplus z3 \oplus z4 \oplus z6 \oplus z7 \oplus z8 = 5 \oplus 106 \oplus 74 \oplus 146 \oplus 129 \oplus 87 = 97$$

$$z'_2 = z1 \oplus z2 \oplus z4 \oplus z5 \oplus z7 \oplus z8 = 5 \oplus 234 \oplus 74 \oplus 124 \oplus 129 \oplus 87 = 15$$

$$z'_3 = z1 \oplus z2 \oplus z3 \oplus z5 \oplus z6 \oplus z8 = 5 \oplus 234 \oplus 106 \oplus 124 \oplus 146 \oplus 87 = 60$$

$$z'_4 = z2 \oplus z3 \oplus z4 \oplus z5 \oplus z6 \oplus z7 = 234 \oplus 106 \oplus 74 \oplus 124 \oplus 146 \oplus 129 = 165$$

$$z'_5 = z1 \oplus z2 \oplus z6 \oplus z7 \oplus z8 = 5 \oplus 234 \oplus 146 \oplus 129 \oplus 87 = 171$$

$$z'_6 = z2 \oplus z3 \oplus z5 \oplus z7 \oplus z8 = 234 \oplus 106 \oplus 124 \oplus 129 \oplus 87 = 42$$

$$z'_7 = z3 \oplus z4 \oplus z5 \oplus z6 \oplus z8 = 106 \oplus 74 \oplus 124 \oplus 146 \oplus 87 = 153$$

$$z'_8 = z1 \oplus z4 \oplus z5 \oplus z6 \oplus z7 = 5 \oplus 74 \oplus 124 \oplus 146 \oplus 129 = 32$$

$$z'_{(64)} = 610F\ 3CA5\ AB2A\ 9920$$

$$L_9 = R_8 \oplus F(L_8, k_9)$$

$$= 102E\ 1766\ 4C97\ EE7E \oplus 610F\ 3CA5\ AB2A\ 9920$$

$$= 7121\ 2BC3\ E7BD\ 775E$$

$$R_9 = 541C\ 060C\ 7FB5\ D463$$

j. Round $\rightarrow$ 10

$$L_{10} = R_9 \oplus F(L_9, k_{10})$$

$$R_{10} = L_9$$

$$L_{10} = R_9 \oplus F(L_9, k_{10})$$

$$= 541C\ 060C\ 7FB5\ D463 \oplus F(L_9, k_{10})$$

$$R_{10} = 7121\ 2BC3\ E7BD\ 775E$$

$$k_{10} = 9303\ 2344\ 8555\ 34E4$$

$$(X_{(64)}, k_{(64)}) \rightarrow Y_{(64)} = (P(S(X_{(64)}, k_{(64)})))$$

$$(P(S(X_{8(64)}, k_{(64)}))) = 71 \oplus 93 = E2 = P(S_1(226)) = Y(185)$$

$$(P(S(X_{7(64)}, k_{(64)}))) = 21 \oplus 03 = 22 = P(S_4(34)) = Y(251)$$

$$(P(S(X_{6(64)}, k_{(64)}))) = 2B \oplus 23 = 08 = P(S_3(8)) = Y(114)$$

$$(P(S(X_{5(64)}, k_{(64)}))) = C3 \oplus 44 = 87 = P(S_2(135)) = Y(47)$$

$$(P(S(X_{4(64)}, k_{(64)}))) = E7 \oplus 85 = 62 = P(S_4(98)) = Y(159)$$

$$(P(S(X_{3(64)}, k_{(64)}))) = BD \oplus 55 = E8 = P(S_3(232)) = Y(27)$$

$$(P(S(X_{2(64)}, k_{(64)}))) = 77 \oplus 34 = 43 = P(S_2(67)) = Y(204)$$

$$(P(S(X_{1(64)}, k_{(64)}))) = 5E \oplus E4 = BA = P(S_1(186)) = Y(111)$$

$$z'_1 = z1 \oplus z3 \oplus z4 \oplus z6 \oplus z7 \oplus z8 = 111 \oplus 27 \oplus 159 \oplus 114 \oplus 251 \oplus 185 = 219$$

$$z'_2 = z1 \oplus z2 \oplus z4 \oplus z5 \oplus z7 \oplus z8 = 111 \oplus 204 \oplus 159 \oplus 47 \oplus 251 \oplus 185 = 81$$

$$z'_3 = z1 \oplus z2 \oplus z3 \oplus z5 \oplus z6 \oplus z8 = 111 \oplus 204 \oplus 27 \oplus 47 \oplus 114 \oplus 185 = 92$$

$$z'_4 = z2 \oplus z3 \oplus z4 \oplus z5 \oplus z6 \oplus z7 = 204 \oplus 27 \oplus 159 \oplus 47 \oplus 114 \oplus 251 = 238$$

$$z'_5 = z1 \oplus z2 \oplus z6 \oplus z7 \oplus z8 = 111 \oplus 204 \oplus 114 \oplus 251 \oplus 185 = 147$$

$$z'_6 = z2 \oplus z3 \oplus z5 \oplus z7 \oplus z8 = 204 \oplus 27 \oplus 47 \oplus 251 \oplus 185 = 186$$

$$z'_7 = z3 \oplus z4 \oplus z5 \oplus z6 \oplus z8 = 27 \oplus 159 \oplus 47 \oplus 114 \oplus 185 = 96$$

$$z'_8 = z1 \oplus z4 \oplus z5 \oplus z6 \oplus z7 = 111 \oplus 159 \oplus 47 \oplus 114 \oplus 251 = 86$$

$$z'_{(64)} = DB51\ 5CEE\ 93BA\ 6056$$

$$L_{10} = R_9 \oplus F(L_9, k_{10})$$

$$= 541C\ 060C\ 7FB5\ D463 \oplus DB51\ 5CEE\ 93BA\ 6056$$

$$= 8F4D\ 5AE2\ EC0F\ B435$$

$$R_{10} = 7121\ 2BC3\ E7BD\ 775E$$

k. Round $\rightarrow$ 11

$$L_{11} = R_{10} \oplus F(L_{10}, k_{11})$$

$$R_{11} = L_{10}$$

$$L_{11} = R_{10} \oplus F(L_{10}, k_{11})$$

$$= 7121\ 2BC3\ E7BD\ 775E \oplus F(L_{10}, k_{11})$$

$$R_{11} = 8F4D\ 5AE2\ EC0F\ B435$$

$$k_{11} = 6F92\ 56B6\ A11A\ 2F20$$

$$(X_{(64)}, k_{(64)}) \rightarrow Y_{(64)} = (P(S(X_{(64)}, k_{(64)})))$$

$$(P(S(X_{8(64)}, k_{(64)}))) = 8F \oplus 6F = E0 = P(S_1(224)) = Y(114)$$

$$(P(S(X_{7(64)}, k_{(64)}))) = 4D \oplus 92 = DF = P(S_4(223)) = Y(46)$$

$$(P(S(X_{6(64)}, k_{(64)}))) = 5A \oplus 56 = 0C = P(S_3(12)) = Y(117)$$

$$(P(S(X_{5(64)}, k_{(64)}))) = E2 \oplus B6 = 54 = P(S_2(84)) = Y(104)$$

$$(P(S(X_{4(64)}, k_{(64)}))) = EC \oplus A1 = 4D = P(S_4(77)) = Y(230)$$

$$(P(S(X_{3(64)}, k_{(64)}))) = 0F \oplus 1A = 15 = P(S_3(21)) = Y(140)$$

$$(P(S(X_{2(64)}, k_{(64)}))) = BA \oplus 2F = 9B = P(S_2(155)) = Y(155)$$

$$(P(S(X_{1(64)}, k_{(64)}))) = 35 \oplus 20 = 15 = P(S_1(21)) = Y(25)$$

$$z'_1 = z1 \oplus z3 \oplus z4 \oplus z6 \oplus z7 \oplus z8 = 25 \oplus 140 \oplus 230 \oplus 117 \oplus 46 \oplus 114 = 90$$

$$z'_2 = z1 \oplus z2 \oplus z4 \oplus z5 \oplus z7 \oplus z8 = 25 \oplus 155 \oplus 230 \oplus 104 \oplus 46 \oplus 114 = 80$$

$$z'_3 = z1 \oplus z2 \oplus z3 \oplus z5 \oplus z6 \oplus z8 = 25 \oplus 155 \oplus 140 \oplus 104 \oplus 117 \oplus 114 = 105$$

$$z'_4 = z2 \oplus z3 \oplus z4 \oplus z5 \oplus z6 \oplus z7 = 155 \oplus 140 \oplus 230 \oplus 104 \oplus 117 \oplus 46 = 194$$

$$z'_5 = z1 \oplus z2 \oplus z6 \oplus z7 \oplus z8 = 25 \oplus 155 \oplus 117 \oplus 46 \oplus 114 = 175$$

$$z'_6 = z2 \oplus z3 \oplus z5 \oplus z7 \oplus z8 = 155 \oplus 140 \oplus 104 \oplus 46 \oplus 114 = 35$$

$$z'_7 = z3 \oplus z4 \oplus z5 \oplus z6 \oplus z8 = 140 \oplus 230 \oplus 104 \oplus 117 \oplus 114 = 5$$

$$z'_8 = z1 \oplus z4 \oplus z5 \oplus z6 \oplus z7 = 25 \oplus 230 \oplus 104 \oplus 117 \oplus 46 = 204$$

$$z'_{(64)} = 5A50\ 69C2\ AF23\ 05CC$$

$$L_{11} = R_{10} \oplus F(L_{10}, k_{11})$$

$$= 7121\ 2BC3\ E7BD\ 775E \oplus 5A50\ 69C2\ AF23\ 05CC$$

$$= 2B71\ 4201\ 489E\ 7292$$

$$R_{11} = 8F4D\ 5AE2\ EC0F\ B435$$

1. Round $\rightarrow$ 12

$$L'_{12} = R_{11} \oplus F(L_{11}, k_{12})$$

$$R'_{12} = L_{11}$$

$$L_{12} = FL(L'_{12}, k_{l_3})$$

$$R_{12} = FL^{-1}(R'_{12}, k_{l_4})$$

$$L'_{12} = R_{11} \oplus F(L_{11}, k_{12})$$

$$= 8F4D\ 5AE2\ EC0F\ B435 \oplus F(L_{11}, k_{12})$$

$$R'_{12} = 2B71\ 4201\ 489E\ 7292$$

$$k_{12} = 8C72\ 2AE9\ BD91\ 3231$$

$$(X_{(64)}, k_{(64)}) \rightarrow Y_{(64)} = (P(S(X_{(64)}, k_{(64)})))$$

$$(P(S(X_{8(64)}, k_{(64)}))) = 2B \oplus 8C = A7 = P(S_1(167)) = Y(144)$$

$$(P(S(X_{7(64)}, k_{(64)}))) = 71 \oplus 72 = 03 = P(S_4(3)) = Y(192)$$

$$(P(S(X_{6(64)}, k_{(64)}))) = 42 \oplus 2A = 68 = P(S_3(104)) = Y(25)$$

$$(P(S(X_{5(64)}, k_{(64)}))) = 01 \oplus E9 = E8 = P(S_2(232)) = Y(108)$$

$$(P(S(X_{4(64)}, k_{(64)}))) = 48 \oplus BD = F5 = P(S_4(245)) = Y(104)$$

$$(P(S(X_{3(64)}, k_{(64)}))) = 9E \oplus 91 = 0F = P(S_3(47)) = Y(13)$$

$$(P(S(X_{2(64)}, k_{(64)}))) = 72 \oplus 32 = 40 = P(S_2(64)) = Y(23)$$

$$(P(S(X_{1(64)}, k_{(64)}))) = 92 \oplus 31 = A3 = P(S_1(163)) = Y(2)$$

$$z'_1 = z1 \oplus z3 \oplus z4 \oplus z6 \oplus z7 \oplus z8 = 2 \oplus 13 \oplus 104 \oplus 25 \oplus 192 \oplus 144 = 46$$

$$z'_2 = z1 \oplus z2 \oplus z4 \oplus z5 \oplus z7 \oplus z8 = 2 \oplus 23 \oplus 104 \oplus 108 \oplus 192 \oplus 144 = 65$$

$$z'_3 = z1 \oplus z2 \oplus z3 \oplus z5 \oplus z6 \oplus z8 = 2 \oplus 23 \oplus 13 \oplus 108 \oplus 25 \oplus 144 = 253$$

$$z'_4 = z2 \oplus z3 \oplus z4 \oplus z5 \oplus z6 \oplus z7 = 23 \oplus 13 \oplus 104 \oplus 108 \oplus 25 \oplus 192 = 199$$

$$z'_5 = z1 \oplus z2 \oplus z6 \oplus z7 \oplus z8 = 2 \oplus 23 \oplus 25 \oplus 192 \oplus 144 = 92$$

$$z'_6 = z2 \oplus z3 \oplus z5 \oplus z7 \oplus z8 = 23 \oplus 13 \oplus 108 \oplus 192 \oplus 144 = 38$$

$$z'_7 = z3 \oplus z4 \oplus z5 \oplus z6 \oplus z8 = 13 \oplus 104 \oplus 108 \oplus 25 \oplus 144 = 128$$

$$z'_8 = z1 \oplus z4 \oplus z5 \oplus z6 \oplus z7 = 2 \oplus 104 \oplus 108 \oplus 25 \oplus 192 = 223$$

$$z'_{(64)} = 2E41 \text{ FDC7 } 5C26 \text{ 80DF}$$

$$L'_{12} = R_{11} \oplus F(L_{11}, k_{12})$$

$$= 8F4D \text{ 5AE2 } EC0F \text{ B435 } \oplus 7DBA \text{ D6ED } D9FA \text{ 1FF9}$$

$$= A10C \text{ A725 } B029 \text{ 34EA}$$

$$R'_{12} = 2B71 \text{ 4201 } 489E \text{ 7292}$$

Menerapkan fungsi FL pada L'_6 dengan kl_1 , untuk mendapatkan L_6

Definisi FL:

$$L_{12} = FL(L'_{12}, kl_3)$$

$$\text{Jika input } (X_{L(32)} \parallel X_{R(32)}, kl_{L(32)} \parallel kl_{R(32)}) \rightarrow Y_{L(32)} \parallel Y_{R(32)}$$

Maka:

$$Y_{R(32)} = ((X_{L(32)} \cap kl_{L(32)}) \lll 1) \oplus X_{R(32)}$$

$$Y_{L(32)} = (Y_{R(32)} \cup kl_{R(32)}) \oplus X_{L(32)}$$

$$\text{Output } Y = Y_L \parallel Y_R$$

Ambil nilai:

$$X = L'_{12} = A10C \text{ A725 } B029 \text{ 34EA} \rightarrow X_L = A10C \text{ A725}, X_R = B029 \text{ 34EA}$$

$$kl_3 = 6A49\ 2A0A\ 6926\ 4A69 \rightarrow kl_{3L} = 6A49\ 2A0A, kl_{3R} = 6926\ 4A69$$

$$\begin{aligned} Y_{R(32)} &= ((X_{L(32)} \cap kl_{L(32)}) \lll 1) \oplus X_{R(32)} \\ &= ((A10C\ A725 \cap 6A49\ 2A0A) \lll 1) \oplus B029\ 34EA \\ &= (2008\ 2200 \lll 1) \oplus B029\ 34EA \end{aligned}$$

$$Y_R = 4010\ 4400 \oplus B029\ 34EA = F039\ 70EA$$

$$\begin{aligned} Y_{L(32)} &= (Y_{R(32)} \cup kl_{R(32)}) \oplus X_{L(32)} \\ &= (F039\ 70EA \cup 6926\ 4A69) \oplus A10C\ A725 \end{aligned}$$

$$Y_L = F93F7AEB \oplus A10C\ A725 = 5833\ DDCE$$

$$L_{12} = FL(L'_6, kl_1) = Y_L \parallel Y_R = 5833\ DDCE \parallel F039\ 70EA$$

$$L_{12} = 5833\ DDCE\ F039\ 70EA$$

Menerapkan FL^{-1} pada R'_6 dengan kl_2 untuk mendapatkan R_6

$$R_{12} = FL^{-1}(R'_{12}, kl_4)$$

Definisi FL^{-1} :

Jika input $(Y_{L(32)} \parallel Y_{R(32)}, kl_{L(32)} \parallel kl_{R(32)}) \rightarrow X_{L(32)} \parallel X_{R(32)}$:

Maka:

$$X_{L(32)} = (Y_{R(32)} \cup kl_{R(32)}) \oplus Y_{L(32)}$$

$$X_{R(32)} = ((X_{L(32)} \cap kl_{L(32)}) \lll 1) \oplus Y_{R(32)}$$

$$\text{Output } X = X_{L(32)} \parallel X_{R(32)}$$

Ambil nilai:

$$Y = R'_{12} = 2B71\ 4201\ 489E\ 7292 \rightarrow Y_L = 2B71\ 4201, Y_R = 489E\ 7292$$

$$kl_4 = 4689\ 0AAA\ 69C9\ 2606 \rightarrow kl_{4L} = 4689\ 0AAA, kl_{4R} = 69C9\ 2606$$

$$\begin{aligned} X_{L(32)} &= (Y_{R(32)} \cup kl_{R(32)}) \oplus Y_{L(32)} \\ &= (489E\ 7292 \cup 69C9\ 2606) \oplus 2B71\ 4201 \end{aligned}$$

$$X_L = 69DF\ 7696 \oplus 2B71\ 4201 = 42AE\ 3497$$

$$\begin{aligned}
X_{R(32)} &= ((X_{L(32)} \cap kl_{L(32)}) \lll 1) \oplus Y_{R(32)} \\
&= ((42AE\ 3497 \cap 4689\ 0AAA) \lll 1) \oplus 489E\ 7292 \\
&= (4288\ 0082 \lll 1) \oplus 489E\ 7292
\end{aligned}$$

$$X_R = 8510\ 0104 \oplus 489E\ 7292 = CD8E\ 7396$$

$$R_{12} = FL^{-1}(R'_{12}, kl_4) = X_L \parallel X_R = 42AE\ 3497 \parallel CD8E\ 7396$$

$$R_{12} = 42AE\ 3497\ CD8E\ 7396$$

Hasil akhir Round 6:

$$L'_{12} = A10C\ A725\ B029\ 34EA \text{ setelah FL: } L_{12} = 5833\ DDCE\ F039\ 70EA$$

$$R'_{12} = 2B71\ 4201\ 489E\ 7292 \text{ setelah FL}^{-1}: R_{12} = 42AE\ 3497\ CD8E\ 7396$$

m. Round $\rightarrow$ 13

$$L_{13} = R_{12} \oplus F(L_{12}, k_{13})$$

$$R_{13} = L_{12}$$

$$\begin{aligned}
L_{13} &= R_{12} \oplus F(L_{12}, k_{13}) \\
&= 42AE\ 3497\ CD8E\ 7396 \oplus F(L_{12}, k_{13})
\end{aligned}$$

$$R_{13} = 5833\ DDCE\ F039\ 70EA$$

$$k_{13} = 5414\ D24C\ 94D2\ D492$$

$$(X_{(64)}, k_{(64)}) \rightarrow Y_{(64)} = (P(S(X_{(64)}, k_{(64)}))$$

$$(P(S(X_{8(64)}, k_{(64)}))) = 58 \oplus 54 = 0C = P(S_1(12)) = Y(234)$$

$$(P(S(X_{7(64)}, k_{(64)}))) = 33 \oplus 14 = 27 = P(S_4(39)) = Y(132)$$

$$(P(S(X_{6(64)}, k_{(64)}))) = DD \oplus D2 = 0F = P(S_3(15)) = Y(160)$$

$$(P(S(X_{5(64)}, k_{(64)}))) = CE \oplus 4C = 82 = P(S_2(130)) = Y(65)$$

$$(P(S(X_{4(64)}, k_{(64)}))) = F0 \oplus 94 = 64 = P(S_4(100)) = Y(41)$$

$$(P(S(X_{3(64)}, k_{(64)}))) = 39 \oplus D2 = EB = P(S_3(235)) = Y(52)$$

$$(P(S(X_{2(64)}, k_{(64)}))) = 70 \oplus D4 = A4 = P(S_2(164)) = Y(155)$$

$$(P(S(X_{1(64)}, k_{(64)}))) = EA \oplus 92 = 78 = P(S_1(120)) = Y(36)$$

$$z'_1 = z1 \oplus z3 \oplus z4 \oplus z6 \oplus z7 \oplus z8 = 36 \oplus 52 \oplus 41 \oplus 160 \oplus 132 \oplus 234 = 247$$

$$z'_2 = z1 \oplus z2 \oplus z4 \oplus z5 \oplus z7 \oplus z8 = 36 \oplus 155 \oplus 41 \oplus 65 \oplus 132 \oplus 234 = 185$$

$$z'_3 = z1 \oplus z2 \oplus z3 \oplus z5 \oplus z6 \oplus z8 = 36 \oplus 155 \oplus 52 \oplus 65 \oplus 160 \oplus 234 = 128$$

$$z'_4 = z2 \oplus z3 \oplus z4 \oplus z5 \oplus z6 \oplus z7 = 155 \oplus 52 \oplus 41 \oplus 65 \oplus 160 \oplus 132 = 227$$

$$z'_5 = z1 \oplus z2 \oplus z6 \oplus z7 \oplus z8 = 36 \oplus 155 \oplus 160 \oplus 132 \oplus 234 = 113$$

$$z'_6 = z2 \oplus z3 \oplus z5 \oplus z7 \oplus z8 = 155 \oplus 52 \oplus 65 \oplus 132 \oplus 234 = 128$$

$$z'_7 = z3 \oplus z4 \oplus z5 \oplus z6 \oplus z8 = 52 \oplus 41 \oplus 65 \oplus 160 \oplus 234 = 22$$

$$z'_8 = z1 \oplus z4 \oplus z5 \oplus z6 \oplus z7 = 36 \oplus 41 \oplus 65 \oplus 160 \oplus 132 = 104$$

$$z'_{(64)} = F7B9\ 80E3\ 7180\ 1668$$

$$L_{13} = R_{12} \oplus F(L_{12}, k_{13})$$

$$= 42AE\ 3497\ CD8E\ 7396 \oplus F7B9\ 80E3\ 7180\ 1668$$

$$= B517\ B474\ BC0E\ 65FE$$

$$R_{13} = 5833\ DDCE\ F039\ 70EA$$

n. Round $\rightarrow$ 14

$$L_{14} = R_{13} \oplus F(L_{13}, k_{14})$$

$$R_{14} = L_{13}$$

$$L_{14} = R_{13} \oplus F(L_{13}, k_{14})$$

$$= 5833\ DDCE\ F039\ 70EA \oplus F(L_{12}, k_{13})$$

$$R_{14} = B517\ B474\ BC0E\ 65FE$$

$$k_{14} = 1554\ D392\ 4C0C\ 8D12$$

$$(X_{(64)}, k_{(64)}) \rightarrow Y_{(64)} = (P(S(X_{(64)}, k_{(64)})))$$

$$(P(S(X_{8(64)}, k_{(64)}))) = B5 \oplus 15 = A0 = P(S_1(160)) = Y(135)$$

$$(P(S(X_{7(64)}, k_{(64)}))) = 17 \oplus 54 = 43 = P(S_4(67)) = Y(98)$$

$$(P(S(X_{6(64)}, k_{(64)}))) = B4 \oplus D3 = 67 = P(S_3(103)) = Y(14)$$

$$(P(S(X_{5(64)}, k_{(64)}))) = 74 \oplus 92 = E6 = P(S_2(230)) = Y(89)$$

$$(P(S(X_{4(64)}, k_{(64)}))) = BC \oplus 4C = F0 = P(S_4(240)) = Y(7)$$

$$(P(S(X_{3(64)}, k_{(64)}))) = 0E \oplus 0C = 02 = P(S_3(2)) = Y(22)$$

$$(P(S(X_{2(64)}, k_{(64)}))) = 65 \oplus 8D = E8 = P(S_2(232)) = Y(108)$$

$$(P(S(X_{1(64)}, k_{(64)}))) = FE \oplus 12 = FC = P(S_1(236)) = Y(60)$$

$$z'_1 = z1 \oplus z3 \oplus z4 \oplus z6 \oplus z7 \oplus z8 = 60 \oplus 22 \oplus 7 \oplus 14 \oplus 98 \oplus 135 = 198$$

$$z'_2 = z1 \oplus z2 \oplus z4 \oplus z5 \oplus z7 \oplus z8 = 60 \oplus 108 \oplus 7 \oplus 89 \oplus 98 \oplus 135 = 235$$

$$z'_3 = z1 \oplus z2 \oplus z3 \oplus z5 \oplus z6 \oplus z8 = 60 \oplus 108 \oplus 22 \oplus 89 \oplus 14 \oplus 135 = 150$$

$$z'_4 = z2 \oplus z3 \oplus z4 \oplus z5 \oplus z6 \oplus z7 = 108 \oplus 22 \oplus 7 \oplus 89 \oplus 14 \oplus 98 = 72$$

$$z'_5 = z1 \oplus z2 \oplus z6 \oplus z7 \oplus z8 = 60 \oplus 108 \oplus 14 \oplus 98 \oplus 135 = 187$$

$$z'_6 = z2 \oplus z3 \oplus z5 \oplus z7 \oplus z8 = 108 \oplus 22 \oplus 89 \oplus 98 \oplus 135 = 198$$

$$z'_7 = z3 \oplus z4 \oplus z5 \oplus z6 \oplus z8 = 22 \oplus 7 \oplus 89 \oplus 14 \oplus 135 = 193$$

$$z'_8 = z1 \oplus z4 \oplus z5 \oplus z6 \oplus z7 = 60 \oplus 7 \oplus 89 \oplus 14 \oplus 98 = 14$$

$$Z'_{(64)} = C6EB\ 9648\ BBC6\ C10E$$

$$L_{14} = R_{13} \oplus F(L_{13}, k_{14})$$

$$= 5833\ DDCE\ F039\ 70EA \oplus C6EB\ 9648\ BBC6\ C10E$$

$$= 9ED8\ 4B86\ 4BFF\ B1E4$$

$$R_{14} = B517\ B474\ BC0E\ 65FE$$

o. Round $\rightarrow$ 15

$$L_{15} = R_{14} \oplus F(L_{14}, k_{15})$$

$$R_{15} = L_{14}$$

$$L_{15} = R_{14} \oplus F(L_{14}, k_{15})$$

$$= B517\ B474\ BC0E\ 65FE \oplus F(L_{14}, k_{15})$$

$$R_{15} = 9ED8\ 4B86\ 4BFF\ B1E4$$

$$k_{15} = 8468\ BC81\ BE49\ 5ADA$$

$$(X_{(64)}, k_{(64)}) \rightarrow Y_{(64)} = (P(S(X_{(64)}, k_{(64)})))$$

$$(P(S(X_{8(64)}, k_{(64)}))) = 9E \oplus 84 = 1A = P(S_1(26)) = Y(79)$$

$$(P(S(X_{7(64)}, k_{(64)}))) = D8 \oplus 68 = B0 = P(S_4(176)) = Y(88)$$

$$(P(S(X_{6(64)}, k_{(64)}))) = 4B \oplus BC = F7 = P(S_3(247)) = Y(224)$$

$$(P(S(X_{5(64)}, k_{(64)}))) = 86 \oplus 81 = 07 = P(S_2(7)) = Y(203)$$

$$(P(S(X_{4(64)}, k_{(64)}))) = 4B \oplus BE = F5 = P(S_4(245)) = Y(104)$$

$$(P(S(X_{3(64)}, k_{(64)}))) = FF \oplus 49 = B6 = P(S_3(182)) = Y(99)$$

$$(P(S(X_{2(64)}, k_{(64)}))) = B1 \oplus 5A = EB = P(S_2(235)) = Y(208)$$

$$(P(S(X_{1(64)}, k_{(64)}))) = E4 \oplus DA = 3E = P(S_1(62)) = Y(108)$$

$$z'_1 = z1 \oplus z3 \oplus z4 \oplus z6 \oplus z7 \oplus z8 = 108 \oplus 99 \oplus 104 \oplus 224 \oplus 88 \oplus 79 = 144$$

$$z'_2 = z1 \oplus z2 \oplus z4 \oplus z5 \oplus z7 \oplus z8 = 108 \oplus 208 \oplus 104 \oplus 203 \oplus 88 \oplus 79 = 8$$

$$z'_3 = z1 \oplus z2 \oplus z3 \oplus z5 \oplus z6 \oplus z8 = 108 \oplus 208 \oplus 99 \oplus 203 \oplus 224 \oplus 79 = 187$$

$$z'_4 = z2 \oplus z3 \oplus z4 \oplus z5 \oplus z6 \oplus z7 = 208 \oplus 99 \oplus 104 \oplus 203 \oplus 224 \oplus 88 = 168$$

$$z'_5 = z1 \oplus z2 \oplus z6 \oplus z7 \oplus z8 = 108 \oplus 208 \oplus 224 \oplus 88 \oplus 79 = 75$$

$$z'_6 = z2 \oplus z3 \oplus z5 \oplus z7 \oplus z8 = 208 \oplus 99 \oplus 203 \oplus 88 \oplus 79 = 111$$

$$z'_7 = z3 \oplus z4 \oplus z5 \oplus z6 \oplus z8 = 99 \oplus 104 \oplus 203 \oplus 224 \oplus 79 = 111$$

$$z'_8 = z1 \oplus z4 \oplus z5 \oplus z6 \oplus z7 = 108 \oplus 104 \oplus 203 \oplus 224 \oplus 88 = 119$$

$$z'_{(64)} = 9008\ BBA8\ 4B6F\ 6F77$$

$$L_{15} = R_{14} \oplus F(L_{14}, k_{15})$$

$$= B517\ B474\ BC0E\ 65FE \oplus 9008\ BBA8\ 4B6F\ 6F77$$

$$= 251F\ 0FDC\ F761\ 0A89$$

$$R_{15} = 9ED8\ 4B86\ 4BFF\ B1E4$$

p. Round $\rightarrow$ 16

$$L_{16} = R_{15} \oplus F(L_{15}, k_{16})$$

$$R_{16} = L_{15}$$

$$L_{16} = R_{15} \oplus F(L_{15}, k_{16})$$

$$= 9ED8\ 4B86\ 4BFF\ B1E4 \oplus F(L_{15}, k_{16})$$

$$R_{16} = 251F\ 0FDC\ F761\ 0A89$$

$$k_{16} = F644\ C8C6\ 31C8\ ABA6$$

$$(X_{(64)}, k_{(64)}) \rightarrow Y_{(64)} = (P(S(X_{(64)}, k_{(64)})))$$

$$(P(S(X_{8(64)}, k_{(64)}))) = 25 \oplus F6 = D3 = P(S_1(211)) = Y(106)$$

$$(P(S(X_{7(64)}, k_{(64)}))) = 1F \oplus 44 = 5B = P(S_4(91)) = Y(198)$$

$$(P(S(X_{6(64)}, k_{(64)}))) = 0F \oplus C8 = C7 = P(S_3(199)) = Y(71)$$

$$(P(S(X_{5(64)}, k_{(64)}))) = DC \oplus C6 = 1A = P(S_2(26)) = Y(158)$$

$$(P(S(X_{4(64)}, k_{(64)}))) = F7 \oplus 31 = C6 = P(S_4(198)) = Y(255)$$

$$(P(S(X_{3(64)}, k_{(64)}))) = 61 \oplus C8 = A9 = P(S_3(169)) = Y(179)$$

$$(P(S(X_{2(64)}, k_{(64)}))) = 0A \oplus AB = A1 = P(S_2(161)) = Y(184)$$

$$(P(S(X_{1(64)}, k_{(64)}))) = 89 \oplus A6 = 2F = P(S_1(47)) = Y(26)$$

$$z'_1 = z1 \oplus z3 \oplus z4 \oplus z6 \oplus z7 \oplus z8 = 26 \oplus 179 \oplus 255 \oplus 71 \oplus 198 \oplus 106 = 189$$

$$z'_2 = z1 \oplus z2 \oplus z4 \oplus z5 \oplus z7 \oplus z8 = 26 \oplus 184 \oplus 255 \oplus 158 \oplus 198 \oplus 106 = 111$$

$$z'_3 = z1 \oplus z2 \oplus z3 \oplus z5 \oplus z6 \oplus z8 = 26 \oplus 184 \oplus 179 \oplus 158 \oplus 71 \oplus 106 = 162$$

$$z'_4 = z2 \oplus z3 \oplus z4 \oplus z5 \oplus z6 \oplus z7 = 184 \oplus 179 \oplus 255 \oplus 158 \oplus 71 \oplus 198 = 235$$

$$z'_5 = z1 \oplus z2 \oplus z6 \oplus z7 \oplus z8 = 26 \oplus 184 \oplus 71 \oplus 198 \oplus 106 = 73$$

$$z'_6 = z2 \oplus z3 \oplus z5 \oplus z7 \oplus z8 = 184 \oplus 179 \oplus 158 \oplus 198 \oplus 106 = 57$$

$$z'_7 = z3 \oplus z4 \oplus z5 \oplus z6 \oplus z8 = 179 \oplus 255 \oplus 158 \oplus 71 \oplus 106 = 255$$

$$z'_8 = z1 \oplus z4 \oplus z5 \oplus z6 \oplus z7 = 26 \oplus 255 \oplus 158 \oplus 71 \oplus 198 = 250$$

$$z'_{(64)} = \text{BD6F A2EB 4939 FFFA}$$

$$L_{16} = R_{15} \oplus F(L_{15}, k_{16})$$

$$= 9\text{ED8 4B86 4BFF B1E4} \oplus \text{BD6F A2EB 4939 FFFA}$$

$$= 23\text{B7 E96D 02C6 4E1E}$$

$$R_{16} = 251\text{F 0FDC F761 0A89}$$

q. Round → 17

$$L_{17} = R_{16} \oplus F(L_{16}, k_{17})$$

$$R_{17} = L_{16}$$

$$L_{17} = R_{16} \oplus F(L_{16}, k_{17})$$

$$= 251\text{F 0FDC F761 0A89} \oplus F(L_{16}, k_{17})$$

$$R_{17} = 23\text{B7 E96D 02C6 4E1E}$$

$$k_{17} = \text{A499 29A5 A924 A829}$$

$$(X_{(64)}, k_{(64)}) \rightarrow Y_{(64)} = (P(S(X_{(64)}, k_{(64)})))$$

$$(P(S(X_{8(64)}, k_{(64)}))) = 23 \oplus \text{A4} = 87 = P(S_1(135)) = Y(151)$$

$$(P(S(X_{7(64)}, k_{(64)}))) = \text{B7} \oplus 99 = 2\text{E} = P(S_4(46)) = Y(209)$$

$$(P(S(X_{6(64)}, k_{(64)}))) = \text{E9} \oplus 29 = \text{C0} = P(S_3(192)) = Y(244)$$

$$(P(S(X_{5(64)}, k_{(64)}))) = 6\text{D} \oplus \text{A5} = \text{C8} = P(S_2(200)) = Y(82)$$

$$(P(S(X_{4(64)}, k_{(64)}))) = 02 \oplus \text{A9} = \text{AB} = P(S_4(171)) = Y(5)$$

$$(P(S(X_{3(64)}, k_{(64)}))) = \text{C6} \oplus 24 = \text{E2} = P(S_3(226)) = Y(220)$$

$$(P(S(X_{2(64)}, k_{(64)}))) = 4\text{E} \oplus \text{A8} = \text{E6} = P(S_2(230)) = Y(89)$$

$$(P(S(X_{1(64)}, k_{(64)}))) = 1\text{E} \oplus 29 = 37 = P(S_1(55)) = Y(61)$$

$$z'_1 = z1 \oplus z3 \oplus z4 \oplus z6 \oplus z7 \oplus z8 = 61 \oplus 220 \oplus 5 \oplus 244 \oplus 209 \oplus 151 = 86$$

$$z'_2 = z1 \oplus z2 \oplus z4 \oplus z5 \oplus z7 \oplus z8 = 61 \oplus 89 \oplus 5 \oplus 82 \oplus 209 \oplus 151 = 25$$

$$z'_3 = z1 \oplus z2 \oplus z3 \oplus z5 \oplus z6 \oplus z8 = 61 \oplus 89 \oplus 220 \oplus 82 \oplus 244 \oplus 151 = 137$$

$$z'_4 = z2 \oplus z3 \oplus z4 \oplus z5 \oplus z6 \oplus z7 = 89 \oplus 220 \oplus 5 \oplus 82 \oplus 244 \oplus 209 = 247$$

$$z'_5 = z1 \oplus z2 \oplus z6 \oplus z7 \oplus z8 = 61 \oplus 89 \oplus 244 \oplus 209 \oplus 151 = 214$$

$$z'_6 = z2 \oplus z3 \oplus z5 \oplus z7 \oplus z8 = 89 \oplus 220 \oplus 82 \oplus 209 \oplus 151 = 145$$

$$z'_7 = z3 \oplus z4 \oplus z5 \oplus z6 \oplus z8 = 220 \oplus 5 \oplus 82 \oplus 244 \oplus 151 = 232$$

$$z'_8 = z1 \oplus z4 \oplus z5 \oplus z6 \oplus z7 = 61 \oplus 5 \oplus 82 \oplus 244 \oplus 209 = 79$$

$$Z'_{(64)} = 5619\ 89F7\ D691\ E84F$$

$$L_{17} = R_{16} \oplus F(L_{16}, k_{17})$$

$$= 251F\ 0FDC\ F761\ 0A89 \oplus 5619\ 89F7\ D691\ E84F$$

$$= 7306\ 862B\ 21F0\ E2C6$$

$$R_{17} = 23B7\ E96D\ 02C6\ 4E1E$$

r. Round $\rightarrow$ 18

$$L_{18} = R_{17} \oplus F(L_{17}, k_{18})$$

$$R_{18} = L_{17}$$

$$L_{18} = R_{17} \oplus F(L_{17}, k_{18})$$

$$= 23B7\ E96D\ 02C6\ 4E1E \oplus F(L_{17}, k_{18})$$

$$R_{18} = 7306\ 862B\ 21F0\ E2C6$$

$$k_{18} = A724\ 9819\ 1A24\ 2AA9$$

$$(X_{(64)}, k_{(64)}) \rightarrow Y_{(64)} = (P(S(X_{(64)}, k_{(64)}))$$

$$(P(S(X_{8(64)}, k_{(64)})) = 73 \oplus A7 = D4 = P(S_1(212)) = Y(231)$$

$$(P(S(X_{7(64)}, k_{(64)})) = 06 \oplus 24 = 22 = P(S_4(34)) = Y(251)$$

$$(P(S(X_{6(64)}, k_{(64)})) = 86 \oplus 98 = 1E = P(S_3(30)) = Y(73)$$

$$(P(S(X_{5(64)}, k_{(64)})) = 2B \oplus 19 = 32 = P(S_2(50)) = Y(53)$$

$$(P(S(X_{4(64)}, k_{(64)})) = 21 \oplus 1A = 3B = P(S_4(59)) = Y(122)$$

$$(P(S(X_{3(64)}, k_{(64)})) = F0 \oplus 24 = D4 = P(S_3(212)) = Y(234)$$

ini adalah dekripsi dengan algoritma Camellia:

Sample ciphertext = 0A05 FAB9 9445 EA17 5518 8BB9 701A A948

$$C_{(128)} = 0A05 \text{ FAB9 } 9445 \text{ EA17 } 5518 \text{ 8BB9 } 701A \text{ A948}$$

$$C_{(128)} \oplus (Kw_{3(64)} \parallel Kw_{4(64)}) = R_{18} \parallel L_{18}$$

$$= 0A05 \text{ FAB9 } 9445 \text{ EA17 } 5518 \text{ 8BB9 } 701A \text{ A948} \oplus (7903 \text{ 7C92 } B5B5 \text{ 08D1 } \parallel 918C \text{ 6391 } 574D \text{ EC89})$$

$$= 7306 \text{ 862B } 21F0 \text{ E2C6 } C494 \text{ E828 } 2757 \text{ 45C1}$$

$$R_{18(64)} = 7306 \text{ 862B } 21F0 \text{ E2C6}$$

$$L_{18(64)} = C494 \text{ E828 } 2757 \text{ 45C1}$$

a. Round $\rightarrow$ 18

$$R_{r-1} = L_r \oplus F(R_r, K_r)$$

$$L_{r-1} = R_r$$

$$R_{17} = L_{18} \oplus F(R_{18}, k_{18})$$

$$L_{17} = R_{18}$$

$$R_{17} = L_{18} \oplus F(R_{18}, k_{18})$$

$$= C494 \text{ E828 } 2757 \text{ 45C1} \oplus F(R_{18}, k_{18})$$

$$L_{17} = 7306 \text{ 862B } 21F0 \text{ E2C6}$$

$$k_{18} = A724 \text{ 9819 } 1A24 \text{ 2AA9}$$

$$(X_{(64)}, k_{(64)}) \rightarrow Y_{(64)} = (P(S(X_{(64)} \oplus k_{(64)})))$$

$$X_{(64)} \oplus k_{(64)} = 7306 \text{ 862B } 21F0 \text{ E2C6} \oplus A724 \text{ 9819 } 1A24 \text{ 2AA9}$$

$$= D422 \text{ 1E32 } 3BD4 \text{ C86F}$$

$$(P(S(X_{8(64)}, k_{(64)}))) = D4 = P(S_1(212)) = Y(231)$$

$$(P(S(X_{7(64)}, k_{(64)}))) = 22 = P(S_4(34)) = Y(251)$$

$$(P(S(X_{6(64)}, k_{(64)}))) = 1E = P(S_3(30)) = Y(73)$$

$$(P(S(X_{5(64)}, k_{(64)}))) = 32 = P(S_2(50)) = Y(53)$$

$$(P(S(X_{4(64)}, k_{(64)}))) = 3B = P(S_4(59)) = Y(122)$$

$$(P(S(X_{3(64)}, k_{(64)}))) = D4 = P(S_3(212)) = Y(234)$$

$$(P(S(X_{2(64)}, k_{(64)}))) = P(S_2(200)) = Y(82)$$

$$(P(S(X_{1(64)}, k_{(64)}))) = 6F = P(S_1(111)) = Y(34)$$

$$z'_1 = z1 \oplus z3 \oplus z4 \oplus z6 \oplus z7 \oplus z8 = 34 \oplus 234 \oplus 122 \oplus 73 \oplus 251 \oplus 231 = 231$$

$$z'_2 = z1 \oplus z2 \oplus z4 \oplus z5 \oplus z7 \oplus z8 = 34 \oplus 82 \oplus 122 \oplus 53 \oplus 251 \oplus 231 = 35$$

$$z'_3 = z1 \oplus z2 \oplus z3 \oplus z5 \oplus z6 \oplus z8 = 34 \oplus 82 \oplus 234 \oplus 53 \oplus 73 \oplus 231 = 1$$

$$z'_4 = z2 \oplus z3 \oplus z4 \oplus z5 \oplus z6 \oplus z7 = 82 \oplus 234 \oplus 122 \oplus 53 \oplus 73 \oplus 251 = 69$$

$$z'_5 = z1 \oplus z2 \oplus z6 \oplus z7 \oplus z8 = 34 \oplus 82 \oplus 73 \oplus 251 \oplus 231 = 37$$

$$z'_6 = z2 \oplus z3 \oplus z5 \oplus z7 \oplus z8 = 82 \oplus 234 \oplus 53 \oplus 251 \oplus 231 = 145$$

$$z'_7 = z3 \oplus z4 \oplus z5 \oplus z6 \oplus z8 = 234 \oplus 122 \oplus 53 \oplus 73 \oplus 231 = 11$$

$$z'_8 = z1 \oplus z4 \oplus z5 \oplus z6 \oplus z7 = 34 \oplus 122 \oplus 53 \oplus 73 \oplus 251 = 223$$

$$z'_{(64)} = E723\ 0145\ 2591\ 0BDF$$

$$R_{17} = L_{18} \oplus F(R_{18}, k_{18})$$

$$= C494\ E828\ 2757\ 45C1 \oplus E723\ 0145\ 2591\ 0BDF$$

$$= 23B7\ E96D\ 02C6\ 4E1E$$

$$L_{17} = 7306\ 862B\ 21F0\ E2C6$$

b. Round $\rightarrow$ 17

$$R_{16} = L_{17} \oplus F(R_{17}, k_{17})$$

$$L_{16} = R_{17}$$

$$R_{16} = L_{17} \oplus F(R_{17}, k_{17})$$

$$= 7306\ 862B\ 21F0\ E2C6 \oplus F(R_{17}, k_{17})$$

$$L_{16} = 23B7\ E96D\ 02C6\ 4E1E$$

$$k_{17} = A499\ 29A5\ A924\ A829$$

$$(X_{(64)}, k_{(64)}) \rightarrow Y_{(64)} = (P(S(X_{(64)} \oplus k_{(64)})))$$

$$\begin{aligned} X_{(64)} \oplus k_{(64)} &= 23B7\ E96D\ 02C6\ 4E1E \oplus A499\ 29A5\ A924\ A829 \\ &= 872E\ C0C8\ ABE2\ E637 \end{aligned}$$

$$(P(S(X_{8(64)}, k_{(64)}))) = 87 = P(S_1(135)) = Y(151)$$

$$(P(S(X_{7(64)}, k_{(64)}))) = 2E = P(S_4(46)) = Y(209)$$

$$(P(S(X_{6(64)}, k_{(64)}))) = C0 = P(S_3(192)) = Y(244)$$

$$(P(S(X_{5(64)}, k_{(64)}))) = C8 = P(S_2(200)) = Y(82)$$

$$(P(S(X_{4(64)}, k_{(64)}))) = AB = P(S_4(171)) = Y(5)$$

$$(P(S(X_{3(64)}, k_{(64)}))) = E2 = P(S_3(226)) = Y(220)$$

$$(P(S(X_{2(64)}, k_{(64)}))) = E6 = P(S_2(230)) = Y(89)$$

$$(P(S(X_{1(64)}, k_{(64)}))) = 37 = P(S_1(55)) = Y(61)$$

$$z'_1 = z1 \oplus z3 \oplus z4 \oplus z6 \oplus z7 \oplus z8 = 61 \oplus 220 \oplus 5 \oplus 244 \oplus 209 \oplus 151 = 86$$

$$z'_2 = z1 \oplus z2 \oplus z4 \oplus z5 \oplus z7 \oplus z8 = 61 \oplus 89 \oplus 5 \oplus 82 \oplus 209 \oplus 151 = 25$$

$$z'_3 = z1 \oplus z2 \oplus z3 \oplus z5 \oplus z6 \oplus z8 = 61 \oplus 89 \oplus 220 \oplus 82 \oplus 244 \oplus 151 = 137$$

$$z'_4 = z2 \oplus z3 \oplus z4 \oplus z5 \oplus z6 \oplus z7 = 89 \oplus 220 \oplus 5 \oplus 82 \oplus 244 \oplus 209 = 247$$

$$z'_5 = z1 \oplus z2 \oplus z6 \oplus z7 \oplus z8 = 61 \oplus 89 \oplus 244 \oplus 209 \oplus 151 = 214$$

$$z'_6 = z2 \oplus z3 \oplus z5 \oplus z7 \oplus z8 = 89 \oplus 220 \oplus 82 \oplus 209 \oplus 151 = 145$$

$$z'_7 = z3 \oplus z4 \oplus z5 \oplus z6 \oplus z8 = 220 \oplus 5 \oplus 82 \oplus 244 \oplus 151 = 232$$

$$z'_8 = z1 \oplus z4 \oplus z5 \oplus z6 \oplus z7 = 61 \oplus 5 \oplus 82 \oplus 244 \oplus 209 = 79$$

$$z'_{(64)} = 5619\ 89F7\ D691\ E84F$$

$$R_{16} = L_{17} \oplus F(R_{17}, k_{17})$$

$$= 7306\ 862B\ 21F0\ E2C6 \oplus 5619\ 89F7\ D691\ E84F$$

$$= 251F\ 0FDC\ F761\ 0A89$$

$$L_{16} = 23B7\ E96D\ 02C6\ 4E1E$$

c. Round $\rightarrow 16$

$$R_{15} = L_{16} \oplus F(R_{16}, k_{16})$$

$$L_{15} = R_{16}$$

$$\begin{aligned} R_{15} &= L_{16} \oplus F(R_{16}, k_{16}) \\ &= 23B7\ E96D\ 02C6\ 4E1E \oplus F(R_{16}, k_{16}) \end{aligned}$$

$$L_{15} = 251F\ 0FDC\ F761\ 0A89$$

$$k_{16} = F644\ C8C6\ 31C8\ ABA6$$

$$(X_{(64)}, k_{(64)}) \rightarrow Y_{(64)} = (P(S(X_{(64)} \oplus k_{(64)})))$$

$$\begin{aligned} X_{(64)} \oplus k_{(64)} &= 251F\ 0FDC\ F761\ 0A89 \oplus F644\ C8C6\ 31C8\ ABA6 \\ &= D35B\ C71A\ C6A9\ A12F \end{aligned}$$

$$(P(S(X_{8(64)}, k_{(64)}))) = D3 = P(S_1(211)) = Y(106)$$

$$(P(S(X_{7(64)}, k_{(64)}))) = 5B = P(S_4(91)) = Y(198)$$

$$(P(S(X_{6(64)}, k_{(64)}))) = C7 = P(S_3(199)) = Y(71)$$

$$(P(S(X_{5(64)}, k_{(64)}))) = 1A = P(S_2(26)) = Y(158)$$

$$(P(S(X_{4(64)}, k_{(64)}))) = C6 = P(S_4(198)) = Y(255)$$

$$(P(S(X_{3(64)}, k_{(64)}))) = P(S_3(169)) = Y(179)$$

$$(P(S(X_{2(64)}, k_{(64)}))) = A1 = P(S_2(161)) = Y(184)$$

$$(P(S(X_{1(64)}, k_{(64)}))) = 2F = P(S_1(47)) = Y(26)$$

$$z'_1 = z1 \oplus z3 \oplus z4 \oplus z6 \oplus z7 \oplus z8 = 26 \oplus 179 \oplus 255 \oplus 71 \oplus 198 \oplus 106 = 189$$

$$z'_2 = z1 \oplus z2 \oplus z4 \oplus z5 \oplus z7 \oplus z8 = 26 \oplus 184 \oplus 255 \oplus 158 \oplus 198 \oplus 106 = 111$$

$$z'_3 = z1 \oplus z2 \oplus z3 \oplus z5 \oplus z6 \oplus z8 = 26 \oplus 184 \oplus 179 \oplus 158 \oplus 71 \oplus 106 = 162$$

$$z'_4 = z2 \oplus z3 \oplus z4 \oplus z5 \oplus z6 \oplus z7 = 184 \oplus 179 \oplus 255 \oplus 158 \oplus 71 \oplus 198 = 235$$

$$z'_5 = z1 \oplus z2 \oplus z6 \oplus z7 \oplus z8 = 26 \oplus 184 \oplus 71 \oplus 198 \oplus 106 = 73$$

$$z'_6 = z2 \oplus z3 \oplus z5 \oplus z7 \oplus z8 = 184 \oplus 179 \oplus 158 \oplus 198 \oplus 106 = 57$$

$$z'_7 = z3 \oplus z4 \oplus z5 \oplus z6 \oplus z8 = 179 \oplus 255 \oplus 158 \oplus 71 \oplus 106 = 255$$

$$z'_8 = z1 \oplus z4 \oplus z5 \oplus z6 \oplus z7 = 26 \oplus 255 \oplus 158 \oplus 71 \oplus 198 = 250$$

$$z'_{(64)} = \text{BD6F A2EB 4939 FFFA}$$

$$\begin{aligned} R_{15} &= L_{16} \oplus F(R_{16}, k_{16}) \\ &= 23B7 E96D 02C6 4E1E \oplus \text{BD6F A2EB 4939 FFFA} \\ &= 9ED8 4B86 4BFF B1E4 \end{aligned}$$

$$L_{15} = 251F 0FDC F761 0A89$$

d. Round $\rightarrow$ 15

$$R_{14} = L_{15} \oplus F(R_{15}, k_{15})$$

$$L_{14} = R_{15}$$

$$\begin{aligned} R_{14} &= L_{15} \oplus F(R_{15}, k_{15}) \\ &= 251F 0FDC F761 0A89 \oplus F(R_{15}, k_{15}) \end{aligned}$$

$$L_{14} = 9ED8 4B86 4BFF B1E4$$

$$k_{15} = 8468 \text{ BC81 BE49 5ADA}$$

$$(X_{(64)}, k_{(64)}) \rightarrow Y_{(64)} = (P(S(X_{(64)} \oplus k_{(64)})))$$

$$\begin{aligned} X_{(64)} \oplus k_{(64)} &= 9ED8 4B86 4BFF B1E4 \oplus 8468 \text{ BC81 BE49 5ADA} \\ &= 1AB0 F707 F5B6 EB3E \end{aligned}$$

$$(P(S(X_{8(64)}, k_{(64)}))) = 1A = P(S_1(26)) = Y(79)$$

$$(P(S(X_{7(64)}, k_{(64)}))) = B0 = P(S_4(176)) = Y(88)$$

$$(P(S(X_{6(64)}, k_{(64)}))) = F7 = P(S_3(247)) = Y(224)$$

$$(P(S(X_{5(64)}, k_{(64)}))) = 07 = P(S_2(7)) = Y(203)$$

$$(P(S(X_{4(64)}, k_{(64)}))) = F5 = P(S_4(245)) = Y(104)$$

$$(P(S(X_{3(64)}, k_{(64)}))) = B6 = P(S_3(182)) = Y(99)$$

$$(P(S(X_{2(64)}, k_{(64)}))) = EB = P(S_2(235)) = Y(208)$$

$$(P(S(X_{1(64)}, k_{(64)}))) = 3E = P(S_1(62)) = Y(108)$$

$$z'_1 = z1 \oplus z3 \oplus z4 \oplus z6 \oplus z7 \oplus z8 = 108 \oplus 99 \oplus 104 \oplus 224 \oplus 88 \oplus 79 = 144$$

$$z'_2 = z1 \oplus z2 \oplus z4 \oplus z5 \oplus z7 \oplus z8 = 108 \oplus 208 \oplus 104 \oplus 203 \oplus 88 \oplus 79 = 8$$

$$z'_3 = z1 \oplus z2 \oplus z3 \oplus z5 \oplus z6 \oplus z8 = 108 \oplus 208 \oplus 99 \oplus 203 \oplus 224 \oplus 79 = 187$$

$$z'_4 = z2 \oplus z3 \oplus z4 \oplus z5 \oplus z6 \oplus z7 = 208 \oplus 99 \oplus 104 \oplus 203 \oplus 224 \oplus 88 = 168$$

$$z'_5 = z1 \oplus z2 \oplus z6 \oplus z7 \oplus z8 = 108 \oplus 208 \oplus 224 \oplus 88 \oplus 79 = 75$$

$$z'_6 = z2 \oplus z3 \oplus z5 \oplus z7 \oplus z8 = 208 \oplus 99 \oplus 203 \oplus 88 \oplus 79 = 111$$

$$z'_7 = z3 \oplus z4 \oplus z5 \oplus z6 \oplus z8 = 99 \oplus 104 \oplus 203 \oplus 224 \oplus 79 = 111$$

$$z'_8 = z1 \oplus z4 \oplus z5 \oplus z6 \oplus z7 = 108 \oplus 104 \oplus 203 \oplus 224 \oplus 88 = 119$$

$$z'_{(64)} = 9008 \text{ BBA8 4B6F 6F77}$$

$$R_{14} = L_{15} \oplus F(R_{15}, k_{15})$$

$$= 251F \text{ 0FDC F761 0A89} \oplus 9008 \text{ BBA8 4B6F 6F77}$$

$$= B517 \text{ B474 BC0E 65FE}$$

$$L_{14} = 9ED8 \text{ 4B86 4BFF B1E4}$$

e. Round $\rightarrow 14$

$$R_{13} = L_{14} \oplus F(R_{14}, k_{14})$$

$$L_{13} = R_{14}$$

$$R_{13} = L_{14} \oplus F(R_{14}, k_{14})$$

$$= 9ED8 \text{ 4B86 4BFF B1E4} \oplus F(R_{14}, k_{14})$$

$$L_{13} = B517 \text{ B474 BC0E 65FE}$$

$$k_{14} = 1554 \text{ D392 4C0C 8D12}$$

$$(X_{(64)}, k_{(64)}) \rightarrow Y_{(64)} = (P(S(X_{(64)} \oplus k_{(64)})))$$

$$X_{(64)} \oplus k_{(64)} = B517 \text{ B474 BC0E 65FE} \oplus 1554 \text{ D392 4C0C 8D12}$$

$$= \text{A043 67E6 F002 E8EC}$$

$$(P(S(X_{8(64)}, k_{(64)}))) = \text{A0} = P(S_1(160)) = Y(135)$$

$$(P(S(X_{7(64)}, k_{(64)}))) = 43 = P(S_4(67)) = Y(98)$$

$$(P(S(X_{6(64)}, k_{(64)}))) = 67 = P(S_3(103)) = Y(14)$$

$$(P(S(X_{5(64)}, k_{(64)}))) = \text{E6} = P(S_2(230)) = Y(89)$$

$$(P(S(X_{4(64)}, k_{(64)}))) = \text{F0} = P(S_4(240)) = Y(7)$$

$$(P(S(X_{3(64)}, k_{(64)}))) = 02 = P(S_3(2)) = Y(22)$$

$$(P(S(X_{2(64)}, k_{(64)}))) = \text{E8} = P(S_2(232)) = Y(108)$$

$$(P(S(X_{1(64)}, k_{(64)}))) = \text{FC} = P(S_1(236)) = Y(60)$$

$$z'_1 = z1 \oplus z3 \oplus z4 \oplus z6 \oplus z7 \oplus z8 = 60 \oplus 22 \oplus 7 \oplus 14 \oplus 98 \oplus 135 = 198$$

$$z'_2 = z1 \oplus z2 \oplus z4 \oplus z5 \oplus z7 \oplus z8 = 60 \oplus 108 \oplus 7 \oplus 89 \oplus 98 \oplus 135 = 235$$

$$z'_3 = z1 \oplus z2 \oplus z3 \oplus z5 \oplus z6 \oplus z8 = 60 \oplus 108 \oplus 22 \oplus 89 \oplus 14 \oplus 135 = 150$$

$$z'_4 = z2 \oplus z3 \oplus z4 \oplus z5 \oplus z6 \oplus z7 = 108 \oplus 22 \oplus 7 \oplus 89 \oplus 14 \oplus 98 = 72$$

$$z'_5 = z1 \oplus z2 \oplus z6 \oplus z7 \oplus z8 = 60 \oplus 108 \oplus 14 \oplus 98 \oplus 135 = 187$$

$$z'_6 = z2 \oplus z3 \oplus z5 \oplus z7 \oplus z8 = 108 \oplus 22 \oplus 89 \oplus 98 \oplus 135 = 198$$

$$z'_7 = z3 \oplus z4 \oplus z5 \oplus z6 \oplus z8 = 22 \oplus 7 \oplus 89 \oplus 14 \oplus 135 = 193$$

$$z'_8 = z1 \oplus z4 \oplus z5 \oplus z6 \oplus z7 = 60 \oplus 7 \oplus 89 \oplus 14 \oplus 98 = 14$$

$$z'_{(64)} = \text{C6EB 9648 BBC6 C10E}$$

$$R_{13} = L_{14} \oplus F(R_{14}, k_{14})$$

$$= \text{9ED8 4B86 4BFF B1E4} \oplus \text{C6EB 9648 BBC6 C10E}$$

$$= \text{5833 DDCE F039 70EA}$$

$$L_{13} = \text{B517 B474 BC0E 65FE}$$

f. Round $\rightarrow$ 13

$$R'_{12} = L_{13} \oplus F(L_{13}, k_{13})$$

$$L'_{12} = R_{13}$$

$$R_{12} = FL(R'_{12}, kl_4)$$

$$L_{12} = FL^{-1}(R'_{12}, kl_3)$$

$$R'_{12} = L_{13} \oplus F(L_{13}, k_{13})$$

$$= B517\ B474\ BC0E\ 65FE \oplus F(L_{13}, k_{13})$$

$$L'_{12} = 5833\ DDCE\ F039\ 70EA$$

$$k_{13} = 5414\ D24C\ 94D2\ D492$$

$$(X_{(64)}, k_{(64)}) \rightarrow Y_{(64)} = (P(S(X_{(64)} \oplus k_{(64)})))$$

$$X_{(64)} \oplus k_{(64)} = 5833\ DDCE\ F039\ 70EA \oplus 5414\ D24C\ 94D2\ D492$$

$$= 0C27\ 0F82\ 64EB\ A478$$

$$(P(S(X_{8(64)}, k_{(64)}))) = 0C = P(S_1(12)) = Y(234)$$

$$(P(S(X_{7(64)}, k_{(64)}))) = 27 = P(S_4(39)) = Y(132)$$

$$(P(S(X_{6(64)}, k_{(64)}))) = 0F = P(S_3(15)) = Y(160)$$

$$(P(S(X_{5(64)}, k_{(64)}))) = 82 = P(S_2(130)) = Y(65)$$

$$(P(S(X_{4(64)}, k_{(64)}))) = 64 = P(S_4(100)) = Y(41)$$

$$(P(S(X_{3(64)}, k_{(64)}))) = EB = P(S_3(235)) = Y(52)$$

$$(P(S(X_{2(64)}, k_{(64)}))) = A4 = P(S_2(164)) = Y(155)$$

$$(P(S(X_{1(64)}, k_{(64)}))) = 78 = P(S_1(120)) = Y(36)$$

$$z'_1 = z1 \oplus z3 \oplus z4 \oplus z6 \oplus z7 \oplus z8 = 36 \oplus 52 \oplus 41 \oplus 160 \oplus 132 \oplus 234 = 247$$

$$z'_2 = z1 \oplus z2 \oplus z4 \oplus z5 \oplus z7 \oplus z8 = 36 \oplus 155 \oplus 41 \oplus 65 \oplus 132 \oplus 234 = 185$$

$$z'_3 = z1 \oplus z2 \oplus z3 \oplus z5 \oplus z6 \oplus z8 = 36 \oplus 155 \oplus 52 \oplus 65 \oplus 160 \oplus 234 = 128$$

$$z'_4 = z2 \oplus z3 \oplus z4 \oplus z5 \oplus z6 \oplus z7 = 155 \oplus 52 \oplus 41 \oplus 65 \oplus 160 \oplus 132 = 227$$

$$z'_5 = z1 \oplus z2 \oplus z6 \oplus z7 \oplus z8 = 36 \oplus 155 \oplus 160 \oplus 132 \oplus 234 = 113$$

$$z'_6 = z2 \oplus z3 \oplus z5 \oplus z7 \oplus z8 = 155 \oplus 52 \oplus 65 \oplus 132 \oplus 234 = 128$$

$$z'_7 = z3 \oplus z4 \oplus z5 \oplus z6 \oplus z8 = 52 \oplus 41 \oplus 65 \oplus 160 \oplus 234 = 22$$

$$z'_8 = z1 \oplus z4 \oplus z5 \oplus z6 \oplus z7 = 36 \oplus 41 \oplus 65 \oplus 160 \oplus 132 = 104$$

$$z'_{(64)} = \text{F7B9 80E3 7180 1668}$$

$$R'_{12} = L_{13} \oplus F(L_{13}, k_{13})$$

$$= \text{B517 B474 BC0E 65FE} \oplus \text{F7B9 80E3 7180 1668}$$

$$= \text{42AE 3497 CD8E 7396}$$

$$L'_{12} = \text{5833 DDCE F039 70EA}$$

Menerapkan fungsi FL pada R'_{12} dengan kl_4 , untuk mendapatkan R_{12}

Definisi FL:

$$R_{12} = \text{FL}(R'_{12}, kl_4)$$

$$\text{Jika input } (X_{L(32)} \parallel X_{R(32)}, kl_{L(32)} \parallel kl_{R(32)}) \rightarrow Y_{L(32)} \parallel Y_{R(32)}$$

Maka:

$$Y_{R(32)} = ((X_{L(32)} \cap kl_{L(32)}) \lll 1) \oplus X_{R(32)}$$

$$Y_{L(32)} = (Y_{R(32)} \cup kl_{R(32)}) \oplus X_{L(32)}$$

$$\text{Output } Y = Y_L \parallel Y_R$$

Ambil nilai:

$$X = R'_{12} = \text{42AE 3497 CD8E 7396} \rightarrow X_L = \text{42AE 3497}, X_R = \text{CD8E 7396}$$

$$kl_4 = \text{4689 0AAA 69C9 2606} \rightarrow kl_{4L} = \text{4689 0AAA}, kl_{4R} = \text{69C9 2606}$$

$$Y_{R(32)} = ((X_{L(32)} \cap kl_{L(32)}) \lll 1) \oplus X_{R(32)}$$

$$= ((\text{42AE 3497} \cap \text{4689 0AAA}) \lll 1) \oplus \text{CD8E 7396}$$

$$= (\text{4288 0082} \lll 1) \oplus \text{CD8E 7396}$$

$$Y_R = \text{8510 0104} \oplus \text{CD8E 7396} = \text{489E 7292}$$

$$Y_{L(32)} = (Y_{R(32)} \cup kl_{R(32)}) \oplus X_{L(32)}$$

$$= (489E\ 7292 \cup 69C9\ 2606) \oplus 42AE\ 3497$$

$$Y_L = 69DF\ 7696 \oplus 42AE\ 3497 = 2B71\ 4201$$

$$R_{12} = FL(R'_{12}, kl_4) = Y_L \parallel Y_R = 2B71\ 4201 \parallel 489E\ 7292$$

$$R_{12} = 2B71\ 4201\ 489E\ 7292$$

Menerapkan FL^{-1} pada L'_{12} dengan kl_3 untuk mendapatkan L_{12}

$$L_{12} = FL^{-1}(L'_{12}, kl_3)$$

Definisi FL^{-1} :

Jika input $(Y_{L(32)} \parallel Y_{R(32)}, kl_{L(32)} \parallel kl_{R(32)}) \rightarrow X_{L(32)} \parallel X_{R(32)}$:

Maka:

$$X_{L(32)} = (Y_{R(32)} \cup kl_{R(32)}) \oplus Y_{L(32)}$$

$$X_{R(32)} = ((X_{L(32)} \cap kl_{L(32)}) \lll 1) \oplus Y_{R(32)}$$

$$\text{Output } X = X_{L(32)} \parallel X_{R(32)}$$

Ambil nilai:

$$Y = L'_{12} = 5833\ DDCE\ F039\ 70EA \rightarrow Y_L = 5833\ DDCE, Y_R = F039\ 70EA$$

$$kl_3 = 6A49\ 2A0A\ 6926\ 4A69 \rightarrow kl_{3L} = 6A49\ 2A0A, kl_{3R} = 6926\ 4A69$$

$$X_{L(32)} = (Y_{R(32)} \cup kl_{R(32)}) \oplus Y_{L(32)}$$

$$= (F039\ 70EA \cup 6926\ 4A69) \oplus 5833\ DDCE$$

$$X_L = F93F\ 7AEB \oplus 5833\ DDCE = A10C\ A725$$

$$X_{R(32)} = ((X_{L(32)} \cap kl_{L(32)}) \lll 1) \oplus Y_{R(32)}$$

$$= ((A10C\ A725 \cap 6A49\ 2A0A) \lll 1) \oplus F039\ 70EA$$

$$= (2008\ 2200 \lll 1) \oplus F039\ 70EA$$

$$X_R = 4010\ 4400 \oplus F039\ 70EA = B029\ 34EA$$

$$L_{12} = FL^{-1}(R'_{12}, kl_3) = X_L \parallel X_R = A10C\ A725 \parallel B029\ 34EA$$

$$L_{12} = A10C A725 B029 34EA$$

Hasil akhir Round 13:

$$R'_{12} = 42AE 3497 CD8E 7396 \text{ setelah } FL^{-1}: R_{12} = 2B71 4201 489E 7292$$

$$L'_{12} = 5833 DDCE F039 70EA \text{ setelah } FL: L_{12} = A10C A725 B029 34EA$$

g. Round $\rightarrow$ 12

$$R_{11} = L_{12} \oplus F(R_{12}, k_{12})$$

$$L_{11} = R_{12}$$

$$R_{11} = L_{12} \oplus F(R_{12}, k_{12})$$

$$= A10C A725 B029 34EA \oplus F(R_{12}, k_{12})$$

$$L_{11} = 2B71 4201 489E 7292$$

$$k_{12} = 8C72 2AE9 BD91 3231$$

$$(X_{(64)}, k_{(64)}) \rightarrow Y_{(64)} = (P(S(X_{(64)} \oplus k_{(64)})))$$

$$X_{(64)} \oplus k_{(64)} = 2B71 4201 489E 7292 \oplus 8C72 2AE9 BD91 3231$$

$$= A703 68E8 F50F 40A3$$

$$(P(S(X_{8(64)}, k_{(64)}))) = A7 = P(S_1(167)) = Y(144)$$

$$(P(S(X_{7(64)}, k_{(64)}))) = 03 = P(S_4(3)) = Y(192)$$

$$(P(S(X_{6(64)}, k_{(64)}))) = 68 = P(S_3(104)) = Y(25)$$

$$(P(S(X_{5(64)}, k_{(64)}))) = E8 = P(S_2(232)) = Y(108)$$

$$(P(S(X_{4(64)}, k_{(64)}))) = F5 = P(S_4(245)) = Y(104)$$

$$(P(S(X_{3(64)}, k_{(64)}))) = 0F = P(S_3(47)) = Y(13)$$

$$(P(S(X_{2(64)}, k_{(64)}))) = 40 = P(S_2(64)) = Y(23)$$

$$(P(S(X_{1(64)}, k_{(64)}))) = A3 = P(S_1(163)) = Y(2)$$

$$z'_1 = z1 \oplus z3 \oplus z4 \oplus z6 \oplus z7 \oplus z8 = 2 \oplus 13 \oplus 104 \oplus 25 \oplus 192 \oplus 144 = 46$$

$$z'_2 = z1 \oplus z2 \oplus z4 \oplus z5 \oplus z7 \oplus z8 = 2 \oplus 23 \oplus 104 \oplus 108 \oplus 192 \oplus 144 = 65$$

$$z'_3 = z1 \oplus z2 \oplus z3 \oplus z5 \oplus z6 \oplus z8 = 2 \oplus 23 \oplus 13 \oplus 108 \oplus 25 \oplus 144 = 253$$

$$z'_4 = z2 \oplus z3 \oplus z4 \oplus z5 \oplus z6 \oplus z7 = 23 \oplus 13 \oplus 104 \oplus 108 \oplus 25 \oplus 192 = 199$$

$$z'_5 = z1 \oplus z2 \oplus z6 \oplus z7 \oplus z8 = 2 \oplus 23 \oplus 25 \oplus 192 \oplus 144 = 92$$

$$z'_6 = z2 \oplus z3 \oplus z5 \oplus z7 \oplus z8 = 23 \oplus 13 \oplus 108 \oplus 192 \oplus 144 = 38$$

$$z'_7 = z3 \oplus z4 \oplus z5 \oplus z6 \oplus z8 = 13 \oplus 104 \oplus 108 \oplus 25 \oplus 144 = 128$$

$$z'_8 = z1 \oplus z4 \oplus z5 \oplus z6 \oplus z7 = 2 \oplus 104 \oplus 108 \oplus 25 \oplus 192 = 223$$

$$z'_{(64)} = 2E41 \text{ FDC7 } 5C26 \text{ 80DF}$$

$$R_{11} = L_{12} \oplus F(R_{12}, k_{12})$$

$$= A10C \text{ A725 } B029 \text{ 34EA } \oplus 2E41 \text{ FDC7 } 5C26 \text{ 80DF}$$

$$= 8F4D \text{ 5AE2 } EC0F \text{ B435}$$

$$L_{11} = 2B71 \text{ 4201 } 489E \text{ 7292}$$

h. Round $\rightarrow$ 11

$$R_{10} = L_{11} \oplus F(R_{11}, k_{11})$$

$$L_{10} = R_{11}$$

$$R_{10} = L_{11} \oplus F(R_{11}, k_{11})$$

$$= 2B71 \text{ 4201 } 489E \text{ 7292 } \oplus F(R_{11}, k_{11})$$

$$L_{10} = 8F4D \text{ 5AE2 } EC0F \text{ B435}$$

$$k_{11} = 6F92 \text{ 56B6 } A11A \text{ 2F20}$$

$$(X_{(64)}, k_{(64)}) \rightarrow Y_{(64)} = (P(S(X_{(64)} \oplus k_{(64)})))$$

$$X_{(64)} \oplus k_{(64)} = 8F4D \text{ 5AE2 } EC0F \text{ B435 } \oplus 6F92 \text{ 56B6 } A11A \text{ 2F20}$$

$$= E0DF \text{ 0C54 } 4D15 \text{ 9B15}$$

$$(P(S(X_{8(64)}, k_{(64)}))) = E0 = P(S_1(224)) = Y(114)$$

$$(P(S(X_{7(64)}, k_{(64)}))) = DF = P(S_4(223)) = Y(46)$$

$$(P(S(X_{6(64)}, k_{(64)}))) = 0C = P(S_3(12)) = Y(117)$$

$$(P(S(X_{5(64)}, k_{(64)}))) = 54 = P(S_2(84)) = Y(104)$$

$$(P(S(X_{4(64)}, k_{(64)}))) = 4D = P(S_4(77)) = Y(230)$$

$$(P(S(X_{3(64)}, k_{(64)}))) = 15 = P(S_3(21)) = Y(140)$$

$$(P(S(X_{2(64)}, k_{(64)}))) = 9B = P(S_2(155)) = Y(155)$$

$$(P(S(X_{1(64)}, k_{(64)}))) = 15 = P(S_1(21)) = Y(25)$$

$$z'_1 = z1 \oplus z3 \oplus z4 \oplus z6 \oplus z7 \oplus z8 = 25 \oplus 140 \oplus 230 \oplus 117 \oplus 46 \oplus 114 = 90$$

$$z'_2 = z1 \oplus z2 \oplus z4 \oplus z5 \oplus z7 \oplus z8 = 25 \oplus 155 \oplus 230 \oplus 104 \oplus 46 \oplus 114 = 80$$

$$z'_3 = z1 \oplus z2 \oplus z3 \oplus z5 \oplus z6 \oplus z8 = 25 \oplus 155 \oplus 140 \oplus 104 \oplus 117 \oplus 114 = 105$$

$$z'_4 = z2 \oplus z3 \oplus z4 \oplus z5 \oplus z6 \oplus z7 = 155 \oplus 140 \oplus 230 \oplus 104 \oplus 117 \oplus 46 = 194$$

$$z'_5 = z1 \oplus z2 \oplus z6 \oplus z7 \oplus z8 = 25 \oplus 155 \oplus 117 \oplus 46 \oplus 114 = 175$$

$$z'_6 = z2 \oplus z3 \oplus z5 \oplus z7 \oplus z8 = 155 \oplus 140 \oplus 104 \oplus 46 \oplus 114 = 35$$

$$z'_7 = z3 \oplus z4 \oplus z5 \oplus z6 \oplus z8 = 140 \oplus 230 \oplus 104 \oplus 117 \oplus 114 = 5$$

$$z'_8 = z1 \oplus z4 \oplus z5 \oplus z6 \oplus z7 = 25 \oplus 230 \oplus 104 \oplus 117 \oplus 46 = 204$$

$$z'_{(64)} = 5A50\ 69C2\ AF23\ 05CC$$

$$R_{10} = L_{11} \oplus F(R_{11}, k_{11})$$

$$= 2B71\ 4201\ 489E\ 7292 \oplus 5A50\ 69C2\ AF23\ 05CC$$

$$= 7121\ 2BC3\ E7BD\ 775E$$

$$L_{10} = 8F4D\ 5AE2\ EC0F\ B435$$

i. Round $\rightarrow$ 10

$$R_9 = L_{10} \oplus F(R_{10}, k_{10})$$

$$L_9 = R_{10}$$

$$R_9 = L_{10} \oplus F(R_{10}, k_{10})$$

$$= 8F4D\ 5AE2\ EC0F\ B435 \oplus F(R_{10}, k_{10})$$

$$L_9 = 7121\ 2BC3\ E7BD\ 775E$$

$$k_{10} = 9303\ 2344\ 8555\ 34E4$$

$$(X_{(64)}, k_{(64)}) \rightarrow Y_{(64)} = (P(S(X_{(64)} \oplus k_{(64)}))$$

$$\begin{aligned} X_{(64)} \oplus k_{(64)} &= 7121\ 2BC3\ E7BD\ 775E \oplus 9303\ 2344\ 8555\ 34E4 \\ &= E222\ 0887\ 62E8\ 43BA \end{aligned}$$

$$(P(S(X_{8(64)}, k_{(64)}))) = E2 = P(S_1(226)) = Y(185)$$

$$(P(S(X_{7(64)}, k_{(64)}))) = 22 = P(S_4(34)) = Y(251)$$

$$(P(S(X_{6(64)}, k_{(64)}))) = 08 = P(S_3(8)) = Y(114)$$

$$(P(S(X_{5(64)}, k_{(64)}))) = 87 = P(S_2(135)) = Y(47)$$

$$(P(S(X_{4(64)}, k_{(64)}))) = 62 = P(S_4(98)) = Y(159)$$

$$(P(S(X_{3(64)}, k_{(64)}))) = E8 = P(S_3(232)) = Y(27)$$

$$(P(S(X_{2(64)}, k_{(64)}))) = 43 = P(S_2(67)) = Y(204)$$

$$(P(S(X_{1(64)}, k_{(64)}))) = BA = P(S_1(186)) = Y(111)$$

$$z'_1 = z1 \oplus z3 \oplus z4 \oplus z6 \oplus z7 \oplus z8 = 111 \oplus 27 \oplus 159 \oplus 114 \oplus 251 \oplus 185 = 219$$

$$z'_2 = z1 \oplus z2 \oplus z4 \oplus z5 \oplus z7 \oplus z8 = 111 \oplus 204 \oplus 159 \oplus 47 \oplus 251 \oplus 185 = 81$$

$$z'_3 = z1 \oplus z2 \oplus z3 \oplus z5 \oplus z6 \oplus z8 = 111 \oplus 204 \oplus 27 \oplus 47 \oplus 114 \oplus 185 = 92$$

$$z'_4 = z2 \oplus z3 \oplus z4 \oplus z5 \oplus z6 \oplus z7 = 204 \oplus 27 \oplus 159 \oplus 47 \oplus 114 \oplus 251 = 238$$

$$z'_5 = z1 \oplus z2 \oplus z6 \oplus z7 \oplus z8 = 111 \oplus 204 \oplus 114 \oplus 251 \oplus 185 = 147$$

$$z'_6 = z2 \oplus z3 \oplus z5 \oplus z7 \oplus z8 = 204 \oplus 27 \oplus 47 \oplus 251 \oplus 185 = 186$$

$$z'_7 = z3 \oplus z4 \oplus z5 \oplus z6 \oplus z8 = 27 \oplus 159 \oplus 47 \oplus 114 \oplus 185 = 96$$

$$z'_8 = z1 \oplus z4 \oplus z5 \oplus z6 \oplus z7 = 111 \oplus 159 \oplus 47 \oplus 114 \oplus 251 = 86$$

$$z'_{(64)} = DB51\ 5CEE\ 93BA\ 6056$$

$$R_9 = L_{10} \oplus F(R_{10}, k_{10})$$

$$= 8F4D\ 5AE2\ EC0F\ B435 \oplus DB51\ 5CEE\ 93BA\ 6056$$

$$= 541C\ 060C\ 7FB5\ D463$$

$$L_9 = 7121\ 2BC3\ E7BD\ 775E$$

j. Round $\rightarrow 9$

$$R_8 = L_9 \oplus F(R_9, k_9)$$

$$L_8 = R_9$$

$$R_8 = L_9 \oplus F(R_9, k_9)$$

$$= 7121\ 2BC3\ E7BD\ 775E \oplus F(R_9, k_9)$$

$$L_8 = 541C\ 060C\ 7FB5\ D463$$

$$k_9 = 5E40\ DF24\ AD6D\ 4234$$

$$(X_{(64)}, k_{(64)}) \rightarrow Y_{(64)} = (P(S(X_{(64)} \oplus k_{(64)})))$$

$$X_{(64)} \oplus k_{(64)} = 166F\ 7958\ 8D3D\ F9A7 \oplus 5E40\ DF24\ AD6D\ 4234$$

$$= 0A5C\ D928\ D2D8\ 9657$$

$$(P(S(X_{8(64)}, k_{(64)}))) = 0A = P(S_1(10)) = Y(87)$$

$$(P(S(X_{7(64)}, k_{(64)}))) = 5C = P(S_4(92)) = Y(129)$$

$$(P(S(X_{6(64)}, k_{(64)}))) = D9 = P(S_3(217)) = Y(146)$$

$$(P(S(X_{5(64)}, k_{(64)}))) = 28 = P(S_2(40)) = Y(124)$$

$$(P(S(X_{4(64)}, k_{(64)}))) = D2 = P(S_4(210)) = Y(74)$$

$$(P(S(X_{3(64)}, k_{(64)}))) = D8 = P(S_3(216)) = Y(106)$$

$$(P(S(X_{2(64)}, k_{(64)}))) = 96 = P(S_2(150)) = Y(234)$$

$$(P(S(X_{1(64)}, k_{(64)}))) = 57 = P(S_1(87)) = Y(5)$$

$$z'_1 = z1 \oplus z3 \oplus z4 \oplus z6 \oplus z7 \oplus z8 = 5 \oplus 106 \oplus 74 \oplus 146 \oplus 129 \oplus 87 = 97$$

$$z'_2 = z1 \oplus z2 \oplus z4 \oplus z5 \oplus z7 \oplus z8 = 5 \oplus 234 \oplus 74 \oplus 124 \oplus 129 \oplus 87 = 15$$

$$z'_3 = z1 \oplus z2 \oplus z3 \oplus z5 \oplus z6 \oplus z8 = 5 \oplus 234 \oplus 106 \oplus 124 \oplus 146 \oplus 87 = 60$$

$$z'_4 = z2 \oplus z3 \oplus z4 \oplus z5 \oplus z6 \oplus z7 = 234 \oplus 106 \oplus 74 \oplus 124 \oplus 146 \oplus 129 = 165$$

$$z'_5 = z1 \oplus z2 \oplus z6 \oplus z7 \oplus z8 = 5 \oplus 234 \oplus 146 \oplus 129 \oplus 87 = 171$$

$$z'_6 = z2 \oplus z3 \oplus z5 \oplus z7 \oplus z8 = 234 \oplus 106 \oplus 124 \oplus 129 \oplus 87 = 42$$

$$z'_7 = z3 \oplus z4 \oplus z5 \oplus z6 \oplus z8 = 106 \oplus 74 \oplus 124 \oplus 146 \oplus 87 = 153$$

$$z'_8 = z1 \oplus z4 \oplus z5 \oplus z6 \oplus z7 = 5 \oplus 74 \oplus 124 \oplus 146 \oplus 129 = 32$$

$$z'_{(64)} = 610F\ 3CA5\ AB2A\ 9920$$

$$R_8 = L_9 \oplus F(R_9, k_9)$$

$$= 7121\ 2BC3\ E7BD\ 775E \oplus 610F\ 3CA5\ AB2A\ 9920$$

$$= 102E\ 1766\ 4C97\ EE7E$$

$$L_8 = 541C\ 060C\ 7FB5\ D463$$

k. Round $\rightarrow$ 8

$$R_7 = L_8 \oplus F(R_8, k_8)$$

$$L_7 = R_8$$

$$R_7 = L_8 \oplus F(R_8, k_8)$$

$$= 541C\ 060C\ 7FB5\ D463 \oplus F(R_8, k_8)$$

$$L_7 = 102E\ 1766\ 4C97\ EE7E$$

$$k_8 = 69C9\ 2606\ 4689\ 0AAA$$

$$(X_{(64)}, k_{(64)}) \rightarrow Y_{(64)} = (P(S(X_{(64)} \oplus k_{(64)})))$$

$$X_{(64)} \oplus k_{(64)} = 102E\ 1766\ 4C97\ EE7E \oplus 69C9\ 2606\ 4689\ 0AAA$$

$$= 79E7\ 3160\ 0A1E\ E4D4$$

$$(P(S(X_{8(64)}, k_{(64)}))) = 79 = P(S_1(121)) = Y(8)$$

$$(P(S(X_{7(64)}, k_{(64)}))) = E7 = P(S_4(231)) = Y(89)$$

$$(P(S(X_{6(64)}, k_{(64)}))) = 31 = P(S_3(49)) = Y(240)$$

$$(P(S(X_{5(64)}, k_{(64)}))) = 60 = P(S_2(96)) = Y(40)$$

$$(P(S(X_{4(64)}, k_{(64)}))) = 0A = P(S_4(10)) = Y(69)$$

$$(P(S(X_{3(64)}, k_{(64)}))) = 1E = P(S_3(30)) = Y(73)$$

$$(P(S(X_{2(64)}, k_{(64)}))) = E4 = P(S_2(228)) = Y(241)$$

$$(P(S(X_{1(64)}, k_{(64)}))) = 7E \oplus AA = D4 = P(S_1(212)) = Y(231)$$

$$z'_1 = z1 \oplus z3 \oplus z4 \oplus z6 \oplus z7 \oplus z8 = 231 \oplus 73 \oplus 69 \oplus 240 \oplus 89 \oplus 8 = 74$$

$$z'_2 = z1 \oplus z2 \oplus z4 \oplus z5 \oplus z7 \oplus z8 = 231 \oplus 241 \oplus 69 \oplus 40 \oplus 89 \oplus 8 = 42$$

$$z'_3 = z1 \oplus z2 \oplus z3 \oplus z5 \oplus z6 \oplus z8 = 231 \oplus 241 \oplus 73 \oplus 40 \oplus 240 \oplus 8 = 143$$

$$z'_4 = z2 \oplus z3 \oplus z4 \oplus z5 \oplus z6 \oplus z7 = 241 \oplus 73 \oplus 69 \oplus 40 \oplus 240 \oplus 89 = 124$$

$$z'_5 = z1 \oplus z2 \oplus z6 \oplus z7 \oplus z8 = 231 \oplus 241 \oplus 240 \oplus 89 \oplus 8 = 183$$

$$z'_6 = z2 \oplus z3 \oplus z5 \oplus z7 \oplus z8 = 241 \oplus 73 \oplus 40 \oplus 89 \oplus 8 = 193$$

$$z'_7 = z3 \oplus z4 \oplus z5 \oplus z6 \oplus z8 = 73 \oplus 69 \oplus 40 \oplus 240 \oplus 8 = 220$$

$$z'_8 = z1 \oplus z4 \oplus z5 \oplus z6 \oplus z7 = 231 \oplus 69 \oplus 40 \oplus 240 \oplus 89 = 35$$

$$z'_{(64)} = 4A2A\ 8F7C\ B7C1\ DC23$$

$$R_7 = L_8 \oplus F(R_8, k_8)$$

$$= 541C\ 060C\ 7FB5\ D463 \oplus 4A2A\ 8F7C\ B7C1\ DC23$$

$$= 1E36\ 8970\ C874\ 0840$$

$$L_7 = 102E\ 1766\ 4C97\ EE7E$$

1. Round $\rightarrow$ 7

$$R'_6 = L_7 \oplus F(L_7, k_7)$$

$$L'_6 = R_7$$

$$R_6 = FL(R'_7, kl_2)$$

$$L_6 = FL^{-1}(R'_7, kl_1)$$

$$R'_6 = L_7 \oplus F(L_7, k_7)$$

$$= 102E\ 1766\ 4C97\ EE7E \oplus F(L_7, k_{17})$$

$$L'_6 = 1E36\ 8970\ C874\ 0840$$

$$k_7 = 6926\ 4A69\ 6A49\ 2A0A$$

$$(X_{(64)}, k_{(64)}) \rightarrow Y_{(64)} = (P(S(X_{(64)} \oplus k_{(64)})))$$

$$X_{(64)} \oplus k_{(64)} = 1E36\ 8970\ C874\ 0840 \oplus 6926\ 4A69\ 6A49\ 2A0A$$

$$= 7710\ C319\ A23D\ 224A$$

$$(P(S(X_{8(64)}, k_{(64)}))) = 77 = P(S_1(119)) = Y(145)$$

$$(P(S(X_{7(64)}, k_{(64)}))) = 10 = P(S_4(16)) = Y(134)$$

$$(P(S(X_{6(64)}, k_{(64)}))) = C3 = P(S_3(195)) = Y(70)$$

$$(P(S(X_{5(64)}, k_{(64)}))) = 19 = P(S_2(25)) = Y(28)$$

$$(P(S(X_{4(64)}, k_{(64)}))) = A2 = P(S_4(162)) = Y(204)$$

$$(P(S(X_{3(64)}, k_{(64)}))) = 3D = P(S_3(61)) = Y(43)$$

$$(P(S(X_{2(64)}, k_{(64)}))) = 22 = P(S_2(34)) = Y(95)$$

$$(P(S(X_{1(64)}, k_{(64)}))) = 4A = P(S_1(74)) = Y(43)$$

$$z'_1 = z1 \oplus z3 \oplus z4 \oplus z6 \oplus z7 \oplus z8 = 43 \oplus 43 \oplus 204 \oplus 70 \oplus 234 \oplus 245 = 149$$

$$z'_2 = z1 \oplus z2 \oplus z4 \oplus z5 \oplus z7 \oplus z8 = 43 \oplus 95 \oplus 204 \oplus 28 \oplus 134 \oplus 145 = 179$$

$$z'_3 = z1 \oplus z2 \oplus z3 \oplus z5 \oplus z6 \oplus z8 = 43 \oplus 95 \oplus 43 \oplus 28 \oplus 70 \oplus 145 = 148$$

$$z'_4 = z2 \oplus z3 \oplus z4 \oplus z5 \oplus z6 \oplus z7 = 92 \oplus 43 \oplus 204 \oplus 28 \oplus 70 \oplus 134 = 103$$

$$z'_5 = z1 \oplus z2 \oplus z6 \oplus z7 \oplus z8 = 43 \oplus 95 \oplus 70 \oplus 134 \oplus 145 = 37$$

$$z'_6 = z2 \oplus z3 \oplus z5 \oplus z7 \oplus z8 = 95 \oplus 43 \oplus 28 \oplus 134 \oplus 145 = 127$$

$$z'_7 = z3 \oplus z4 \oplus z5 \oplus z6 \oplus z8 = 43 \oplus 204 \oplus 28 \oplus 70 \oplus 145 = 44$$

$$z'_8 = z1 \oplus z4 \oplus z5 \oplus z6 \oplus z7 = 43 \oplus 204 \oplus 28 \oplus 70 \oplus 134 = 59$$

$$z'_{(64)} = 95B3\ 9467\ 257F\ 2C3B$$

$$R'_6 = L_7 \oplus F(L_7, k_7)$$

$$= 102E\ 1766\ 4C97\ EE7E \oplus 95B3\ 9467\ 257F\ 2C3B$$

$$= 859D\ 8301\ 69E8\ C245$$

$$L'_6 = 1E36\ 8970\ C874\ 0840$$

Menerapkan fungsi FL pada R'_6 dengan kl_2 , untuk mendapatkan R_6

Definisi FL:

$$R_6 = FL(R'_6, kl_2)$$

Jika input $(X_{L(32)} \parallel X_{R(32)}, kl_{L(32)} \parallel kl_{R(32)}) \rightarrow Y_{L(32)} \parallel Y_{R(32)}$

Maka:

$$Y_{R(32)} = ((X_{L(32)} \cap kl_{L(32)}) \lll 1) \oplus X_{R(32)}$$

$$Y_{L(32)} = (Y_{R(32)} \cup kl_{R(32)}) \oplus X_{L(32)}$$

$$\text{Output } Y = Y_L \parallel Y_R$$

Ambil nilai:

$$X = R'_6 = 859D\ 8301\ 69E8\ C245 \rightarrow X_L = 859D\ 8301, X_R = 69E8\ C245$$

$$kl_2 = F644\ C8C6\ 31C8\ ABA6 \rightarrow kl_{2L} = F644\ C8C6, kl_{2R} = 31C8\ ABA6$$

$$Y_{R(32)} = ((X_{L(32)} \cap kl_{L(32)}) \lll 1) \oplus X_{R(32)}$$

$$= ((859D\ 8301 \cap F644\ C8C6) \lll 1) \oplus 69E8\ C245$$

$$= (8404\ 8000 \lll 1) \oplus 69E8\ C245$$

$$Y_R = 0809\ 0001 \oplus 69E8\ C245 = 61E1\ C244$$

$$Y_{L(32)} = (Y_{R(32)} \cup kl_{R(32)}) \oplus X_{L(32)}$$

$$= (61E1\ C244 \cup 31C8\ ABA6) \oplus 859D\ 8301$$

$$Y_L = 71E9\ EBE6 \oplus 859D\ 8301 = F474\ 68E7$$

$$R_6 = FL(R'_6, kl_2) = Y_L \parallel Y_R = F474\ 68E7 \parallel 61E1\ C244$$

$$R_6 = F474\ 68E7\ 61E1\ C244$$

Menerapkan FL^{-1} pada L'_6 dengan kl_1 untuk mendapatkan L_6

$$R_6 = FL^{-1}(L'_6, kl_1)$$

Definisi FL^{-1} :

Jika input $(Y_{L(32)} \parallel Y_{R(32)}, kl_{L(32)} \parallel kl_{R(32)}) \rightarrow X_{L(32)} \parallel X_{R(32)}$:

Maka:

$$X_{L(32)} = (Y_{R(32)} \cup kl_{R(32)}) \oplus Y_{L(32)}$$

$$X_{R(32)} = ((X_{L(32)} \cap kl_{L(32)}) \lll 1) \oplus Y_{R(32)}$$

$$\text{Output } X = X_{L(32)} \parallel X_{R(32)}$$

Ambil nilai:

$$Y = L'_6 = 1E36\ 8970\ C874\ 0840 \rightarrow Y_L = 1E36\ 8970, Y_R = C874\ 0840$$

$$kl_1 = 8468\ BC81\ BE49\ 5ADA \rightarrow kl_{1L} = 8468\ BC81, kl_{1R} = BE49\ 5ADA$$

$$\begin{aligned} X_{L(32)} &= (Y_{R(32)} \cup kl_{R(32)}) \oplus Y_{L(32)} \\ &= (C874\ 0840 \cup BE49\ 5ADA) \oplus 1E36\ 8970 \end{aligned}$$

$$X_L = FE7D\ 5ADA \oplus 1E36\ 8970 = E04B\ D3AA$$

$$\begin{aligned} X_{R(32)} &= ((X_{L(32)} \cap kl_{L(32)}) \lll 1) \oplus Y_{R(32)} \\ &= ((E04B\ D3AA \cap 8468\ BC81) \lll 1) \oplus C874\ 0840 \\ &= (8048\ 9080 \lll 1) \oplus C874\ 0840 \end{aligned}$$

$$X_R = 0091\ 2101 \oplus C874\ 0840 = C8E5\ 2941$$

$$L_6 = FL^{-1}(R'_6, kl_1) = X_L \parallel X_R = E04B\ D3AA \parallel C8E5\ 2941$$

$$L_6 = E04B\ D3AA\ C8E5\ 2941$$

Hasil akhir Round 13:

$$R'_6 = 859D\ 8301\ 69E8\ C245 \text{ setelah } FL^{-1}: R_6 = F474\ 68E7\ 61E1\ C244$$

$$L'_6 = 1E36\ 8970\ C874\ 0840 \text{ setelah } FL: L_6 = E04B\ D3AA\ C8E5\ 2941$$

m. Round $\rightarrow 6$

$$R_5 = L_6 \oplus F(R_6, k_6)$$

$$L_5 = R_6$$

$$\begin{aligned} R_5 &= L_6 \oplus F(R_6, k_6) \\ &= E04B\ D3AA\ C8E5\ 2941 \oplus F(R_6, k_6) \end{aligned}$$

$$L_5 = F474\ 68E7\ 61E1\ C244$$

$$k_6 = 69C9\ 2606\ 4689\ 0AAA$$

$$(X_{(64)}, k_{(64)}) \rightarrow Y_{(64)} = (P(S(X_{(64)} \oplus k_{(64)})))$$

$$\begin{aligned} X_{(64)} \oplus k_{(64)} &= F474\ 68E7\ 61E1\ C244 \oplus 574D\ EC89\ 918C\ 6391 \\ &= A339\ 846E\ F06D\ A1D5 \end{aligned}$$

$$(P(S(X_{8(64)}, k_{(64)}))) = A3 = P(S_1(163)) = Y(2)$$

$$(P(S(X_{7(64)}, k_{(64)}))) = 39 = P(S_4(57)) = Y(207)$$

$$(P(S(X_{6(64)}, k_{(64)}))) = 84 = P(S_3(132)) = Y(208)$$

$$(P(S(X_{5(64)}, k_{(64)}))) = 6E = P(S_2(110)) = Y(229)$$

$$(P(S(X_{4(64)}, k_{(64)}))) = F0 = P(S_4(240)) = Y(7)$$

$$(P(S(X_{3(64)}, k_{(64)}))) = 6D = P(S_3(109)) = Y(12)$$

$$(P(S(X_{2(64)}, k_{(64)}))) = A1 = P(S_2(161)) = Y(184)$$

$$(P(S(X_{1(64)}, k_{(64)}))) = D5 = P(S_1(213)) = Y(70)$$

$$z'_1 = z1 \oplus z3 \oplus z4 \oplus z6 \oplus z7 \oplus z8 = 70 \oplus 12 \oplus 7 \oplus 208 \oplus 207 \oplus 2 = 80$$

$$z'_2 = z1 \oplus z2 \oplus z4 \oplus z5 \oplus z7 \oplus z8 = 70 \oplus 184 \oplus 7 \oplus 229 \oplus 207 \oplus 2 = 209$$

$$z'_3 = z1 \oplus z2 \oplus z3 \oplus z5 \oplus z6 \oplus z8 = 70 \oplus 184 \oplus 12 \oplus 229 \oplus 208 \oplus 2 = 197$$

$$z'_4 = z2 \oplus z3 \oplus z4 \oplus z5 \oplus z6 \oplus z7 = 184 \oplus 12 \oplus 7 \oplus 229 \oplus 208 \oplus 207 = 73$$

$$z'_5 = z1 \oplus z2 \oplus z6 \oplus z7 \oplus z8 = 70 \oplus 184 \oplus 208 \oplus 207 \oplus 2 = 227$$

$$z'_6 = z2 \oplus z3 \oplus z5 \oplus z7 \oplus z8 = 184 \oplus 12 \oplus 229 \oplus 207 \oplus 2 = 156$$

$$z'_7 = z3 \oplus z4 \oplus z5 \oplus z6 \oplus z8 = 12 \oplus 7 \oplus 229 \oplus 208 \oplus 2 = 60$$

$$z'_8 = z1 \oplus z4 \oplus z5 \oplus z6 \oplus z7 = 70 \oplus 7 \oplus 229 \oplus 208 \oplus 207 = 187$$

$$z'_{(64)} = 50D1\ C549\ E39C\ 3CBB$$

$$R_5 = L_6 \oplus F(R_6, k_6)$$

$$= E04B\ D3AA\ C8E5\ 2941 \oplus 50D1\ C549\ E39C\ 3CBB$$

$$= \text{B09A 16E3 2B79 15FA}$$

$$L_5 = \text{F474 68E7 61E1 C244}$$

n. Round $\rightarrow 5$

$$R_4 = L_5 \oplus F(R_5, k_5)$$

$$L_4 = R_5$$

$$R_4 = L_5 \oplus F(R_5, k_5)$$

$$= \text{F474 68E7 61E1 C244} \oplus F(R_5, k_5)$$

$$L_4 = \text{B09A 16E3 2B79 15FA}$$

$$K_5 = \text{B5B5 08D1 7903 7C92}$$

$$(X_{(64)}, k_{(64)}) \rightarrow Y_{(64)} = (P(S(X_{(64)} \oplus k_{(64)})))$$

$$X_{(64)} \oplus k_{(64)} = \text{B09A 16E3 2B79 15FA} \oplus \text{B5B5 08D1 7903 7C92}$$

$$= \text{052F 1E32 527A 6968}$$

$$(P(S(X_{8(64)}, k_{(64)}))) = 05 = P(S_1(5)) = Y(39)$$

$$(P(S(X_{7(64)}, k_{(64)}))) = 2F = P(S_4(47)) = Y(4)$$

$$(P(S(X_{6(64)}, k_{(64)}))) = 1E = P(S_3(30)) = Y(73)$$

$$(P(S(X_{5(64)}, k_{(64)}))) = 32 = P(S_2(50)) = Y(114)$$

$$(P(S(X_{4(64)}, k_{(64)}))) = 52 = P(S_4(82)) = Y(205)$$

$$(P(S(X_{3(64)}, k_{(64)}))) = 7A = P(S_3(122)) = Y(116)$$

$$(P(S(X_{2(64)}, k_{(64)}))) = 69 = P(S_2(105)) = Y(30)$$

$$(P(S(X_{1(64)}, k_{(64)}))) = 68 = P(S_1(104)) = Y(50)$$

$$z'_1 = z1 \oplus z3 \oplus z4 \oplus z6 \oplus z7 \oplus z8 = 50 \oplus 116 \oplus 205 \oplus 73 \oplus 4 \oplus 39 = 225$$

$$z'_2 = z1 \oplus z2 \oplus z4 \oplus z5 \oplus z7 \oplus z8 = 50 \oplus 30 \oplus 205 \oplus 114 \oplus 4 \oplus 39 = 176$$

$$z'_3 = z1 \oplus z2 \oplus z3 \oplus z5 \oplus z6 \oplus z8 = 50 \oplus 30 \oplus 116 \oplus 114 \oplus 73 \oplus 39 = 68$$

$$z'_4 = z2 \oplus z3 \oplus z4 \oplus z5 \oplus z6 \oplus z7 = 30 \oplus 116 \oplus 205 \oplus 114 \oplus 73 \oplus 4 = 152$$

$$z'_5 = z1 \oplus z2 \oplus z6 \oplus z7 \oplus z8 = 50 \oplus 30 \oplus 73 \oplus 4 \oplus 39 = 70$$

$$z'_6 = z2 \oplus z3 \oplus z5 \oplus z7 \oplus z8 = 30 \oplus 116 \oplus 114 \oplus 4 \oplus 39 = 59$$

$$z'_7 = z3 \oplus z4 \oplus z5 \oplus z6 \oplus z8 = 116 \oplus 205 \oplus 114 \oplus 73 \oplus 39 = 165$$

$$z'_8 = z1 \oplus z4 \oplus z5 \oplus z6 \oplus z7 = 50 \oplus 205 \oplus 114 \oplus 73 \oplus 4 = 192$$

$$z'_{(64)} = \text{E1B0 4498 463B A5C0}$$

$$\begin{aligned} R_4 &= L_5 \oplus F(R_5, k_5) \\ &= \text{F474 68E7 61E1 C244} \oplus \text{E1B0 4498 463B A5C0} \\ &= \text{15C4 2C7F 27DA 6784} \end{aligned}$$

$$L_4 = \text{B09A 16E3 2B79 15FA}$$

o. Round $\rightarrow 4$

$$R_3 = L_4 \oplus F(R_4, k_4)$$

$$L_3 = R_4$$

$$\begin{aligned} R_3 &= L_4 \oplus F(R_4, k_4) \\ &= \text{B09A 16E3 2B79 15FA} \oplus F(R_4, k_4) \end{aligned}$$

$$L_3 = \text{15C4 2C7F 27DA 6784}$$

$$K_4 = \text{1A24 2AA9 A724 9819}$$

$$(X_{(64)}, k_{(64)}) \rightarrow Y_{(64)} = (P(S(X_{(64)} \oplus k_{(64)})))$$

$$\begin{aligned} X_{(64)} \oplus k_{(64)} &= \text{15C4 2C7F 27DA 6784} \oplus \text{1A24 2AA9 A724 9819} \\ &= \text{0FE0 06D6 80FE FF9D} \end{aligned}$$

$$(P(S(X_{8(64)}, k_{(64)}))) = 0F = P(S_1(15)) = Y(65)$$

$$(P(S(X_{7(64)}, k_{(64)}))) = E0 = P(S_4(224)) = Y(121)$$

$$(P(S(X_{6(64)}, k_{(64)}))) = 06 = P(S_3(6)) = Y(96)$$

$$(P(S(X_{5(64)}, k_{(64)}))) = D6 = P(S_2(214)) = Y(226)$$

$$(P(S(X_{4(64)}, k_{(64)}))) = 80 = P(S_4(128)) = Y(130)$$

$$(P(S(X_{3(64)}, k_{(64)}))) = FE = P(S_3(254)) = Y(64)$$

$$(P(S(X_{2(64)}, k_{(64)}))) = FF = P(S_2(255)) = Y(61)$$

$$(P(S(X_{1(64)}, k_{(64)}))) = 9D = P(S_1(157)) = Y(63)$$

$$z'_1 = z1 \oplus z3 \oplus z4 \oplus z6 \oplus z7 \oplus z8 = 63 \oplus 64 \oplus 130 \oplus 96 \oplus 121 \oplus 65 = 165$$

$$z'_2 = z1 \oplus z2 \oplus z4 \oplus z5 \oplus z7 \oplus z8 = 63 \oplus 61 \oplus 130 \oplus 226 \oplus 121 \oplus 65 = 90$$

$$z'_3 = z1 \oplus z2 \oplus z3 \oplus z5 \oplus z6 \oplus z8 = 63 \oplus 61 \oplus 64 \oplus 226 \oplus 96 \oplus 65 = 129$$

$$z'_4 = z2 \oplus z3 \oplus z4 \oplus z5 \oplus z6 \oplus z7 = 61 \oplus 64 \oplus 130 \oplus 226 \oplus 96 \oplus 121 = 04$$

$$z'_5 = z1 \oplus z2 \oplus z6 \oplus z7 \oplus z8 = 63 \oplus 61 \oplus 96 \oplus 121 \oplus 65 = 90$$

$$z'_6 = z2 \oplus z3 \oplus z5 \oplus z7 \oplus z8 = 61 \oplus 64 \oplus 226 \oplus 121 \oplus 65 = 167$$

$$z'_7 = z3 \oplus z4 \oplus z5 \oplus z6 \oplus z8 = 64 \oplus 130 \oplus 226 \oplus 96 \oplus 65 = 01$$

$$z'_8 = z1 \oplus z4 \oplus z5 \oplus z6 \oplus z7 = 63 \oplus 130 \oplus 226 \oplus 96 \oplus 121 = 70$$

$$z'_{(64)} = A55A\ 8104\ 5AA7\ 0146$$

$$R_3 = L_4 \oplus F(R_4, k_4)$$

$$= B09A\ 16E3\ 2B79\ 15FA \oplus A55A\ 8104\ 5AA7\ 0146$$

$$= 15C0\ 97E7\ 71DE\ 14BC$$

$$L_3 = 15C4\ 2C7F\ 27DA\ 6784$$

p. Round $\rightarrow$ 3

$$R_2 = L_3 \oplus F(R_3, k_3)$$

$$L_2 = R_3$$

$$R_2 = L_3 \oplus F(R_3, k_3)$$

$$= 15C4\ 2C7F\ 27DA\ 6784 \oplus F(R_3, k_3)$$

$$L_2 = 15C0\ 97E7\ 71DE\ 14BC$$

$$K_3 = A924\ A829\ A499\ 29A5$$

$$(X_{(64)}, k_{(64)}) \rightarrow Y_{(64)} = (P(S(X_{(64)} \oplus k_{(64)})))$$

$$\begin{aligned}
X_{(64)} \oplus k_{(64)} &= 15C0\ 97E7\ 71DE\ 14BC \oplus A924\ A829\ A499\ 29A5 \\
&= BCE4\ 3FCE\ D547\ 3D19
\end{aligned}$$

$$(P(S(X_{8(64)}, k_{(64)}))) = BC = P(S_1(188)) = Y(19)$$

$$(P(S(X_{7(64)}, k_{(64)}))) = E4 = P(S_4(228)) = Y(245)$$

$$(P(S(X_{6(64)}, k_{(64)}))) = 3F = P(S_3(63)) = Y(166)$$

$$(P(S(X_{5(64)}, k_{(64)}))) = CE = P(S_2(206)) = Y(105)$$

$$(P(S(X_{4(64)}, k_{(64)}))) = D5 = P(S_4(213)) = Y(185)$$

$$(P(S(X_{3(64)}, k_{(64)}))) = 47 = P(S_3(71)) = Y(150)$$

$$(P(S(X_{2(64)}, k_{(64)}))) = 3D = P(S_2(61)) = Y(172)$$

$$(P(S(X_{1(64)}, k_{(64)}))) = 19 = P(S_1(25)) = Y(14)$$

$$z'_1 = z1 \oplus z3 \oplus z4 \oplus z6 \oplus z7 \oplus z8 = 14 \oplus 150 \oplus 185 \oplus 166 \oplus 145 \oplus 19 = 05$$

$$z'_2 = z1 \oplus z2 \oplus z4 \oplus z5 \oplus z7 \oplus z8 = 14 \oplus 172 \oplus 185 \oplus 105 \oplus 245 \oplus 19 = 148$$

$$z'_3 = z1 \oplus z2 \oplus z3 \oplus z5 \oplus z6 \oplus z8 = 14 \oplus 172 \oplus 150 \oplus 105 \oplus 166 \oplus 19 = 232$$

$$z'_4 = z2 \oplus z3 \oplus z4 \oplus z5 \oplus z6 \oplus z7 = 172 \oplus 150 \oplus 185 \oplus 105 \oplus 166 \oplus 245 = 185$$

$$z'_5 = z1 \oplus z2 \oplus z6 \oplus z7 \oplus z8 = 14 \oplus 172 \oplus 166 \oplus 245 \oplus 19 = 226$$

$$z'_6 = z2 \oplus z3 \oplus z5 \oplus z7 \oplus z8 = 172 \oplus 150 \oplus 105 \oplus 245 \oplus 19 = 181$$

$$z'_7 = z3 \oplus z4 \oplus z5 \oplus z6 \oplus z8 = 150 \oplus 185 \oplus 105 \oplus 166 \oplus 245 = 21$$

$$z'_8 = z1 \oplus z4 \oplus z5 \oplus z6 \oplus z7 = 14 \oplus 185 \oplus 105 \oplus 166 \oplus 245 = 141$$

$$Z'_{(64)} = 0594\ E8B9\ E2B5\ 158D$$

$$R_2 = L_3 \oplus F(R_3, k_3)$$

$$= 15C4\ 2C7F\ 27DA\ 6784 \oplus 0594\ E8B9\ E2B5\ 158D$$

$$= 1050\ C4C6\ C56F\ 7209$$

$$L_2 = 15C0\ 97E7\ 71DE\ 14BC$$

q. Round $\rightarrow 2$

$$R_1 = L_2 \oplus F(R_2, k_2)$$

$$L_1 = R_2$$

$$R_1 = L_2 \oplus F(R_2, k_2)$$

$$= 15C0\ 97E7\ 71DE\ 14BC \oplus F(R_2, k_2)$$

$$L_1 = 1050\ C4C6\ C56F\ 7209$$

$$K_2 = C722\ AE9B\ D913\ 2318$$

$$(X_{(64)}, k_{(64)}) \rightarrow Y_{(64)} = (P(S(X_{(64)} \oplus k_{(64)})))$$

$$X_{(64)} \oplus k_{(64)} = 1050\ C4C6\ C56F\ 7209 \oplus C722\ AE9B\ D913\ 2318$$

$$= D772\ 6A5D\ 1C7C\ 5111$$

$$(P(S(X_{8(64)}, k_{(64)}))) = D7 = P(S_1(215)) = Y(186)$$

$$(P(S(X_{7(64)}, k_{(64)}))) = 72 = P(S_4(114)) = Y(248)$$

$$(P(S(X_{6(64)}, k_{(64)}))) = 6A = P(S_3(106)) = Y(78)$$

$$(P(S(X_{5(64)}, k_{(64)}))) = 5D = P(S_2(93)) = Y(46)$$

$$(P(S(X_{4(64)}, k_{(64)}))) = 1C = P(S_4(28)) = Y(217)$$

$$(P(S(X_{3(64)}, k_{(64)}))) = 7C = P(S_3(124)) = Y(48)$$

$$(P(S(X_{2(64)}, k_{(64)}))) = 51 = P(S_2(81)) = Y(176)$$

$$(P(S(X_{1(64)}, k_{(64)}))) = 11 = P(S_1(17)) = Y(239)$$

$$z'_1 = z1 \oplus z3 \oplus z4 \oplus z6 \oplus z7 \oplus z8 = 239 \oplus 48 \oplus 217 \oplus 78 \oplus 248 \oplus 186 = 10$$

$$z'_2 = z1 \oplus z2 \oplus z4 \oplus z5 \oplus z7 \oplus z8 = 239 \oplus 176 \oplus 217 \oplus 46 \oplus 248 \oplus 186 = 234$$

$$z'_3 = z1 \oplus z2 \oplus z3 \oplus z5 \oplus z6 \oplus z8 = 239 \oplus 176 \oplus 48 \oplus 46 \oplus 78 \oplus 186 = 181$$

$$z'_4 = z2 \oplus z3 \oplus z4 \oplus z5 \oplus z6 \oplus z7 = 176 \oplus 48 \oplus 217 \oplus 46 \oplus 78 \oplus 248 = 193$$

$$z'_5 = z1 \oplus z2 \oplus z6 \oplus z7 \oplus z8 = 239 \oplus 176 \oplus 78 \oplus 248 \oplus 186 = 83$$

$$z'_6 = z2 \oplus z3 \oplus z5 \oplus z7 \oplus z8 = 176 \oplus 48 \oplus 46 \oplus 248 \oplus 186 = 236$$

$$z'_7 = z3 \oplus z4 \oplus z5 \oplus z6 \oplus z8 = 48 \oplus 217 \oplus 46 \oplus 78 \oplus 186 = 51$$

$$z'_8 = z1 \oplus z4 \oplus z5 \oplus z6 \oplus z7 = 239 \oplus 217 \oplus 46 \oplus 78 \oplus 248 = 174$$

$$z'_{(64)} = 0AEA\ B5C1\ 53EC\ 33AE$$

$$\begin{aligned} R_1 &= L_2 \oplus F(R_2, k_2) \\ &= 15C0\ 97E7\ 71DE\ 14BC \oplus 0AEA\ B5C1\ 53EC\ 33AE \\ &= 1F2A\ 2226\ 2232\ 2712 \end{aligned}$$

$$L_1 = 1050\ C4C6\ C56F\ 7209$$

r. Round $\rightarrow 1$

$$R_0 = L_1 \oplus F(R_1, k_1)$$

$$L_0 = R_1$$

$$\begin{aligned} R_0 &= L_1 \oplus F(R_1, k_1) \\ &= 1050\ C4C6\ C56F\ 7209 \oplus F(R_1, k_1) \end{aligned}$$

$$L_0 = 1F2A\ 2226\ 2232\ 2712$$

$$k_1 = F925\ 6B6A\ 11A2\ F206$$

$$(X_{(64)}, k_{(64)}) \rightarrow Y_{(64)} = (P(S(X_{(64)} \oplus k_{(64)})))$$

$$\begin{aligned} X_{(64)} \oplus k_{(64)} &= 1F2A\ 2226\ 2232\ 2712 \oplus F925\ 6B6A\ 11A2\ F206 \\ &= E60F\ 494C\ 3390\ D514 \end{aligned}$$

$$(P(S(X_{8(64)}, k_{(64)}))) = E6 = P(S_1(230)) = Y(172)$$

$$(P(S(X_{7(64)}, k_{(64)}))) = 0F = P(S_4(15)) = Y(146)$$

$$(P(S(X_{6(64)}, k_{(64)}))) = 49 = P(S_3(73)) = Y(9)$$

$$(P(S(X_{5(64)}, k_{(64)}))) = 4C = P(S_2(76)) = Y(225)$$

$$(P(S(X_{4(64)}, k_{(64)}))) = 33 = P(S_4(51)) = Y(17)$$

$$(P(S(X_{3(64)}, k_{(64)}))) = 90 = P(S_3(144)) = Y(8)$$

$$(P(S(X_{2(64)}, k_{(64)}))) = D5 = P(S_2(213)) = Y(140)$$

$$(P(S(X_{1(64)}, k_{(64)})) = 14 = P(S_1(20)) = Y(69)$$

$$z'_1 = z1 \oplus z3 \oplus z4 \oplus z6 \oplus z7 \oplus z8 = 69 \oplus 8 \oplus 17 \oplus 9 \oplus 146 \oplus 172 = 107$$

$$z'_2 = z1 \oplus z2 \oplus z4 \oplus z5 \oplus z7 \oplus z8 = 69 \oplus 140 \oplus 17 \oplus 225 \oplus 146 \oplus 172 = 7$$

$$z'_3 = z1 \oplus z2 \oplus z3 \oplus z5 \oplus z6 \oplus z8 = 69 \oplus 140 \oplus 8 \oplus 225 \oplus 9 \oplus 172 = 133$$

$$z'_4 = z2 \oplus z3 \oplus z4 \oplus z5 \oplus z6 \oplus z7 = 140 \oplus 8 \oplus 17 \oplus 225 \oplus 9 \oplus 146 = 239$$

$$z'_5 = z1 \oplus z2 \oplus z6 \oplus z7 \oplus z8 = 69 \oplus 140 \oplus 9 \oplus 146 \oplus 172 = 254$$

$$z'_6 = z2 \oplus z3 \oplus z5 \oplus z7 \oplus z8 = 140 \oplus 8 \oplus 225 \oplus 146 \oplus 172 = 91$$

$$z'_7 = z3 \oplus z4 \oplus z5 \oplus z6 \oplus z8 = 8 \oplus 17 \oplus 225 \oplus 9 \oplus 172 = 93$$

$$z'_8 = z1 \oplus z4 \oplus z5 \oplus z6 \oplus z7 = 69 \oplus 17 \oplus 225 \oplus 9 \oplus 146 = 46$$

$$z'_{(64)} = 6B07\ 85EF\ FE5B\ 5D2E$$

$$R_0 = L_1 \oplus F(R_1, k_1)$$

$$= 1050\ C4C6\ C56F\ 7209 \oplus 6B07\ 85EF\ FE5B\ 5D2E$$

$$= 7B57\ 4129\ 3B34\ 2F27$$

$$L_0 = 1F2A\ 2226\ 2232\ 2712$$

$$M_{(128)} = (L_{0(64)} \parallel R_{0(64)}) \oplus (kw_{1(64)} \parallel kw_{2(64)})$$

$$M_{(128)} = (1F2A\ 2226\ 2232\ 2712 \parallel 7B57\ 4129\ 3B34\ 2F27) \oplus (534B\ 5249\ 5053\ 4932 \parallel 3032\ 3448\ 5553\ 4E49)$$

$$M_{(128)} = 4C61\ 706F\ 7261\ 6E20\ 4B65\ 7561\ 6E67\ 616E$$

Setelah hasil plaintext didapatkan, kemudian plaintext hexadecimal dikonversikan ke dalam bentuk karakter yaitu Laporan Keuangan.

4.2. Hasil

Pada bab ini akan dijelaskan tampilan akhir hasil dari aplikasi yang telah dibuat, yang digunakan untuk memberikan gambaran yang jelas mengenai tampilan-tampilan yang terdapat pada Sistem Keamanan Data Informasi Keuangan

Pada SD Muhammadiyah 08 Medan, yang memanfaatkan Algoritma Kriptografi Camellia. Sehingga hasil implementasinya dapat dilihat sesuai dengan hasil program yang telah dibuat. Adapun hasil tampilan sistem tersebut adalah sebagai berikut:

4. Tampilan Halaman Form Login

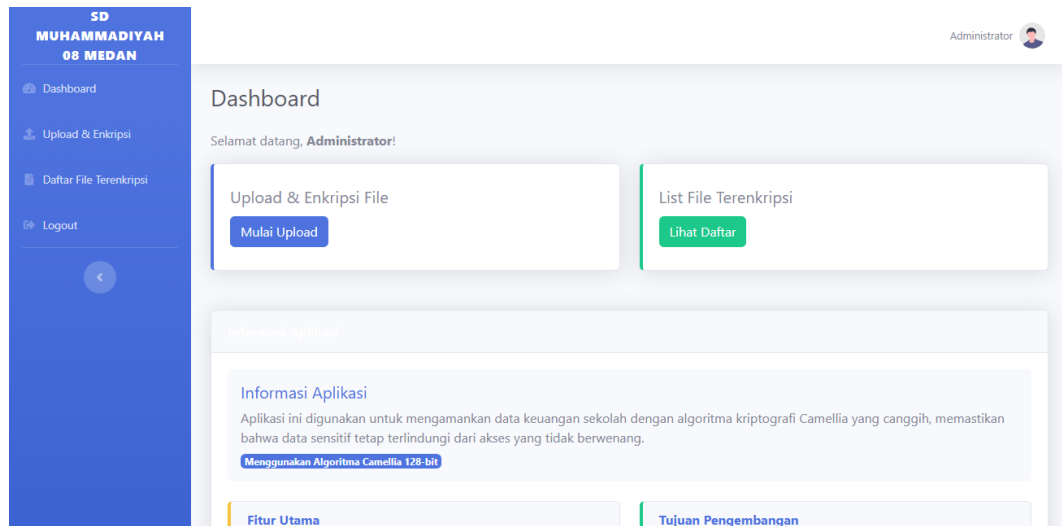
Tampilan halaman form login merupakan halaman awal ketika pengguna mengakses sistem. Pada halaman ini, pengguna diminta untuk memasukkan username dan password yang valid agar dapat masuk ke dalam sistem. Hasil tampilan halaman form login dapat dilihat pada gambar berikut:

The image shows a web-based login form titled "Login Admin". Below the title, it reads "Aplikasi Keamanan Data Keuangan Menggunakan Algoritma Camellia 128 bit". In the center is a circular logo with a red border, containing a green sun-like symbol and the text "SD MUHAMMADIYAH 08 MEDAN". Below the logo are two input fields: "Username" and "Password". Under these fields is a blue "Login" button. At the bottom of the form, there is a small copyright notice: "© 2025 SD Muhammadiyah 08 Medan". The entire form is enclosed in a blue rectangular border.

Gambar 4.1. Tampilan Halaman Form Login

5. Tampilan Halaman Dashboard

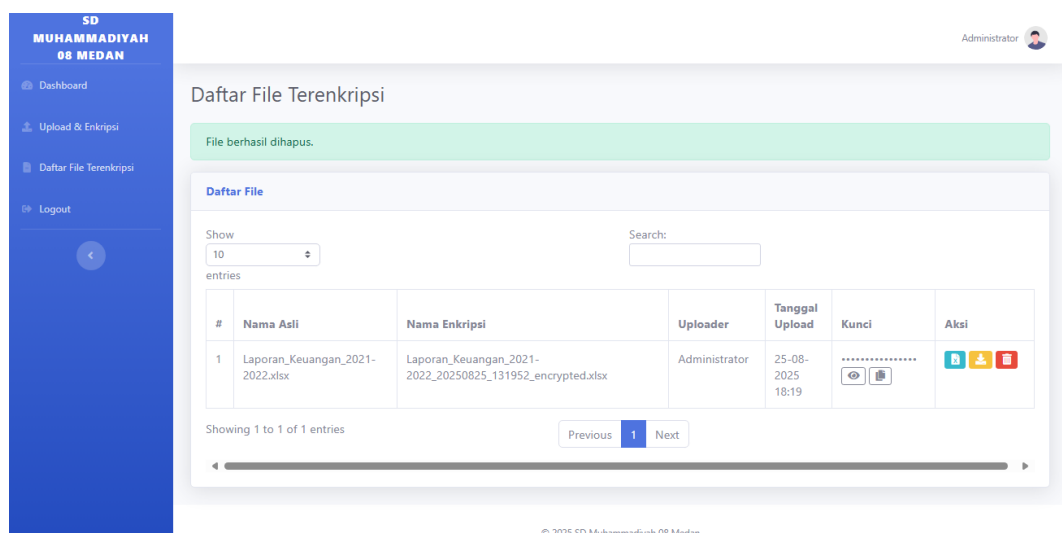
Tampilan halaman dashboard adalah tampilan utama setelah pengguna berhasil login. Pada halaman ini ditampilkan menu-menu utama yang memudahkan pengguna dalam mengakses fitur sistem. Hasil tampilan halaman dashboard dapat dilihat pada gambar berikut:



Gambar 4.2. Tampilan Halaman Dashboard

6. Tampilan Halaman Daftar File Terenkripsi

Halaman ini menampilkan daftar seluruh data keuangan sekolah yang telah terenkripsi. Pada halaman ini, pengguna dapat melihat file-file yang tersimpan dalam keadaan terenkripsi dan terdapat opsi untuk melakukan dekripsi kembali jika pengguna membutuhkan akses ke data asli. Hasil tampilan halaman daftar file terenkripsi dapat dilihat pada gambar berikut:



Gambar 4.3. Tampilan Halaman Daftar File Terenkripsi

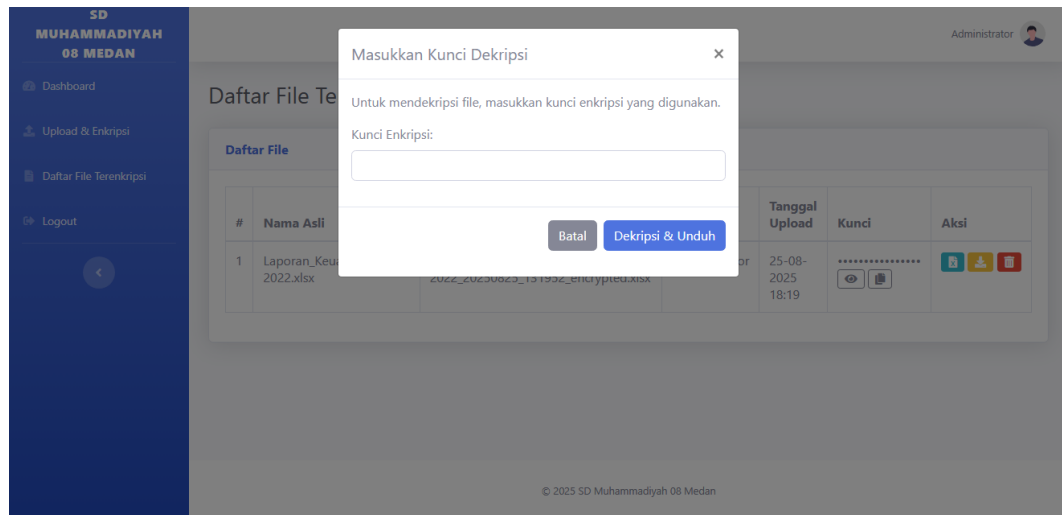
7. Tampilan Halaman Form Upload dan Enkripsi

Halaman form enkripsi digunakan untuk melakukan proses pengaman data dengan cara mengunggah file keuangan dan memasukkan kunci enkripsi. Sistem akan memproses file tersebut menggunakan algoritma Camellia sehingga file tersimpan dalam bentuk terenkripsi. Hasil tampilan halaman form enkripsi dapat dilihat pada gambar berikut:

Gambar 4.4. Tampilan Halaman Form Upload dan Enkripsi

8. Tampilan Halaman Form Dekripsi

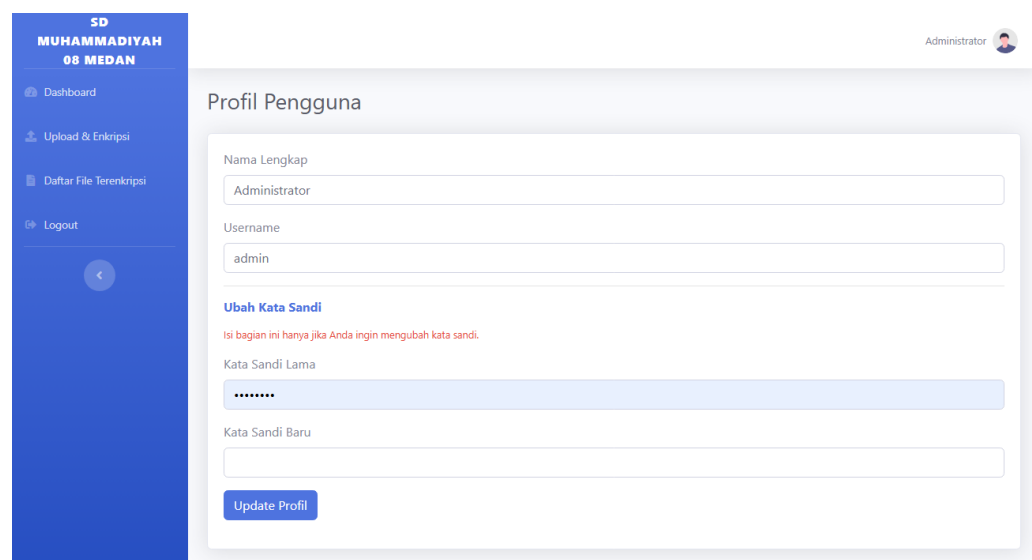
Halaman form dekripsi digunakan untuk mengembalikan file terenskripsi menjadi file asli. Pada halaman ini, pengguna perlu memilih file terenkripsi yang ingin dibuka dan memasukkan kunci enkripsi yang sesuai. Hasil tampilan halaman form dekripsi dapat dilihat pada gambar berikut:



Gambar 4.5. Tampilan Halaman Form Dekripsi

9. Tampilan Halaman Form Kelola Akun

Halaman informasi profil menampilkan detail pengguna yang sedang login, seperti nama lengkap dan username. Selain itu, pada halaman ini juga tersedia fitur untuk memperbarui informasi profil jika terjadi perubahan data pengguna. Hasil tampilan halaman form kelola akun dapat dilihat pada gambar berikut:



Gambar 4.6. Tampilan Halaman Form Kelola Akun

4.3. Pembahasan dan Uji Coba

Pada Tahap ini berisi analisis hasil penelitian dan uji coba untuk memastikan bahwa sistem berjalan sesuai dengan kebutuhan pengguna dan tujuan penelitian.

Data yang diperoleh diolah, dibandingkan dengan teori yang relevan, serta diinterpretasikan untuk menjawab rumusan masalah. Selain itu, dilakukan uji coba untuk memastikan bahwa sistem berfungsi dengan baik dan dapat dioperasikan dengan mudah oleh pengguna.

4.2.1. Pembahasan

Pembahasan ini menjelaskan mengenai perangkat keras (*hardware*) dan perangkat lunak (*software*) yang digunakan dalam penelitian atau pengembangan sistem Keamanan Data Informasi Keuangan Pada SD Muhammadiyah 08 Medan, yang memanfaatkan Algoritma Kriptografi Camellia. Adapun perangkat yang digunakan dalam penelitian ini, antara lain:

1. Perangkat Keras (*Hardware*)

Spesifikasi minimum laptop yang digunakan untuk menjalankan sistem adalah sebagai berikut:

- a. *Processor* minimal *intel core i3*.
- b. RAM minimal 4 GB.
- c. *Harddisk* atau SSD minimal 128 GB.

2. Perangkat Lunak (*Software*)

Perangkat lunak yang digunakan untuk pengembangan dan pengujian sistem adalah sebagai berikut:

- a. Sistem Operasi minimal Windows 7.
- b. *Browser Google Chrome* atau *Mozilla Firefox*.
- c. Microsoft Excel.

4.2.2. Uji Coba

Pada tahap uji coba akan dilakukan pengujian sistem untuk memastikan bahwa semua fitur berfungsi dengan baik dan memenuhi kebutuhan pengguna. Sistem yang telah dirancang akan uji menggunakan *blackbox testing* sebagai berikut:

1. Uji Coba Form Login Sistem

Bagian ini menguji fungsi form login untuk memastikan bahwa proses masuk ke sistem hanya dapat dilakukan oleh pengguna yang memiliki akun yang valid. Rincian uji coba dapat dilihat pada tabel berikut:

Tabel 4.1. *Blackbox Testing* Form Login Sistem

No	Skenario Pengujian	Input	Output Yang Diharapkan	Hasil Uji
1	User mengakses Aplikasi Keamanan Data	Membuka URL aplikasi melalui browser	Sistem akan menampilkan halaman login	Sesuai
2	User melakukan login dengan memasukkan username dan password benar	Username & Password Valid	Sistem akan mengarahkan ke halaman dashboard	Sesuai
3	User melakukan login dengan memasukkan username dan password salah	Username atau Password salah	Sistem akan menampilkan pesan error “Username tidak ditemukan!” atau “Password salah!”	Sesuai

2. Uji Coba Form Daftar File Terenkripsi

Bagian ini menguji form daftar file terenkripsi untuk memverifikasi bahwa sistem dapat menampilkan data keuangan dengan benar dan dapat melihat kunci enkripsi. Rincian uji coba dapat dilihat pada tabel berikut:

Tabel 4.2. Blackbox Testing Form Daftar File Terenkripsi

No	Skenario Pengujian	Input	Output Yang Diharapkan	Hasil Uji
1	Mengakses menu Daftar File Terenkripsi.	Klik Menu	Sistem menampilkan data keuangan dalam bentuk terenkripsi	Sesuai
2	User ingin melihat kunci enkripsi	Klik tombol mata (show) pada kolom kunci	Sistem menampilkan kunci enkripsi yang sebenarnya	Sesuai

3. Uji Coba Form Upload & Enkripsi

Bagian ini menguji form upload & enkripsi untuk memastikan file yang diunggah berhasil terenkripsi dengan benar menggunakan algoritma Camellia. Rincian uji coba dapat dilihat pada tabel berikut:

Tabel 4.3. Blackbox Testing Form Upload & Enkripsi

No	Skenario Pengujian	Input	Output Yang Diharapkan	Hasil Uji
1	User mengakses menu upload & enkripsi	Klik menu upload & enkripsi pada sistem	Sistem akan menampilkan halaman enkripsi	Sesuai

2	User mengunggah file dan memasukkan kunci enkripsi (128 bit)	File & Kunci Enkripsi	Sistem akan membangkitkan kunci, lalu melakukan proses enkripsi	Sesuai
---	--	-----------------------	---	--------

4. Uji Coba Form Dekripsi

Bagian ini menguji form dekripsi untuk memastikan file terenkripsi dapat dikembalikan ke format aslinya. Rincian uji coba dapat dilihat pada tabel berikut:

Tabel 4.4. *Blackbox Testing* Form Dekripsi

No	Skenario Pengujian	Input	Output Yang Diharapkan	Hasil Uji
1	User mengakses menu Daftar File Terenkripsi.	Klik menu Daftar File Terenkripsi pada sistem	Sistem akan menampilkan halaman Dekripsi	Sesuai
2	User mencari file yang ingin didekripsi, memilih file, memasukkan kunci yang sesuai	Masukkan kunci yang benar untuk dekripsi lalu klik button Dekripsi & unduh	Sistem akan melakukan proses dekripsi dan terunduh	Sesuai
3	User mencari file yang ingin didekripsi, memilih file, memasukkan kunci yang sesuai, lalu klik tombol dekripsi	Masukkan kunci yang salah untuk dekripsi	Sistem menampilkan pesan error “Kunci dekripsi salah”	Sesuai

5. Uji Coba Form Kelola Akun

Bagian ini menguji form kelola akun untuk memastikan apakah pengguna dapat memperbarui informasi profilnya dengan benar dan tersimpan di database.

Rincian uji coba dapat dilihat pada tabel berikut:

Tabel 4.5. *Blackbox Testing* Form Kelola Akun

No	Skenario Pengujian	Input	Output Yang Diharapkan	Hasil Uji
1	User mengakses menu kelola akun	Klik header menu sistem, lalu klik menu kelola akun	Sistem akan menampilkan halaman kelola akun	Sesuai
2	User edit username atau password	Masukkan username atau password yang baru	Data berhasil diperbarui dan sistem mengupdate database	Sesuai

6. Uji Coba Logout Sistem

Bagian ini menguji logout sistem untuk memastikan pengguna dapat keluar dari sistem dengan aman tanpa menyisakan sesi aktif. Rincian uji coba dapat dilihat pada tabel berikut:

Tabel 4.6. *Blackbox Testing* Logout Sistem

No	Skenario Pengujian	Input	Output Yang Diharapkan	Hasil Uji
1	User mengakses menu header	Klik header menu sistem	Sistem akan menampilkan dropdown menu	Sesuai

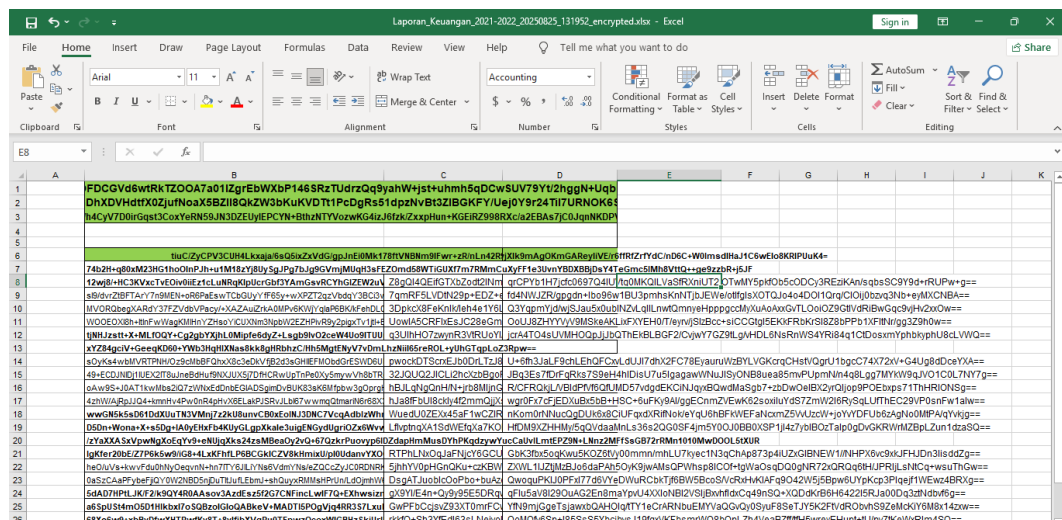
2	User klik menu logout	Klik menu logout pada dropdown	Sistem menghapus session dan mengarahkan ke halaman login user	Sesuai
---	-----------------------	--------------------------------	--	--------

4.2.3. Hasil Pengujian Sistem

Pengujian dilakukan untuk memastikan bahwa sistem berfungsi dengan baik dan memenuhi kebutuhan pengguna. Hasil pengujian sistem menunjukkan bahwa aplikasi telah berjalan sesuai dengan tujuan perancangan. Seluruh fitur utama seperti login, pengelolaan data keuangan, enkripsi, dekripsi, pengelolaan akun, serta logout dapat berfungsi sebagaimana mestinya.

Proses enkripsi terhadap file data keuangan berjalan dengan baik. Pada tahap ini, file asli yang berbentuk excel dienkripsi menggunakan algoritma Camellia dengan panjang kunci 128 bit. Proses enkripsi menghasilkan sebuah file baru yang dapat diunduh dengan format excel yang tidak dapat dibaca secara langsung. Hal ini membuktikan bahwa data telah berhasil dikonversi dengan baik.

Contoh hasil enkripsi file dapat dilihat pada gambar berikut:



Gambar 4.7. Contoh Hasil Enkripsi File

Dapat dilihat pada gambar tersebut data asli diubah menjadi karakter yang tidak dapat dibaca. Selain itu, dilakukan pengujian proses dekripsi dengan menggunakan file terenkripsi. Hasil dekripsi menunjukkan bahwa sistem berhasil mengembalikan file ke bentuk aslinya tanpa ada perubahan isi maupun format. Hal ini membuktikan bahwa sistem mampu menjaga kerahasiaan sekaligus memastikan integritas data keuangan tetap terjaga. Dengan demikian, hasil pengujian menunjukkan bahwa proses enkripsi dan dekripsi pada algoritma Camellia pada data keuangan telah berhasil dilakukan.

4.4. Kelebihan dan Kekurangan Sistem

Setiap sistem yang dibangun tentu memiliki kelebihan dan kekurangan, berikut kelebihan dan kekurangan dari sistem keamanan data informasi keuangan yang diimplementasikan menggunakan algoritma Camellia.

4.3.1. Kelebihan Sistem

Sistem keamanan data informasi keuangan ini memiliki beberapa kelebihan, antara lain:

1. Dengan menerapkan algoritma kriptografi Camellia, data keuangan sekolah dapat terenkripsi dengan baik, sehingga data keuangan terlindungi dari akses yang tidak sah
2. Antarmuka aplikasi dirancang agar mudah digunakan, sehingga pengguna dengan berbagai tingkat pemahaman teknologi dapat mengoperasikan sistem dengan baik.
3. Proses enkripsi dan dekripsi berhasil dilakukan tanpa mengubah isi maupun format file asli, sehingga data keuangan tetap konsisten.

4. Sistem berbasis web sehingga memudahkan pengguna dalam mengakses tanpa perlu melakukan instalansi aplikasi tambahan.

4.3.2. Kekurangan Sistem

Meskipun memiliki beberapa kelebihan, sistem ini juga memiliki beberapa kekurangan, antara lain:

1. Hasil enkripsi menggunakan algoritma kriptografi Camellia pada sistem dibungkus dengan fungsi BASE64 bawaan PHP. Hal ini dilakukan untuk mencegah karakter heksadesimal yang tidak terbaca oleh komputer. Tanpa pembungkusan ini, hasil dekripsi file Excel dapat menghasilkan nilai yang tidak valid atau "false".
2. Sistem ini sangat membutuhkan akses internet karena seluruh proses berjalan pada server.
3. Sistem saat ini hanya menggunakan kunci 128 bit, belum memanfaatkan variasi panjang kunci lainnya.

BAB V

KESIMPULAN DAN SARAN

5.1. Kesimpulan

Berdasarkan hasil pembahasan dan uji coba yang telah dilakukan, dapat disimpulkan beberapa hal mengenai sistem yang telah dibangun, yaitu:

1. Sistem keamanan data informasi keuangan yang dibangun menggunakan algoritma kriptografi Camellia dapat diimplementasikan dengan baik dan berfungsi sesuai dengan tujuan penelitian.
2. Sistem telah berhasil melakukan proses enkripsi terhadap data keuangan dalam format excel menjadi file terenkripsi yang tidak dapat dibaca. Sebaliknya, proses dekripsi mampu mengembalikan file terenkripsi menjadi file asli tanpa ada perubahan isi maupun format file.
3. Sistem yang dibangun memiliki antarmuka yang sangat sederhana dan mudah digunakan oleh user (*user-friendly*).
4. Dengan penerapan algoritma kriptografi Camellia, sistem mampu menjaga kerahasiaan, integritas, dan ketersediaan data keuangan, sehingga dapat menjadi solusi untuk mengurangi risiko kebocoran atau manipulasi data.
5. File yang digunakan dalam sistem ini masih terbatas pada format Excel, sehingga sistem belum mendukung jenis file lainnya.

5.2. Saran

Untuk menyempurnakan sistem yang telah dibangun, maka penulis memberikan beberapa saran sebagai berikut:

1. Penulis berharap pihak sekolah SD Muhammadiyah 08 medan nantinya dapat menggunakan sistem ini dengan baik sesuai ketentuan yang telah diberikan.
2. Pada pengembangan selanjutnya, sistem diharapkan dapat mendukung penggunaan panjang kunci 192 bit atau 256 bit sehingga tersedia pilhan panjang kunci sesuai kebutuhan keamanan.
3. Pada pengembangan selanjutnya, Sistem diharapkan dapat dikembangkan untuk mendukung pengamanan berbagai format file selain excel, seperti PDF dan Word.
4. Penulis berharap dimasa mendatang, banyak sistem keamanan yang dibangun dengan memanfaatkan algoritma kriptografi Camellia.

DAFTAR PUSTAKA

- Alfirdaus, M. H., Tahir, M., Dewanti, N. E., Ardianto, R., Azurah, N. N., & Cahyono, N. F. (2023). Perancangan Aplikasi Enkripsi Deskripsi Menggunakan Metode Caesar Chiper Berbasis Web. *Jurnal Teknik Mesin, Industri, Elektro Dan Informatika*, 2(2), 64–76.
- Ani, H., & Nasution, S. D. (2020). *Implementasi Algoritma Camellia Dalam Penyandian Pesan Sms Pada Telepon Seluler. 1.*
- Aoki, K., Ichikawa, T., Kanda, M., Matsui, M., Moriai, S., Nakajima, J., & Tokita, T. (N.D.). *Camellia: A 128-Bit Block Cipher Suitable For Multiple Platforms-Design And Analysis.*
- Aoki, K., Ichikawa, T., Kanda, M., Matsui, M., Moriai, S., Nakajima, J., & Tokita, T. (2000). Specification Of Camellia-A 128-Bit Block Cipher. *Specification Version, 2.*
- Arief, S. F., & Sugiarti, Y. (2022). Literature Review: Analisis Metode Perancangan Sistem Informasi Akademik Berbasis Web. *Jurnal Ilmiah Ilmu Komputer Fakultas Ilmu Komputer Universitas Al Asyariah Mandar*, 8(2), 87–93.
- Aryanto, M. B., Tahir, M., Devita, S. I., Mustofa, Z. N., Ainiyah, Q., & Sundoro, S. (2023). Implementasi Enkrip Dan Dekrip File Menggunakan Metode Advance Encryption Standard (Aes-128). *Jurnal Ilmiah Sistem Informasi Dan Ilmu Komputer*, 3(1), 89–104.
- Cristy, N., & Riandari, F. (2021). Implementasi Metode Advanced Encryption Standard (Aes 128 Bit) Untuk Mengamankan Data Keuangan. *Jurnal Ilmu Komputer Dan Sistem Informasi (Jikoms)*, 4(2), 75–85.

- Damanik, B. (2021). Rancangan Sistem Informasi Smp Negeri 1 Tuhemberua Kabupaten Nias Utara Menggunakan Php Codeigniter. *Jurnal Mahajana Informasi*, 6(1), 6–15.
- Fauzan, A., Mufti, M., Ferdiansyah, F., & Purwanto, P. (2023). Implementasi Advanced Encryption Standard (Aes-128) Untuk Aplikasi Keamanan File Pada Yayasan Perhimpunan Inti. *Prosiding Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (Senafiti)*, 2(1), 126–133.
- Febrianto, R., & Waluyo, S. (2023). Implementasi Algoritme Kriptografi Advanced Encryption Standard (Aes-256) Untuk Mengamankan Database Penilaian Karyawan Pada Kjpp Ndr. *Bit (Fakultas Teknologi Informasi Universitas Budi Luhur)*, 20(1), 44–49.
- Ferdy Riza, Muttaqin, Mahdianta Pandia, Sudirman, Fera Damayanti, Mufida Khairani, Rosyidah Siregar, Pitrasacha Adytia, Wahyuni, Tenku Mohd Diansyah Janner Simarmata, & Muharman Lubis. (2024). *Pengantar Ilmu Kriptografi* (Matias Julyus Fika Sirait, Ed.; Cetakan 1, Vol. 7). Yayasan Kita Menulis.
- Galih, A. P. (2020). Keamanan Informasi (Information Security) Pada Aplikasi Perpustakaan Ipusnas. *Al Maktabah*, 5(1), 9–17.
- Hasibuan, Y. W., Isnarto, I., & Veronica, R. B. (2022). Perancangan Dan Implementasi Aplikasi Kriptografi Algoritma Hill Cipher Dalam Dekripsi Enkripsi Data Keuangan Nasabah Bank Sampoerna Menggunakan Kode Ascii. *Unnes Journal Of Mathematics*, 11(1), 54–68.

- Hidayah, A., & Yani, A. (2019). Membangun Website Sma Pgri Gunung Raya Ranau Menggunakan Php Dan Mysql. *Jtim: Jurnal Teknik Informatika Mahakarya*, 2(2), 41–52.
- Husaini, F., Pardede, A. M. H., & Gultom, I. (2022). Penerapan Enkripsi Menggunakan Metode Elgamal Guna Meningkatkan Keamanan Data. *Juki: Jurnal Komputer Dan Informatika*, 4(1), 67–73.
- Hutabri, E., & Putri, A. D. (2019). Perancangan Media Pembelajaran Interaktif Berbasis Android Pada Mata Pelajaran Ilmu Pengetahuan Sosial Untuk Anak Sekolah Dasar. *Jurnal Sustainable: Jurnal Hasil Penelitian Dan Industri Terapan*, 8(2), 57–64.
- Jamaludin, J., & Romindo, R. (2019). Sistem Informasi Akademik Berbasis Web Menggunakan Metode Waterfall Pada Sma Kemala Bhayangkari I Medan. *Semantika (Seminar Nasional Teknik Informatika)*, 2(1), 17–27.
- Lengkong, C. M., Sengkey, R., & Sugiarso, B. A. (2019). Sistem Informasi Pariwisata Berbasis Web Di Kabupaten Minahasa. *Jurnal Teknik Informatika*, 14(1), 15–20.
- Malau, E. P. (2019). Pengamanan Aplikasi Menggunakan Algoritma Camelia. *Jurnal Informatika Kaputama (Jik)*, 3(1), 44–50.
- Mariko, S. (2019). Aplikasi Website Berbasis Html Dan Javascript Untuk Menyelesaikan Fungsi Integral Pada Mata Kuliah Kalkulus. *Jurnal Inovasi Teknologi Pendidikan*, 6(1), 80–91.
- Murdowo, S. (2020). Manual Perhitungan Menggunakan Kriptografi Klasik Playfair Chiper. *Jurnal Ilmiah Infokam*, 16(1).

- Permatasari, A., & Suhendi, S. (2020). Rancang Bangun Sistem Informasi Pengelolaan Talent Film Berbasis Aplikasi Web. *Jurnal Informatika Terpadu*, 6(1), 29–37.
- Porman Malau, E. (2019). Pengamanan Aplikasi Menggunakan Algoritma Camelia. In *Jik* (Vol. 3, Issue 1).
- Pratama, Y., Ayassy, B. M., Hidayatullah, C., Sinaga, F. P., & Zy, A. T. (2025). Kriptografi Klasik Dan Keamanan Dasar: Implementasi Kasir Restoran Dengan Pendekatan Metode Caesar Cipher. *Jati (Jurnal Mahasiswa Teknik Informatika)*, 9(2), 1966–1971.
- Putra, N. B. N., Raihana, F. A., Mondong, W. M. A., & Kardian, A. R. (2023). Analisis Enkripsi Kriptografi Asimetris Algoritma Rsa Berbasis Pemrograman Batch Pada Media Flashdisk. *Jurasik (Jurnal Riset Sistem Informasi Dan Teknik Informatika)*, 8(1), 142–154.
- Ratu, A. U. B. N., Rada, Y., & Uly, H. Y. P. (2024). Sistem Informasi Geografis Pemetaan Pariwisata Pada Kabupaten Sumba Timur Berbasis Web. *Jati (Jurnal Mahasiswa Teknik Informatika)*, 8(4), 7541–7546.
- Romandhon, M. G. A., Junaidi, A., & Sihananto, A. N. (2024). Penerapan Hybrid Cryptography Menggunakan Camellia Dan Dual Modulus Rsa Pada Pertukaran File. *Jurnal Informatika Dan Teknik Elektro Terapan*, 12(3s1).
- Rosaly, R., & Prasetyo, A. (2019). *Pengertian Flowchart Beserta Fungsi Dan Simbol-Simbol Flowchart Yang Paling Umum Digunakan*.
- Saragi, D. R., Gultom, J. M., Tampubolon, J. A., & Gunawan, I. (2020). Pengamanan Data File Teks (Word) Menggunakan Algoritma Rc4. *Jurnal Sistem Komputer Dan Informatika (Json) Hal*, 114, 119.

- Sasono, D. M. A., Tahir, M., Angel, F., Azizah, M., Utami, L. F., & Septiana, N. (2023). Perbandingan Kriptography Klasik Caesar Cipher Dengan Kriptography Modern Aes Dalam Tingkat Keamanan Jaringan Komputer. *Jurnal Informasi, Sains Dan Teknologi*, 6(1), 72–77.
- Sulistiati, T., Yuliansyah, F., Romzi, M., & Aryani, R. (2020). Membangun Website Toko Online Pempek Nthree Menggunakan Php Dan Mysql. *Jtim: Jurnal Teknik Informatika Mahakarya*, 3(1), 35–44.
- Syahrani, M. (2020). Membangun Kepercayaan Data Dalam Penelitian Kualitatif. *Primary Education Journal (Pej)*, 4(2), 19–23.
- Tarigan, R. A., Ramadhan, P. S., & Ginting, E. F. (2021). Implementasi Kriptografi Untuk Keamanan Data Keuangan Dengan Metode Rsa (Rivest Shamir Adleman) Pada Smp It Ar Rasyid. *Jurnal Cyber Tech*, 4(7).

LAMPIRAN

1. Surat Penetapan Dosen Pembimbing


MAJELIS PENDIDIKAN TINGGI PENELITIAN & PENGEMBANGAN PIMPINAN PUSAT MUHAMMADIYAH
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
FAKULTAS ILMU KOMPUTER DAN TEKNOLOGI INFORMASI
UMSU Terakreditasi A Berdasarkan Keputusan Badan Akreditasi Nasional Perguruan Tinggi No. 89/SK/BAN-PT/Akred/PT/III/2019
Pusat Administrasi: Jalan Mukhtar Basri No. 3 Medan 20238 Telp. (061) 6622400 - 66224567 Fax. (061) 6625474 - 6631003
Website: <http://www.umsu.ac.id> Email: info@umsu.ac.id Facebook: [umsuMEDAN](#) Instagram: [umsuMEDAN](#) Twitter: [umsuMEDAN](#) YouTube: [umsuMEDAN](#)

PENETAPAN DOSEN PEMBIMBING
PROPOSAL/SKRIPSI MAHASISWA
NOMOR : 22/IL.3-AU/UMSU-09/F/2025

Assalamu'alaikum Warahmatullahi Wabarakatuh

Dekan Fakultas Ilmu Komputer dan Teknologi Informasi Universitas Muhammadiyah Sumatera Utara, berdasarkan Persetujuan permohonan judul penelitian Proposal / Skripsi dari Ketua / Sekretaris.

Program Studi : Sistem Informasi
Pada tanggal : 03 Januari 2025

Dengan ini menetapkan Dosen Pembimbing Proposal / Skripsi Mahasiswa.

Nama : Asma'ul Husniah
NPM : 2109010105
Semester : VII (Tujuh)
Program studi : Sistem Informasi
Judul Proposal / Skripsi : Analisis dan Implementasi Sistem Informasi Keuangan Menggunakan Zachman Framework Pada Yayasan Mentari Meraki Asa.

Dosen Pembimbing : Ferdy Riza, S.T, M.Kom.

Dengan demikian di izinkan menulis Proposal / Skripsi dengan ketentuan

1. Penulisan berpedoman pada buku panduan penulisan Proposal / Skripsi Fakultas Ilmu Komputer dan Teknologi Informasi UMSU
2. Pelaksanaan Sidang Skripsi harus berjarak 3 bulan setelah dikeluarkannya Surat Penetapan Dosen Pembimbing Skripsi.
3. **Proyek Proposal / Skripsi** dinyatakan " **BATAL** " bila tidak selesai sebelum Masa Kadaluaarsa tanggal : **03 Januari 2026**
4. Revisi judul.....

Wassalamu'alaikum Warahmatullahi Wabarakatuh.

Ditetapkan di : Medan
 Pada Tanggal : 03 Rajab 1446 H
 03 Januari 2025 M

a.n.Dekan
 Wakil Dekan I

Hanih Matmana, S.T., M.Kom.
 NIDN : 0121119102




Cc. File





2. Lembar Perubahan Judul



UMSU

Unggul | Cerdas | Terpercaya

Bila masyarakat akan terdampak, akan ditanggulangi

MAJELIS PENDIDIKAN TINGGI PENELITIAN & PENGEMBANGAN PIMPINAN PUSAT MUHAMMADIYAH

UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA

FAKULTAS ILMU KOMPUTER DAN TEKNOLOGI INFORMASI

UMSU Terakreditasi A Berdasarkan Keputusan Badan Akreditasi Nasional Perguruan Tinggi No. 99/SK/BAN-PT/Akred/PT/III/2019

Pusat Administrasi: Jalan Mukhtar Basri No. 3 Medan 20238 Telp. (061) 6622400 - 66224567 Fax. (061) 6625474 - 6631003

<https://fkti.umsu.ac.id>

fkti@umsu.ac.id

[umsu.medan](https://www.facebook.com/umsu.medan)

[umsu.medan](https://www.instagram.com/umsu.medan)

[umsu.medan](https://www.tiktok.com/@umsu.medan)

[umsu.medan](https://www.youtube.com/channel/UC...)

PERUBAHAN TOPIK/JUDUL PENELITIAN

Nomor agenda	:
Tanggal persetujuan	: 30 Januari 2025
Topik yang disetujui Program Studi	: Analisis dan Implementasi Sistem Informasi Keuangan Menggunakan Zachman Framework Pada Yayasan Mentari Meraki Asa
Nama Dosen pembimbing	: Ferdy Riza, S. T, M.Kom
Judul yang disetujui Dosen Pembimbing	: Analisis dan Implementasi Sistem Keamanan Data Informasi Keuangan Menggunakan Algoritma Camellia Pada SD Muhammadiyah 08 Medan

Medan, 30 Januari 2025

Disahkan oleh
Ketua Proram Studi
Sistem Informasi

Persetujuan
Dosen Pembimbing

Martiano S.Pd, S.Kom., M.Kom

Ferdy Riza, S. T, M.Kom

3. Lembar Bimbingan Skripsi



MAJELIS PENDIDIKAN TINGGI PENELITIAN & PENGEMBANGAN PIMPINAN PUSAT MUHAMMADIYAH
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
FAKULTAS ILMU KOMPUTER DAN TEKNOLOGI INFORMASI

UMSU Terakreditasi A Berdasarkan Keputusan Badan Akreditasi Nasional Perguruan Tinggi No. 89/SK/BAN-PT/Akred/PT/III/2019
 Pusat Administrasi: Jalan Mukhtar Basri No. 3 Medan 20238 Telp. (061) 6622400 - 66224567 Fax. (061) 6625474 - 6631003
<https://fkt.umsu.ac.id> fkt@umsu.ac.id [umsuMEDAN](https://www.facebook.com/umsuMEDAN) [umsuMEDAN](https://www.instagram.com/umsuMEDAN) [umsuMEDAN](https://www.youtube.com/umsuMEDAN) [umsuMEDAN](https://www.tiktok.com/umsuMEDAN)

Unggul | Cerdas | Terpercaya

Berita Acara Pembimbingan Proposal

Nama Mahasiswa : Asma'ul Husniah Program Studi : Sistem Informasi
 NPM : 2109010105 Konsentrasi :
 Nama Dosen Pembimbing : Ferdy Riza, S. T, M.Kom Judul Penelitian :

Tanggal Bimbingan	Hasil Evaluasi	Paraf Dosen
30/01/25	Ganti Judul	<i>[Signature]</i>
12/02/25	Perbaiki latar belakang, sitasi, dan pembahasan	<i>[Signature]</i>
24/02/25	Kec bab I -> lanjut bab II	<i>[Signature]</i>
02/05/25	Perbaiki latar belakang dan sitasi	<i>[Signature]</i>
16/06/25	latar belakang dan pembahasan, dan tujuan	<i>[Signature]</i>
19/06/25	lanjut bab II	<i>[Signature]</i>

Diketahui oleh :

Ketua Program Studi
Sistem Informasi

(.....)

Medan,.....

Disetujui oleh :

Dosen Pembimbing

[Signature]

(.....)



MAJELIS PENDIDIKAN TINGGI PENELITIAN & PENGEMBANGAN PIMPINAN PUSAT MUHAMMADIYAH
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
FAKULTAS ILMU KOMPUTER DAN TEKNOLOGI INFORMASI

UMSU Terakreditasi A Berdasarkan Keputusan Badan Akreditasi Nasional Perguruan Tinggi No. 89/SK/BAN-PT/Akred/PT/BB/2019

Pusat Administrasi: Jalan Mukhtar Basri No. 3 Medan 20238 Telp. (061) 6622400 - 66224567 Fax (061) 6625474 - 6631003

<https://fkti.umsu.ac.id>

fkti@umsu.ac.id

[f umsumedan](#)

[u umsumedan](#)

[t umsumedan](#)

[u umsumedan](#)

Berita Acara Pembimbingan Proposal

Nama Mahasiswa : Asma'ul Husniah Program Studi : Sistem Informasi
 NPM : 2109010105 Konsentrasi :
 Nama Dosen Pembimbing : Ferdy Riza, S. T, M.Kom Judul Penelitian : Analisis dan Implementasi
 Sistem Keamanan Data Informasi
 Keuangan Pada SD Muhammadiyah
 Medan

Tanggal Bimbingan	Hasil Evaluasi	Paraf Dosen
25/06/25	Pembahasan Bab II	
04/06/25	lanjut bab III	
16/07/25	Tunjukkan prosedur rutin - rutin dengan	
18/07/25	ACC sempurna seminar	

Diketahui oleh :
 Ketua Program Studi
 Sistem Informasi

(.....)

Medan,

Disetujui oleh :
 Dosen Pembimbing

(Ferdy Riza, S.T, M.Kom)



UMSU
Unggul | Cerdas | Terpercaya

UMSU Terakreditasi A Berdasarkan Keputusan Badan Akreditasi Nasional Perguruan Tinggi No. 89/SK/BAH-PT/Akred/PT/16/2019
Pusat Administrasi: Jalan Mukhtar Basri No. 3 Medan 20238 Telp. (061) 6622400 - 66224567 Fax. (061) 6625474 - 6631003

MAJELIS PENDIDIKAN TINGGI PENELITIAN & PENGEMBANGAN PIMPINAN PUSAT MUHAMMADIYAH
UNIVERSITAS MUHAMMADIYAH SUMATERA UTARA
FAKULTAS ILMU KOMPUTER DAN TEKNOLOGI INFORMASI

UMSU Terakreditasi A Berdasarkan Keputusan Badan Akreditasi Nasional Perguruan Tinggi No. 89/SK/BAH-PT/Akred/PT/16/2019
Pusat Administrasi: Jalan Mukhtar Basri No. 3 Medan 20238 Telp. (061) 6622400 - 66224567 Fax. (061) 6625474 - 6631003

Website: www.umsu.ac.id

Email: info@umsu.ac.id

Facebook: [umsu.medan](https://www.facebook.com/umsu.medan)

Instagram: [umsu.medan](https://www.instagram.com/umsu.medan)

Twitter: [umsu.medan](https://twitter.com/umsu.medan)

YouTube: [umsu.medan](https://www.youtube.com/umsu.medan)

Berita Acara Pembimbingan Proposal

Nama Mahasiswa : Asma'ul Husniah Program Studi : Sistem Informasi
NPM : 2109010105 Konsentrasi :
Nama Dosen Pembimbing : Ferdy Riza, S. T, M.Kom Judul Penelitian : Analisis dan Implementasi
Sistem Keamanan Data Informasi
Keuangan Pada SD Muhammadiyah
Medan

Tanggal Bimbingan	Hasil Evaluasi	Paraf Dosen
30-08-25	Perbaiki sub bab IV	
02-09-25	ACC Sidang	

Medan, 29 Agustus 2025

Diketahui oleh :
Ketua Program Studi
Sistem Informasi

(.....)

Disetujui oleh :
Dosen Pembimbing

(.....)

4. LoA Jurnal



LETTER OF ACCEPTANCE (LoA)

Kepada Yth Bpk/Ibu/Sdr

Asma'ul Husniah, Ferdy Riza

Di

Tempat

Dengan ini kami sampaikan bahwa naskah dengan rincian berikut dinyatakan diterima untuk diterbitkan di sudo Jurnal Teknik Informatika, ISSN: 2829-7342 (Online) terbitan Volume 4 Nomor 3 Edisi September 2025.

Judul	Analisis Dan Implementasi Sistem Keamanan Data Informasi Keuangan Menggunakan Algoritma Camellia Pada SD Muhammadiyah 08 Medan
Penulis	Asma'ul Husniah, Ferdy Riza
Correspondent Email	ferdyriza@umsu.ac.id

Demikianlah surat keterangan ini kami buat untuk dapat digunakan seperlunya.



Medan, 07 Oktober 2025

Editor in Chief

Oris Krianto Sulaiman, S.T., M.Kom.

sudo Jurnal Teknik Informatika
Ilmu Bersama Center
Email: jurnalsudo@gmail.com



sudo Jurnal Teknik Informatika is licensed under a
[Creative Commons Attribution-ShareAlike 4.0 International License](https://creativecommons.org/licenses/by-sa/4.0/)

5. Hasil Cek Turnitin

Skripsi Asma'ul Husniah.docx			
ORIGINALITY REPORT			
21%	15%	14%	6%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS
PRIMARY SOURCES			
1	ejurnal.seminar-id.com Internet Source	5%	
2	Daniel Denning. "A Key Agile 17.4 Gbit/sec Camellia Implementation", Lecture Notes in Computer Science, 2004 Publication	3%	
3	Wu Wenling. "Collision Attack and Pseudorandomness of Reduced-Round Camellia", Lecture Notes in Computer Science, 2004 Publication	3%	
4	budi.insan.co.id Internet Source	2%	
5	Submitted to Universitas Muhammadiyah Sumatera Utara Student Paper	1%	
6	docplayer.info Internet Source	1%	
7	Submitted to Universitas Putera Batam Student Paper	1%	
8	eprint.iacr.org Internet Source	1%	
9	ojs.umrah.ac.id Internet Source	1%	

10	jurnal.larisma.or.id Internet Source	<1 %
11	info.isl.ntt.co.jp Internet Source	<1 %
12	elib.pnc.ac.id Internet Source	<1 %
13	Submitted to Universitas Musamus Merauke Student Paper	<1 %
14	openlibrarypublications.telkomuniversity.ac.id Internet Source	<1 %
15	repository.umsu.ac.id Internet Source	<1 %
16	ejournal.fikom-unasman.ac.id Internet Source	<1 %
17	Submitted to UIN Syarif Hidayatullah Jakarta Student Paper	<1 %
18	smart.stmikplk.ac.id Internet Source	<1 %
19	doku.pub Internet Source	<1 %
20	Submitted to Universitas Budi Luhur Student Paper	<1 %
21	repo.darmajaya.ac.id Internet Source	<1 %
22	repository.bsi.ac.id Internet Source	<1 %
23	repository.teknokrat.ac.id Internet Source	<1 %