Management of Information System Journal
Vol 3, No 2, Maret 2025, Hal. 21 - 37
ISSN: 2964-9455 (media online)
DOI: 10.47065/mis.v2i3. 1919
https://journal.fkpt.org/index.php/MIS

Implementasi Algoritma Seal Pada Pengamanan Data Penjualan Tiket PT. Amanda Tour & Travel

Suwondo

Mahasiswa Program Studi Teknik Informatika Universitas Budi Darma Medan
Email : suwondorevolusi2210@gmail.com

Abstrak- *SEAL merupakan salah satu jenis stream cipher, yaitu memproses unit atau input data, pesan atau informasi pada satu saat. Unit atau data pada umumnya sebuah byte. Dengan cara ini enkripsi atau dekripsi dapat dilaksanakan pada panjang yang variabel. Algoritma ini tidak harus menunggu sejumlah input data, pesan atau informasi tertentu sebelum diproses, atau menambahkan byte tambahan untuk mengenkrip. Teknis penyandian yang dipergunakan pada algoritma SEAL adalah dengan memanfaatkan enkripsi dan deskripsi setiap data yang diinput, untuk mengamnakan data pelanggan pada PT. Amanda Tour & Travel yang merupakan salah satu perusahaan travel di medan yang menyediakan layanan pemesanan tiket pesawat. Untuk pembuktian hasil enkripsi soal ditunjukkan dengan akses langsung ke dalam system dengan menerapkan algoritma seal yang tersimpan pada database menggunakan antar muka akses database. Algoritma kriptografi yang akan digunakan dalam pengamanan PT. Amanda Tour & Travel adalah algoritma kriptografi simetris dan bersifat stream cipher sehingga data hasil enkripsi (cipherteks) mempunyai ukuran yang sama dengan data asli (plainteks). Teknik kriptografi simetris dipilih karena diharapkan dengan algoritma ini proses enkripsi– dekripsi data dapat mengamankan data pelanggan dengan baik.*
Kata Kunci : *Algoritma Seal, Pengamanan Data, kriptografi.*

Abstract*- SEAL is a type of stream cipher, which processes units or input data, messages or information at one time. Units or data are generally bytes. In this way, encryption or decryption can be performed on variable lengths. This algorithm does not have to wait for a certain amount of input data, messages or information before processing, or add additional bytes for encryption. The encryption technique used in the SEAL algorithm is to encrypt and decrypt each input data to secure customer data at PT. Amanda Tour & Travel, a travel company in Medan that provides airline ticket booking services. To prove the encryption results, direct access to the system is demonstrated by applying the SEAL algorithm stored in the database using a database access interface. The cryptographic algorithm to be used in securing PT. Amanda Tour & Travel is a symmetric cryptographic algorithm and a stream cipher, so that the encrypted data (ciphertext) has the same size as the original data (plaintext). Symmetric cryptography was chosen because it is expected that this algorithm will securely encrypt and decrypt customer data.*
Keywords: Seal Algorithm, Data Security, Cryptography.

1. PENDAHULUAN

1.1 Latar Belakang

Arus informasi yang semakin marak untuk menggunakan media digital, dalam bentuk file memungkinkan orang lain untuk bisa membuka data yang bukan haknya. Rahasia perusahaan, data-data penting menjadi sangat berarti untuk dilakukan proses enkripsi. Hal ini sangat membantu bagi pihak-pihak yang berkepentingan dengan data untuk melindungi datanya dari orang pihak-pihak lain.

Pada kenyataannya ada banyak sekali tipe data yang dapat di-enkripsi, salah satu diantaranya adalah data teks. Saat ini sudah ada beberapa algoritma untuk menjaga keamanan data teks, seperti DES, AES (Rijndael), Blowfish, TEA, XOR256 Block, XOR256 Stream dan SEAL. Masing-masing algoritma memiliki kelebihan yang berbeda-beda. Dalam penelitian ini penulis akan membahas mengenai algoritma SEAL untuk pengamanan data file teks.

Algoritma Seal merupakan salah satu algoritma kriptografi untuk mengamankan data. Oleh sebab itu, perlu dibangun sebuah sistem untuk mengaplikasikan algoritma SEAL dengan melibatkan proses enkripsi dan dekripsi sehingga dapat dianalisis lebih dalam mengenai struktur chiper dan cara kerja algoritma kriptografi SEAL dengan beberapa pengujian sehingga dapat dilakukan analisa terhadap perubahan hasil keluaran (output) yang terjadi jika terjadi perubahan pada masukan (input) sehingga dapat diketahui seberapa baik proses enkripsi dengan algoritma kriptografi SEAL dalam memproteksi data.

PT. Amanda *Tour & Travel* adalah salah satu perusahaan travel di medan yang menyediakan layanan pemesanan tiket pesawat. Perusahaan ini didirikan pada tahun 2014. Pada awal konsepnya PT. Amanda *Tour & Travel* dalam memasarkan tiket atau jasa yang dijual, diperlukan berbagai strategi dan kebijaksanaan dalam memasarkan produk yang berfungsi untuk membantu membandingkan harga tiket pesawat dari berbagai situs *online* dan semakin banyak jumlah *travel* yang berkembang saat ini membuat para pengelolah ingin menunjukan strategi pemasaran yang lebih baik.

Management of Information System Journal
Vol 3, No 2, Maret 2025, Hal. 21 - 37
ISSN: 2964-9455 (media online)
DOI: 10.47065/mis.v2i3. 1919
https://journal.fkpt.org/index.php/MIS

Pengamanan data penjualan tiket pada PT. Amanda *tour & travel* dilakukan dengan mengimplementasikan algoritma kriptografi terhadap *record* dalam basis datanya dengan tujuan membuat *record* yang tersimpan menjadi lebih rahasia dan sulit diakses oleh pihak lain. Kriptografi sendiri adalah ilmu yang berstandarkan pada teknik matematika untuk berurusan dengan keamanan informasi, seperti kerahasiaan, keutuhan data, dan otentikasi entitas. Tujuan utama sistem kriptografi adalah mengamankan informasi yang bersifat rahasia serta menjaga keutuhan data dan informasi[1]. Data penting dan vital yang tersimpan pada basis data seringkali menjadi target empuk bagi para penyerang. Serangan yang terjadi dapat dilakukan oleh pihak luar (*hacker*) maupun pihak dalam (pegawai yang tidak puas). Kriptografi memiliki beberapa jenis algortima untuk mengamankan pengamanan data, diantaranya adalah algoritma SEAL

2. METODOLOGI

3.1 Sejarah Kriptografi

Kriptografi memiliki sejarah yang sangat menarik dan panjang. Kriptografi sudah digunakan 4000 tahun yang lalu dan diperkenalkan oleh orang-orang Mesir untuk mengirim pesan kepada pasukan militer yang berada dilapangan. Dengan demikian pesan tersebut tidak bisa dibaca oleh pihak musuh walaupun kurir pembawa pesan tersebut tertangkap oleh musuh.
Pada zaman Romawi kuno dikisahkan tentang Julius Caesar yang ingin mengirimkan satu pesan rahasia kepada seorang Jendral di medan perang. Pesan tersebut harus dikirimkan melalui seorang kurir, tetapi karena pesan tersebut mengandung rahasia Julius Caesar tidak ingin pesan tersebut terbuka ditengah jalan. Julius Caesar kemudian memikirkan cara mengatasinya, yaitu dengan mengacak pesan tersebut menjdi suatu pesan yang tidak dapat dipahami oleh siapapun kecuali hanya dapat dipahami oleh Jendral saja. (Dony, 2005:77-78)
Ilmu Kriptografi sebenarnya sudah mulai dipelajari manusia sejak tahun 400 SM, yaitu pada zaman Yunani kuno. Dari catatan bahwa "Penyandian Transposisi" merupakan sistem kriptografi pertama yang digunakan atau dimanfaatkan. Bidang ilmu ini terus berkembang seiring dengan kemajuan peradaban manusia, dan memegang peranan penting dalam strategi peperangan yang terjadi dalam sejarah manusia, mulai dari sistem kriptografi "*Caesar Chiper*" ang terkenal pada zaman Romawi kuno, "*Playfair Cipher*" yang digunakan Inggris dan "ADFVGX Cipher" yang digunakan Jerman pada Perang Dunia, hingga algoritma-algoritma kriptografi rotor yang populer pada Perang Dunia II , seperti Sigaba / M-134 (Amerika Serikat), Typex (Inggris), Purple (Jepang), dan mesin kriptografi legendaris Enigma (Jermn).
Induk dari keilmuan dari kriptografi sebenarnya adalah matematika, khususnya teori aljabar yang mendasar ilmu bilangan . Oleh karena itu kriptografi semakin berkembang ketika komputer ditemukan. Sebab dengan penemuan komputer memungkinkan dilakukanya perhitungan yang rumit dan komplekdalam waktu yang relatif sangat singkat, suatu hal yang sebelumnya tidak dapat dilakukan. Dari hal tersebut lahirlah banyak teori dan algotitma penyandian data yang semakin kompleks dan sulit dipecahkan.
Dewasa ini bidang ilmu kriptografi memiliki kemungkinan aplikasi yang sangat luas, mulai dari bidang militer, telekomunikasi, jaringan komputer, keuangan dan perbakan, pendidikan dan singkatnya dimana suatu kerahasiaan data amat diperlukan disitulah kriptografi memegang peranan penting. Produk-produk yamg menggunakan kriptografi sebagai dasarnyapun cukup beragam, mulai dari kartu ATM, E-Commerce, secure e-mail dan lain-lain.

3.2 Algoritma SEAL

SEAL merupakan salah satu jenis stream cipher, yaitu memproses unit atau input data, pesan atau informasi pada satu saat. Unit atau data pada umumnya sebuah byte[2]. Dengan cara ini enkripsi atau dekripsi dapat dilaksanakan pada panjang yang variabel. Algoritma ini tidak harus menunggu sejumlah input data, pesan atau informasi tertentu sebelum diproses, atau menambahkan byte tambahan untuk mengenkrip. SEAL dibuat oleh Rogaway dan Coppersmith dan dipatentkan oleh perusahaan IBM pada tahun 1993. SEAL digunakan secara luas pada beberapa aplikasi dan umumnya dinyatakan sangat aman[2].

Cara Kerja Enkripsi SEAL: Untuk mengenkripsi SEAL diperlukan input berupa password dan file plaintext yang akan dienkripsikan. Kemudian file plaintext tersebut diubah ke dalam byte dan password. Setelah mendapatkan 160 bit output SHA maka output tersebut dimasukkan kembali ke algoritma SHA dengan modifikasi w[0] = i mod 5 untuk membentuk tabel permutasi box (T), subtitusi box (S), dan kunci (R) yang diperlukan. Tabel T merupakan array sebanyak 512, untuk array T[0]-T[509] diperoleh dengan menginputkan i = (0x500). Untuk array S[510]-S[511] diperoleh dengan menginputkan i = (-1+0x500). Tabel S merupakan array sebanyak 256, untuk array S[0]-S[3] diperoleh dengan menginputkan i = (-1+0x1000). Untuk array S[4]-S[253] diperoleh dengan menginputkan i = (0x1000). Untuk array S[254]-S[255] diperoleh dengan

Management of Information System Journal
Vol 3, No 2, Maret 2025, Hal. 21 - 37
ISSN: 2964-9455 (media online)
DOI: 10.47065/mis.v2i3. 1919
https://journal.fkpt.org/index.php/MIS

menginputkan i = (-2+0x1000). Tabel R merupakan array sebanyak 16. Untuk array R[0]-R[2] diperoleh dengan menginputkan i = (-2+0x2000). Untuk array R[3]-R[12] diperoleh dengan menginputkan i = (0x2000). Untuk array R[13]-S[15] diperoleh dengan menginputkan i = (-1+0x2000). Setelah mendapatkan tabel T, S, R, masing-masing byte pada password diXOR-kan dengan array pada tabel dengan urutan, pertama yaitu xor tabel R dengan urutan tabel R[4*i], R[4*i+1], R[4*i+2], R[4*i+3]. Kemudian xor tabel T dengan urutan tabel T[4*i], T[4*i+1], T[4*i+2], T[4*i+3]. Terakhir xor tabel S dengan urutan tabel S[4*i], S[4*i+1], S[4*i+2], S[4*i+3]. Terdapat 4 buah output pada akhir proses xor, kemudian digabungkan menjadi satu. Hasil penggabungan output tersebut dikembalikan dari byte ke word[2].

Cara Dekripsi Algoritma SEAL :

Dekripsi SEAL memiliki proses pengolahan plaintext dan password yang sama seperti enkripsi. Urutan dalam xor dibalik, dimulai dari tabel S, kemudian T, dan yang terakhir R. Hasil akhir dekripsi disimpan dalam file asli dan ditampilkan pada layar[2].

3. ANALISA DAN PEMBAHASAN

4.1 Analisis Permasalahan

Pengamanan data penjualan tiket pada PT. Amanda *tour & travel* dilakukan dengan mengimplementasikan algoritma kriptografi terhadap *record* dalam basis datanya dengan tujuan membuat *record* yang tersimpan menjadi lebih rahasia dan sulit diakses oleh pihak lain. Kriptografi sendiri adalah ilmu yang berstandarkan pada teknik matematika untuk berurusan dengan keamanan informasi, seperti kerahasiaan, keutuhan data, dan otentikasi entitas. File penjualan tiket yang disimpan kedalam database agar tidak dapat disalah gunakan oleh orang yang tidak bekepentingan maka dilakukan pengamanan data dengan Algoritma Seal. Dengan menggunakan Algoritma Seal pada file data biner terenkripsi tidak dapat dibaca oleh komputer sebelum data base tersebut di enkripsikan kembali. Hal tersebut terjadi dikarenakan pada proses enkripsi, akan terjadi pengacakan data biner pada file tersebut sehingga informasi penting yang digunakan aplikasi pada komputer untuk membaca file tersebut tidak valid dan file akan dianggap *corrupt* (rusak), ataupun tidak dikenali oleh sistem yang akan membaca file tersebut pada komputer.
Pengamanan terhadap data berupa file yang dilakukan dengan cara melakukan enkripsi pada data binner file tersebut sudah selayaknya menggunakan metode yang dapat dieksekusi dengan cepat, ringan, dan aman. Sehingga Algoritma Seal sangat cocok untuk diimplementasikan membangun sistem keamanan data base pada sebuah perusahaan penjualan tiket demi keamaan data konsumen.
Algoritma Seal atau sistem pengamanan databse pada perusahaan penjualan tike di PT. Amanda *tour & travel* dapat digunakan untuk mengacak kode biner pada file tersebut, SEAL merupakan salah satu jenis stream cipher, yaitu memproses unit atau input data, pesan atau informasi pada satu saat. Unit atau data pada umumnya sebuah *byte*. Dengan cara ini enkripsi atau dekripsi dapat dilaksanakan pada panjang yang variabel. Algoritma ini tidak harus menunggu sejumlah input data, pesan atau informasi tertentu sebelum diproses, atau menambahkan byte tambahan untuk mengenkrip. Sehingga pada penelitian ini dapat digunakan untuk mengenkripsi file agar file tidak dapat digunakan oleh sistem operasi atau aplikasi yang berjalan pada sistem komputer yang belum diinstal aplikasi yang diracang saat ini.

4.2 Algoritma Sistem SEAL

Algoritma Seal merupakan metode enkripsi menggunakan metode simetrik dan pengolahan dalam bentuk blok chiper, jadi kata kunci yang sama digunakan untuk proses enkripsi dan dekripsi. Parameter-parameter yang digunakan dalam algoritmat Seal adalah sebagai berikut:

1. Jumlah putaran ini disimbolkan dengan *r* yang merupakan parameter untuk rotasi dengan nilai 0, 1, 2, …… 255.
2. Jumlah *word* dalam bit disimbolkan dengan *w*. Nilai bit yang di *support* adalah 16 bit, 32 bit, dan 64 bit.
3. Kata kunci (*key word*) Variable ini disimbolkan dengan *b* dengan range 0, 1, 2, …. 255. *Key word* ini dikembangkan menjadi *array S* yang digunakan sebagai *key* pada proses untuk enkripsi dan dekripsi.

Ada 3 proses utama dalam algoritma seal, yaitu perluasan kunci, enkripsi dan dekripsi. Perluasan kunci merupakan proses membangkitkan kunci internal dengan memanfaatkan komputasi rotasi left regular shift (<<<) dan right regular shift (>>>), dengan panjang kunci tergantung dari jumlah putaran. Kunci internal kemudian digunakan dalam proses enkripsi dan dekripsi. Proses enkripsi dibagi menjadi tiga, yaitu: penjumlahan integer, XOR dan rotasi.

Management of Information System Journal
Vol 3, No 2, Maret 2025, Hal. 21 - 37
ISSN: 2964-9455 (media online)
DOI: 10.47065/mis.v2i3. 1919
https://journal.fkpt.org/index.php/MIS

Langkah-langkah mengenkripsi data menggunakan algoritma Seal yaitu:
Diberikan contoh:

- Plaintext(x) = COMPUTER
- Key(k) = 13 34 57 79 9B BC DF F1

Langkah Pertama :

Ubahlah plaintext kedalam bentuk biner
C : 01000011
O : 01001111
M : 01001101
P : 01010000
U : 01010101
T : 01010100
E : 01000101
R : 01010010
Ubahlah key kedalam bentuk biner
13 : 00010011
34 : 00110100
57 : 01010111
79 : 01111001
9B : 10011011
BC : 10111100
DF : 11011111
F1 : 11110001

Langkah Kedua :
Lakukan Initial Permutation (IP) pada bit plaintext menggunakan tabel IP berikut:
Tabel Initial Permutation(IP)

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

Urutan bit pada plaintext urutan ke 58 ditaruh diposisi 1,
Urutan bit pada plaintext urutan ke 50 ditaruh di posisi 2,
Urutan bit pada plaintext urutan ke 42 ditaruh di posisi 3, dst
Sehingga hasil outputnya adalah
IP(x) : 11111111 10111000 01110110 01010111 00000000 00000000 00000110 10000011
Pecah bit pada IP(x) menjadi 2 bagian yaitu:
L_0 : 11111111 10111000 01110110 01010111 (tabel IP dengan warna kuning)
R_0 : 00000000 00000000 00000110 10000011 (tabel IP dengan warna hijau)

Langkah Ketiga :

Generate kunci yang akan digunakanuntuk mengenkripsi plaintext dengan menggunakan tabel permutasi kompresi PC-1, pada langkah ini terjadi kompresi dengan membuang 1 bit masing-masing blok kunci dari 64 bit menjadi 56 bit.

Tabel PC-1

Management of Information System Journal
Vol 3, No 2, Maret 2025, Hal. 21 - 37
ISSN: 2964-9455 (media online)
DOI: 10.47065/mis.v2i3. 1919
https://journal.fkpt.org/index.php/MIS

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	45	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

Dapat kita lihat pada tabel diatas, tidak terdapat urutan bit 8,16,24,32,40,48,56,64 karena telah dikompress.
Berikut hasil outpunya :
CD(k) : 1111000 0110011 0010101 0101111 0101010 1011001 1001111 0001111
Pecah CD(k) menjadi dua bagian kiri dan kanan, sehingga menjadi
C_0 : 1111000 0110011 0010101 0101111(tabel PC-1 warna kuning)
D_0 : 0101010 1011001 1001111 0001111 (tabel PC-1 warna hijau)

Langkah Keempat :
Lakukan pergeseran kiri (Left Shift) pada C_0 dan D_0, sebanyak 1 atau 2 kali berdasarkan kali putaran yang ada pada tabel putaran sebagai berikut:
Tabel Left Shift

Putaran ke - i	Jumlah Pergeseran(Left Shift)
1	1
2	1
3	2
4	2
5	2
6	2
7	2
8	2
9	1
10	2
11	2
12	2
13	2
14	2
15	2
16	1

Untuk putaran ke 1, dilakukan pegeseran 1 bit ke kiri
Untuk putaran ke 2, dilakukan pergeseran 1 bit kekiri
Untuk putaran ke 3, dilakukan pergeseran 2 bit kekiri, dst

Berikut hasil outputnya:
C_0 : 1111000 0110011 0010101 0101111
D_0 : 0101010 1011001 1001111 0001111

Digeser 1 bit ke kiri
C_1 : 1110000 1100110 0101010 1011111
D_1 : 1010101 0110011 0011110 0011110

Digeser 2 bit ke kiri
C_2 : 1100001 1001100 1010101 0111111
D_2 : 0101010 1100110 0111100 0111101

Management of Information System Journal
Vol 3, No 2, Maret 2025, Hal. 21 - 37
ISSN: 2964-9455 (media online)
DOI: 10.47065/mis.v2i3. 1919
https://journal.fkpt.org/index.php/MIS

Digeser 2 bit ke kiri
C_3 : 0000110 0110010 1010101 1111111
D_3 : 0101011 0011001 1110001 1110101

Digeser 2 bit ke kiri
C_4 : 0011001 1001010 1010111 1111100
D_4 : 0101100 1100111 1000111 1010101

Digeser 2 bit ke kiri
C_5 : 1100110 0101010 1011111 1110000
D_5 : 0110011 0011110 0011110 1010101

Digeser 2 bit ke kiri
C_6 : 0011001 0101010 1111111 1000011
D_6 : 1001100 1111000 1111010 1010101

Digeser 2 bit ke kiri
C_7 : 1100101 0101011 1111110 0001100
D_7 : 0110011 1100011 1101010 1010110

Digeser 2 bit ke kiri
C_8 : 0010101 0101111 1111000 0110011
D_8 : 1001111 0001111 0101010 1011001

Digeser 1 bit ke kiri
C_9 : 0101010 1011111 1110000 1100110
D_9 : 0011110 0011110 1010101 0110011

Digeser 2 bit ke kiri
C_{10} : 0101010 1111111 1000011 0011001
D_{10} : 1111000 1111010 1010101 1001100

Digeser 2 bit ke kiri
C_{11} : 0101011 1111110 0001100 1100101
D_{11} : 1100011 1101010 1010110 0110011

Digeser 2 bit ke kiri
C_{12} : 0101111 1111000 0110011 0010101
D_{12} : 0001111 0101010 1011001 1001111

Digeser 2 bit ke kiri
C_{13} : 0111111 1100001 1001100 1010101
D_{13} : 0111101 0101010 1100110 0111100

Digeser 2 bit ke kiri
C_{14} : 1111111 0000110 0110010 1010101
D_{14} : 1110101 0101011 0011001 1110001

Digeser 2 bit ke kiri
C_{15} : 1111100 0011001 1001010 1010111
D_{15} : 1010101 0101100 1100111 1000111

Digeser 1 bit ke kiri
C_{16} : 1111000 0110011 0010101 0101111
D_{16} : 0101010 1011001 1001111 0001111

Setiap hasil putaran digabungkan kembali menjadi C_iD_i dan diinput kedalam tabel Permutation Compression 2

Management of Information System Journal
Vol 3, No 2, Maret 2025, Hal. 21 - 37
ISSN: 2964-9455 (media online)
DOI: 10.47065/mis.v2i3. 1919
https://journal.fkpt.org/index.php/MIS

(PC-2) dan terjadi kompresi data C_iD_i 56 bit menjadi CiDi 48 bit.

Tabel PC-2

14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

Berikut hasil outputnya:

C_1D_1 = 1110000 1100110 0101010 1011111 1010101 0110011 0011110 0011110
K_1 = 000110 110000 001011 101111 111111 000111 000001 110010

C_2D_2 = 1100001 1001100 1010101 0111111 0101010 1100110 0111100 0111101
K_2 = 011110 011010 111011 011001 110110 111100 100111 100101

C_3D_3 = 0000110 0110010 1010101 1111111 0101011 0011001 1110001 1110101
K_3 = 010101 011111 110010 001010 010000 101100 111110 011001

C_4D_4 = 0011001 1001010 1010111 1111100 0101100 1100111 1000111 1010101
K_4 = 011100 101010 110111 010110 110110 110011 010100 011101

C_5D_5 = 1100110 0101010 1011111 1110000 0110011 0011110 0011110 1010101
K_5 = 011111 001110 110000 000111 111010 110101 001110 101000

C_6D_6 = 0011001 0101010 1111111 1000011 1001100 1111000 1111010 1010101
K_6 = 011000 111010 010100 111110 010100 000111 101100 101111

C_7D_7 = 1100101 0101011 1111110 0001100 0110011 1100011 1101010 1010110
K_7 = 111011 001000 010010 110111 111101 100001 100010 111100

C_8D_8 = 0010101 0101111 1111000 0110011 1001111 0001111 0101010 1011001
K_8 = 111101 111000 101000 111010 110000 010011 101111 111011

C_9D_9 = 0101010 1011111 1110000 1100110 0011110 0011110 1010101 0110011
K_9 = 111000 001101 101111 101011 111011 011110 011110 000001

$C_{10}D_{10}$ = 0101010 1111111 1000011 0011001 1111000 1111010 1010101 1001100
K_{10} = 101100 011111 001101 000111 101110 100100 011001 001111

$C_{11}D_{11}$ = 0101011 1111110 0001100 1100101 1100011 1101010 1010110 0110011
K_{11} = 001000 010101 111111 010011 110111 101101 001110 000110

$C_{12}D_{12}$ = 0101111 1111000 0110011 0010101 0001111 0101010 1011001 1001111
K_{12} = 011101 010111 000111 110101 100101 000110 011111 101001

$C_{13}D_{13}$ = 0111111 1100001 1001100 1010101 0111101 0101010 1100110 0111100
K_{13} = 100101 111100 010111 010001 111110 101011 101001 000001

Management of Information System Journal
Vol 3, No 2, Maret 2025, Hal. 21 - 37
ISSN: 2964-9455 (media online)
DOI: 10.47065/mis.v2i3. 1919
https://journal.fkpt.org/index.php/MIS

$C_{14}D_{14}$ = 1111111 0000110 0110010 1010101 1110101 0101011 0011001 1110001
K_{14} = 010111 110100 001110 110111 111100 101110 011100 111010

$C_{15}D_{15}$ = 1111100 0011001 1001010 1010111 1010101 0101100 1100111 1000111
K_{15} = 101111 111001 000110 001101 001111 010011 111100 001010

$C_{16}D_{16}$ = 1111000 0110011 0010101 0101111 0101010 1011001 1001111 0001111
K_{16} = 110010 110011 110110 001011 000011 100001 011111 110101

Langkah Kelima :

Pada langkah ini, kita akan meng-ekspansi data R_{i-1} 32 bit menjadi R_i 48 bit sebanyak 16 kali putaran dengan nilai perputaran 1<= i <=16 menggunakan Tabel Ekspansi (E).

Tabel Ekspansi(E)

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

Hasil $E(R_{i-1})$ kemudian di XOR dengan K_i dan menghasilkan Vektor Matriks A_i.

Berikut hasil outputnya:

Iterasi 1
E(R(1)-1) = 100000 000000 000000 000000 000000 001101 010000 000110
K1 = 000110 110000 001011 101111 111111 000111 000001 110010
---------- XOR
A1 = 100110 110000 001011 101111 111111 001010 010001 110100 {

UPDATE (18 maret 2015) , berhubung bagian dibawah ini yang paling ribet, maka saya tambahkan keterangan ditengah-tengah proses iterasi. Bisa kita lihat pada iterasi1 diatas setelah kita dapatkan hasil XOR antara E(R(1)-1) dengan K1 dan menghasilkan A1, maka proses berikutnya langsung masuk ke **LANGKAH KEENAM** terlebih dahulu, dimana A1 akan dimasukan ke dalam S-Box dan menghasilkan output B1.
B1 kemudian akan dipermutasikan lagi dengan tabel P-Box dan menghasilkan nilai PB1 yang kemudian di XOR-kan dengan L0 dan menghasilkan nilai **R1**. Nilai R1 ini digunakan untuk melanjutkan iterasi ke-2.}

Iterasi – 2

E(R(2)-1) = 011010 101110 100001 010110 100110 100101 010000 001101
K2 = 011110 011010 111011 011001 110110 111100 100111 100101
---------- XOR
A2 = 000100 110100 011010 001111 010000 011001 110111 101000

Iterasi – 3

E(R(3)-1) = 010001 010111 111011 110011 110001 010101 010010 100001
K3 = 010101 011111 110010 001010 010000 101100 111110 011001
---------- XOR
A3 = 000100 001000 001001 111001 100001 111001 101100 111000

Management of Information System Journal
Vol 3, No 2, Maret 2025, Hal. 21 - 37
ISSN: 2964-9455 (media online)
DOI: 10.47065/mis.v2i3. 1919
https://journal.fkpt.org/index.php/MIS

Iterasi – 4

E(R(4)-1) = 010111 110001 010111 110011 110101 011100 001111 110001
K4 = 011100 101010 110111 010110 110110 110011 010100 011101
---------- XOR
A4 = 001011 011011 100000 100101 000011 101111 011011 101100

Iterasi – 5

E(R(5)-1) = 110110 101001 011100 000101 011001 011010 100110 100011
K5 = 011111 001110 110000 000111 111010 110101 001110 101000
---------- XOR
A5 = 101001 100111 101100 000010 100011 101111 101000 001011

Iterasi – 6

E(R(6)-1) = 100101 011011 110001 010110 101110 101100 000111 111010
K6 = 011000 111010 010100 111110 010100 000111 101100 101111
---------- XOR
A6 = 111101 100001 100101 101000 111010 101011 101011 010101

Iterasi – 7

E(R(7)-1) = 110010 100001 011111 110010 100111 111101 011001 010011
K7 = 111011 001000 010010 110111 111101 100001 100010 111100
---------- XOR
A7 = 001001 101001 001101 000101 011010 011100 111011 101111

Iterasi – 8

E(R(8)-1) = 111100 001010 101001 010101 010011 110000 001010 100011
K8 = 111101 111000 101000 111010 110000 010011 101111 111011
---------- XOR
A8 = 000001 110010 000001 101111 100011 100011 100101 011000

Iterasi – 9

E(R(9)-1) = 010010 101111 111000 000000 000010 101111 110101 010001
K9 = 111000 001101 101111 101011 111011 011110 011110 000001
---------- XOR
A9 = 101010 100010 010111 101011 111001 110001 101011 010000

Iterasi – 10

E(R(10)-1)= 100111 111000 001110 100010 100111 110111 111000 001010
K10 = 101100 011111 001101 000111 101110 100100 011001 001111
---------- XOR
A10 = 001011 100111 000011 100101 001001 010011 100001 000101

Iterasi – 11

E(R(11)-1)= 010011 110111 111010 101010 101111 110011 110001 011001
K11 = 001000 010101 111111 010011 110111 101101 001110 000110
---------- XOR
A11 = 011011 100010 000101 111001 011000 011110 111111 011111

Management of Information System Journal
Vol 3, No 2, Maret 2025, Hal. 21 - 37
ISSN: 2964-9455 (media online)
DOI: 10.47065/mis.v2i3. 1919
https://journal.fkpt.org/index.php/MIS

Iterasi – 12

E(R(12)-1)= 001001 011010 101001 011111 110001 010111 110010 101100
K12 = 011101 010111 000111 110101 100101 000110 011111 101001
---------- XOR
A12 = 010100 001101 101110 101010 010100 010001 101101 000101

Iterasi – 13

E(R(13)-1)= 100110 100111 110111 111011 111110 101110 101100 001010
K13 = 100101 111100 010111 010001 111110 101011 101001 000001
---------- XOR
A13 = 000011 011011 100000 101010 000000 000101 000101 001011

Iterasi – 14

E(R(14)-1)= 111001 010111 110000 001000 001000 001000 001011 111011
K14 = 010111 110100 001110 110111 111100 101110 011100 111010
---------- XOR
A14 = 101110 100011 111110 111111 110100 100110 010111 000001

Iterasi – 15

E(R(15)-1)= 000110 101100 001100 000001 011001 011010 100101 010100
K15 = 101111 111001 000110 001101 001111 010011 111100 001010
---------- XOR
A15 = 101001 010101 001010 001100 010110 001001 011001 011110

Iterasi – 16

E(R(16)-1)= 101101 011101 010100 000101 010101 010001 010110 100010
K16 = 110010 110011 110110 001011 000011 100001 011111 110101
---------- XOR
A16 = 011111 101110 100010 001110 010110 110000 001001 010111

Langkah Keenam :

Setiap Vektor A_i disubstitusikan kedelapan buah S-Box(Substitution Box), dimana blok pertama disubstitusikan dengan S_1, blok kedua dengan S_2 dan seterusnya dan menghasilkan output vektor B_i 32 bit.

S1 :

	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
00	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
01	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
10	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
11	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

S2 :

	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
00	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
01	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5

Management of Information System Journal
Vol 3, No 2, Maret 2025, Hal. 21 - 37
ISSN: 2964-9455 (media online)
DOI: 10.47065/mis.v2i3. 1919
https://journal.fkpt.org/index.php/MIS

10	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
11	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

S3 :

	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
00	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
01	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
10	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
11	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

S4 :

	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
00	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
01	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
10	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
11	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

S5 :

	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
00	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
01	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	15
10	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
11	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

S6 :

	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
00	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
01	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
10	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
11	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

S7 :

	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
00	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
01	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
10	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
11	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

S8 :

	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
00	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
01	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
10	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8

Management of Information System Journal
Vol 3, No 2, Maret 2025, Hal. 21 - 37
ISSN: 2964-9455 (media online)
DOI: 10.47065/mis.v2i3. 1919
https://journal.fkpt.org/index.php/MIS

11	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

Cara menggunakan S-Box : (Untuk detail penggunaan S-Box, silahkan lihat dihalaman

Kita ambil contoh S1, kemudian konversi setiap angka didalam tabel S1 yang berwarna putih menjadi biner, sehingga menjadi bentuk seperti dibawah:

S1 :

	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
00	1110	0100	1101	0001	0010	1111	1011	1000	0011	1010	0110	1100	0101	1001	0000	0111
01	0000	1111	0111	0100	1110	0010	1101	0001	1010	0110	1100	1011	1001	0101	0011	1000
10	0100	0001	1110	1000	1101	0110	0010	1011	1111	1100	1001	0111	0011	1010	0101	0000
11	1111	1100	1000	0010	0100	1001	0001	0111	0101	1011	0011	1110	1010	0000	0110	1101

Kemudian kita ambil sampel blok bit pertama dari A_1 yaitu **1**00110**0**
Kita pisahkan blok menjadi 2 yaitu:

- Bit pertama dan terakhir yaitu 1 dan 0 digabungkan menjadi 10
- Bit kedua hingga ke lima 0011

Kemudian dibandingkan dengan memeriksa perpotongan antara keduanya didapatkan nilai 1000(warna merah) dan seterusnya untuk blok kedua hingga blok kedelapan kita bandingkan dengan S2 hingga S8.

Berdasarkan cara diatas diperoleh hasil sebagai berikut:

B_1 = 1000 0101 0100 1000 0011 0010 1110 1010
B_2 = 1101 1100 0100 0011 1000 0000 1111 1001
B_3 = 1101 0110 0011 1100 1011 0110 0111 1111
B_4 = 0010 1001 1101 0000 1011 1010 1111 1110
B_5 = 0100 0001 0011 1101 1000 1010 1100 0011
B_6 = 0110 1101 1101 1100 0011 0101 0100 0110
B_7 = 1110 0011 0110 1011 0000 0101 0010 1101
B_8 = 0000 1000 1101 1000 1000 0011 1101 0101
B_9 = 0110 1110 1110 0001 1010 1011 0100 1010
B_{10} = 0010 0001 0111 0000 0100 0001 0110 1101
B_{11} = 0101 1110 0000 1100 1101 1011 1100 0010
B_{12} = 0110 1000 0000 1011 0011 0110 1010 1101
B_{13} = 1111 1001 1101 1011 0010 0100 1011 0011
B_{14} = 1011 1000 0111 1110 1100 0101 1100 0001
B_{15} = 0100 0001 0011 1001 1111 0111 0010 0111
B_{16} = 1000 0001 0110 1010 1111 0111 0100 1011

Langkah Ketujuh:

Setelah didapatkan nilai vektor B_i, langkah selanjutnya adalah memutasikan bit vektor B_i menggunakan tabel P-Box, kemudian dikelompokkan menjadi 4 blok dimana tiap-tiap blok memiliki 32 bit data.
Tabel P-Box

16	7	20	21	29	12	28	17
1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9
19	13	30	6	22	11	4	25

Sehingga hasil yang didapat adalah sebagai berikut:

$P(B_1)$ = 00101000 10110011 01000100 11010001

Management of Information System Journal
Vol 3, No 2, Maret 2025, Hal. 21 - 37
ISSN: 2964-9455 (media online)
DOI: 10.47065/mis.v2i3. 1919
https://journal.fkpt.org/index.php/MIS

$P(B_2)$ = 10001011 11011001 10001100 00010011
$P(B_3)$ = 01101111 10110010 10011100 11111110
$P(B_4)$ = 00111111 00111011 01000111 10100001
$P(B_5)$ = 10010101 00110010 11011000 01000101
$P(B_6)$ = 00100100 00011011 11110011 11111000
$P(B_7)$ = 11001000 11000001 11101110 01101100
$P(B_8)$ = 00000111 00111001 00101001 01100001
$P(B_9)$ = 11011001 00111011 10100011 10010100
$P(B_{10})$ = 00001100 00010101 01101110 00100100
$P(B_{11})$ = 01110001 00111110 10110000 01010011
$P(B_{12})$ = 10101000 01101000 10001110 11101001
$P(B_{13})$ = 10000110 11001011 11001111 11001011
$P(B_{14})$ = 00000101 11011101 00111010 01001111
$P(B_{15})$ = 10100101 00100110 11101100 11101100
$P(B_{16})$ = 00101001 11110111 01101000 11001100

Hasil P(Bi) kemudian di XOR kan dengan Li-1 untuk mendapatkan nilai Ri. Sedangkan nilai Li sendiri diperoleh dari Nilai Ri-1 untuk nilai 1 <= i <= 16.

L0 = 11111111 10111000 01110110 01010111
R0 = 00000000 00000000 00000110 10000011

P(B1) = 00101000 10110011 01000100 11010001
L(1)-1 = 11111111 10111000 01110110 01010111
----------XOR
R1 = 11010111 00001011 00110010 10000110

P(B2) = 10001011 11011001 10001100 00010011
L(2)-1 = 00000000 00000000 00000110 10000011
----------XOR
R2 = 10001011 11011001 10001010 10010000

P(B3) = 01101111 10110010 10011100 11111110
L(3)-1 = 11010111 00001011 00110010 10000110
----------XOR
R3 = 10111000 10111001 10101110 01111000

P(B4) = 00111111 00111011 01000111 10100001
L(4)-1 = 10001011 11011001 10001010 10010000
----------XOR
R4 = 10110100 11100010 11001101 00110001

P(B5) = 10010101 00110010 11011000 01000101
L(5)-1 = 10111000 10111001 10101110 01111000
----------XOR
R5 = 00101101 10001011 01110110 00111101

P(B6) = 00100100 00011011 11110011 11111000
L(6)-1 = 10110100 11100010 11001101 00110001
----------XOR
R6 = 10010000 11111001 00111110 11001001

P(B7) = 11001000 11000001 11101110 01101100
L(7)-1 = 00101101 10001011 01110110 00111101
----------XOR
R7 = 11100101 01001010 10011000 01010001

Management of Information System Journal
Vol 3, No 2, Maret 2025, Hal. 21 - 37
ISSN: 2964-9455 (media online)
DOI: 10.47065/mis.v2i3. 1919
https://journal.fkpt.org/index.php/MIS

P(B8) = 00000111 00111001 00101001 01100001
L(8)-1 = 10010000 11111001 00111110 11001001
----------XOR
R8 = 10010111 11000000 00010111 10101000

P(B9) = 11011001 00111011 10100011 10010100
L(9)-1 = 11100101 01001010 10011000 01010001
----------XOR
R9 = 00111100 01110001 00111011 11000101

P(B10) = 00001100 00010101 01101110 00100100
L(10)-1 = 10010111 11000000 00010111 10101000
----------XOR
R10 = 10011011 11010101 01111001 10001100

P(B11) = 01110001 00111110 10110000 01010011
L(11)-1 = 00111100 01110001 00111011 11000101
----------XOR
R11 = 01001101 01001111 10001011 10010110

P(B12) = 10101000 01101000 10001110 11101001
L(12)-1 = 10011011 11010101 01111001 10001100
----------XOR
R12 = 00110011 10111101 11110111 01100101

P(B13) = 10000110 11001011 11001111 11001011
L(13)-1 = 01001101 01001111 10001011 10010110
----------XOR
R13 = 11001011 10000100 01000100 01011101

P(B14) = 00000101 11011101 00111010 01001111
L(14)-1 = 00110011 10111101 11110111 01100101
----------XOR
R14 = 00110110 01100000 11001101 00101010

P(B15) = 10100101 00100110 11101100 11101100
L(15)-1 = 11001011 10000100 01000100 01011101
----------XOR
R15 = 01101110 10100010 10101000 10110001

P(B16) = 00101001 11110111 01101000 11001100
L(16)-1 = 00110110 01100000 11001101 00101010
----------XOR
R16 = 00011111 10010111 10100101 11100110

L16 = 01101110 10100010 10101000 10110001

Langkah Kedelapan:

Langkah terakhir adalah menggabungkan R_{16} dengan L_{16} kemudian dipermutasikan untuk terakhir kali dengan tabel Invers Initial Permutasi(IP^{-1}).

Tabel IP^{-1}

40	8	48	16	56	24	64	32

Management of Information System Journal
Vol 3, No 2, Maret 2025, Hal. 21 - 37
ISSN: 2964-9455 (media online)
DOI: 10.47065/mis.v2i3. 1919
https://journal.fkpt.org/index.php/MIS

39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

Sehingga Input :
$R_{16}L_{16}$ = 00011111 10010111 10100101 11100110 01101110 10100010 10101000 10110001
Menghasilkan Output:
Cipher(dalam biner) = **01010110 11110001 11010101 11001000 01010010 0101111 10000001 00111111**

Proses Enkripsi Metode Seal

Diasumsikan terdapat dua buah blok input sebesar w bit, A dan B. Dan diasumsikan juga bahwa pembentukan kunci internal telah dilakukan, sehingga array S[0...t-1] telah dihitung. Sehingga *pseudecode* untuk proses enkripsi seperti di bawah:

A ← A + KI [0]
B ← B + KI [1]
for i ← 1 to r do
A ← ((A⊕B) <<< B) + KI [2i]
B ← ((B⊕A) <<< A) + KI [2i+1]
End for

Contoh Kasus Enkripsi Seal pada pengamanan penjualan tiket pada PT. Amanda *tour & travel* sebagai berikut :

N ← N + KI [0]
E ← E + KI [1]
M ← M + KI [2]
E ← E + KI [3]
S S + KI [4]
I ← I + KI [5]
for i ← 1 to r do
N ← ((N⊕E⊕M⊕E⊕S⊕I) <<< I) + NI [6i]
I ← ((I⊕S⊕E⊕M⊕E⊕N) <<< N) + NI [6i+1]
End for

4.2.2 Proses Dekripsi Metode Seal

Algoritma pada proses dekripsi merupakan kebalikan dari proses enkripsi. Jika tadinya digeser ke kiri, maka pada proses dekripsi dilakukan pergeseran ke kanan (*right regular shift*).

for i ← r downto 1 do
B ← ((B – KI [2i+1])>>>A) ⊕A
A ← ((A – KI [2i])>>>B) ⊕B
endfor
B ← B - KI[1]
A ← A - KI[0]

Untuk mendekripsi cipherteks, diperlukan NI yang sama dengan NI saat mengenkripsi. Proses pembangkitan NI pada kedua proses tersebut juga sama.

Contoh Kasus Dekripsi Seal pada ada pengamanan penjualan tiket pada PT. Amanda *tour & travel*sebagai berikut :

I ← I + KI [0]
S ← S + KI [1]
E ← E + KI [2]
M ← M + KI [3]
E ← E + KI [4]
N ← N + KI [5]

Management of Information System Journal
Vol 3, No 2, Maret 2025, Hal. 21 - 37
ISSN: 2964-9455 (media online)
DOI: 10.47065/mis.v2i3. 1919
https://journal.fkpt.org/index.php/MIS

for i ←1 to r do
I ←(I-NI [6i+1] >>>I) ⊕ S⊕E⊕M⊕E⊕N
N ←(N-NI [6i] >>>N) ⊕E⊕M⊕E⊕S⊕I

4.2.3 Pembentukan kunci internal

K[0-1]...K [b] disalin ke tabel L [0-1]...L [b] dengan aturan di-padding dengan karakter 0 hingga ukuran L [i] menjadi w/2 bit. Contoh Kasus ada pengamanan penjualan tiket pada PT. Amanda *tour & travel* Sebagai berikut:

K[0] = n L[0] = n000
K[1] = e L[1] = e000
K[2] = m L[2] = m000
K[3] = e L[3] = e000
K[4] = s L[4] = s000
K[5] = i L[5] = i000

Kemudian, inisialisasi tabel kunci internal NI dengan ukuran t = 2r + 2 seperti berikut:

KI [0] ←P
for i ←1 to t – 1 do
KI[i] ←KI [i – 1]
Endfor

Algoritma pembentukan kunci internal menggunakan konstanta P dan Q yang didapatkan dari fungsi yang melibatkan bilangan irasional sebagai berikut:

$P = Odd[(e - 2)2^w]$
$Q = Odd[(f – 1)2^w]$

Keterangan:

e = 2.718281828459.....
ø = 1.618033988749.....

Nilai ø dapat juga didapatkan dengan rumus:

$$ø = \frac{1+\sqrt{5}}{2}$$

Sedangkan fungsi Odd(x) menghasilkan nilai integer ganjil yang paling dekat dengan x. Untuk nilai-nilai w yang diperbolehkan (16, 32 dan 64), nilai Pw dan Qw adalah sebagai berikut (dalam heksadesimal):

P_{16} = b7e1
Q_{16} = 9e37
P_{32} = b7e15163
Q_{32} = 9e3779b9
P_{64} = b7e151628aed2a6b
Q_{64} = 9e3779b97f4a7c15

Contoh kasus penyelesaian algoritma Seal dengan 12 ronde dengan ukuran blok 64 bit (Seal-32/12/b) bisa diserang dengan menggunakan 2^{44} plaintext. Hal ini menunjukkan bahwa Algoritma Seal-32/12/b memiliki tingkat keamanan yang sangat baik digunakan.

Tabel berikut ini menunjukkan jumlah plaintext yang dibutuhkan untuk melancarkan serangan diferensial terhadap algoritma seal seperti pada tabel dibawah ini.

Tabel 1 Diferensial terhadap Algoritma Seal

Ronde	4	6	8	10	12	14	16	18
Chosen Plantext	2^7	2^{16}	2^{28}	2^{36}	2^{44}	2^{52}	2^{61}	>>
Know Plaintext	2^{36}	2^{41}	2^{47}	2^{51}	2^{55}	2^{59}	2^{63}	>>

4. KESIMPULAN

Berdasarkan hasil penelitian yang dilakukan, maka peneliti mengambil kesimpulan sebagai berikut : Proses pengamanan data penjualan tiket PT. Amanda *Tour & Trave*l dilakukan dengan menerapkan meotde SEAL dimana identitas konsumen maupun tujuan akan di lakukan enkripsi data, sehingga data mereka tidak dapat dibaca oleh orang yang tidak berkepentingan. Penerapan Algoritma SEAL pada pengamanan data penjualan tiket PT. Amanda *Tour & Trave*l dengan melakukan perhitungan nilai biner pada saat melakukan enkripsi dimana data konsumen akan dirubah kedalam nilai biner dengan melihat tabel Assci sehingga

Management of Information System Journal
Vol 3, No 2, Maret 2025, Hal. 21 - 37
ISSN: 2964-9455 (media online)
DOI: 10.47065/mis.v2i3. 1919
https://journal.fkpt.org/index.php/MIS

perubahan data dari enkripsi ke Deskripsi akan diproses dengan metode SEAL. Perancang aplikasi pengamanan data penjualan tiket dengan algoritma SEAL menggunakan Visual Basic net 2018, penerapan algoritma dilakukan perancangan desain layout terlebih dahulu untuk dapat menjalankan aplikasi pengamanan data.

DAFTAR PUSTAKA

[1]. R. Sadikin, "Kriptografi Untuk Keamanan Jaringan dan Implementasinya
[2]. Dalam Bahasa Java", Yogyakarta : ANDI. 2012.
[3]. Semuil Tjihardi, Marvin Chandra Wijaya, "Pengamanan Data Dengan Menggunakan Algoritma Stream Chiper Seal", Konfrensi Nasional Sistem dan Informatika, KNS&109-010, 2009.
[4]. Donny Arius, Pengantar Ilmu Kriptografi : Teori, Analisis, Dan Implementasi, Yogyakarta : ANDI. 2008.
[5]. R. Munir, "Kriptografi", Bandung : Informatika. 2006.
[6]. M. Nafarin Penganggaran Perusahaan, Jakarta : Salemba Empat, 2009.
[7]. Assauri Sofyan, Manajemen Pemasaran Edisi Pertama, Jakarta : Rajawali Pers, 2011
[8]. S. Sembiring, " Perancangan Aplikasi Steganografi Untuk Menyisipkan
[9]. Pesan", Pelita Informatika Budidarma, Vol. IV, No.2, ISSN : 2301-9425. 2011.
[10]. Z. Mawati, J. Kharis, S. Yuliana, " Aplikasi Pengamanan File Video Menggunakan Teknik Kriptografi Algoritma Transposisi Zig-Zag", Jurnal Mahajana Informasi, Vol. III, No.2, ISSN : 2257-8290. 2018.
[11]. Ade Hendini, "Pemodal UML Sistem Informasi Monitoring Penjualan dan Stok Barang (Studi Kasus : Distro Zhezha Pontianak)", Jurnal Khatulistiwa Informatika, Vol.IV,No.2, 2006.
[12]. [Abdul Kadir, Pengenalan Algoritma Pendekatan secara Visual dan Interaktif Menggunakan RAPTOR, Yogyakarta : ANDI. 2013.
[13]. Astria Firman, Hans. F. Wowor, Xaverius Najoan, " Sistem Informasi Perpustakaan Online Berbasis Web", E-Journal Teknik Elektro dan Komputer, Vol.V, No.2. ISSN 2301-8402, 2016
[14]. Hendrayudi, " Dasar-Dasar Pemograman Microsoft Visual Basic 2008,
[15]. Bandung : PT.Satu Nusa. 2011.
[16]. Haryanto Bambang, Rekayasa Sistem Berorientasi Objek, Bandung : Informatika, 2004.