Jurnal Nasional Informatika dan Teknologi Jaringan
E-ISSN : 2540-7600
P-ISSN : 2540-7597

MODEL KEAMANAN INFORMASI BERBASIS TANDA TANGAN DIGITAL DENGAN DATA ENCRYPTION STANDARD (DES) ALGORITHM

Oris Krianto Sulaiman[1], Mohamad Ihwani[2], Salman Fajar Rizki[3]
[1]*Universitas Negeri Medan*
Jl. Willem Iskandar Pasar v Medan Estate, Medan 20221
fairystrawhat@gmail.com
[2]*Universitas Negeri Medan*
Jl. Willem Iskandar Pasar v Medan Estate, Medan 20221
[3]*Universitas Negeri Medan*
Jl. Willem Iskandar Pasar v Medan Estate, Medan 20221

***Abstrak*—Keamanan dan kerahasiaan informasi merupakan hal yang sangat penting, banyak hal yang telah dilakukan agar keamanan dan kerahasiaan informasi ini terjaga dengan utuh , salah satunya dengan menggunakan teknik kriptografi, kriptografi berperan untuk menjaga kemanan informasi dengan menyandikan informasi tersebut, salah satu algoritma kriptografi untuk penyandian yaitu DES, dimana DES akan melakukan pengacakan berdasarkan s-box hingga 16 putaran, selain menjaga kemanan dan kerahasiaan diperlukan juga nirpenyangkalan dengan menggunakan digital signature algorithm (DSA) atau tanda tangan digital yang mana bertujuan untuk melakukan verifikasi apakah pesan atau informasi tersebut diterima dalam keadaan asli dari pengiriman atau telah dimodifikasi sehingga pesan atau informasi tersebut tidaklah asli.**

***Keywords*— *Kriptografi, DSA, DES.*.**

I. PENDAHULUAN

Kriptografi merupakan ilmu mengenai teknik enkripsi dimana data diacak menggunakan suatu kunci enkripsi menjadi sesuatu yang sulit dibaca oleh seseorang yang tidak memiliki kunci dekripsi. Dekripsi menggunakan kunci dekripsi untuk mendapatkan kembali data asli. Proses enkripsi dilakukan menggunakan suatu algoritma dengan beberapa parameter [1].

Data Encryption Standar (DES) Data Encryption Standar (DES) merupakan algoritma cipher blok yang di jadikan standar algoritma enkripsi kunci-simetri, Algoritma DES dikembangkan di IBM dibawah kepemimpinan W.L. Tuchman pada tahun 1972.

DES termasuk kedalam sistem kriptografi simetri dan tergolong jenis cipher blok. DES beroperasi pada ukuran blok 64bit. DES mengenkripsi 64 bit plainteks menjadi 64 bit cipherteks dengan menggunakan 56 bit kunci internal (interlan key) atau subkey, kunci internal dibangkitkan dari kunci eksternal (external key) yang panjangnya 64 bit.

DES berperan dalam melakukan enkripsi pesan atau informasi untuk kemanan, namun DES tidak mempunyai kemampuan untuk nirpenyangkalan, DSA (Digital Signature Algorithm) atau tanda tangan digital mempunyai kemampuan nirpenyangkalan, pada model kemanan ini akan dilakukan kombinasi algoritma DES untuk menjaga kemanan dan kerahasian pesan atau informasi dan DSA untuk nirpenyangkalan , sehingga model ini memenuhi 2 aspek kemanan kriptografi yaitu kerahasian (confidentiality) dan Nirpenyangkalan (non-repudiation).

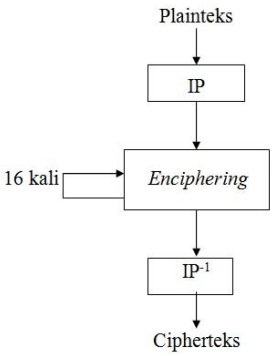
II. TINJAUAN PUSTAKA

A. Data Encryption Standar (DES)

DES termasuk kedalam sistem kriptografi simetri dan tergolong jenis cipher blok. DES beroperasi pada ukuran blok 64bit. DES mengenkripsi 64 bit plainteks menjadi 64 bit cipherteks dengan menggunakan 56 bit kunci internal (interlan key) atau subkey, kunci internal dibangkitkan dari kunci eksternal (external key) yang panjangnya 64 bit.

Skema global algoritma DES adalah sebagai berikut:

1. Blok plainteks dipermutasi dengan matriks permutasi awal (initial permutation atau IP)
2. Hasil permutasi awal kemudian di-enchipering sebanyak 16 kali (16 putaran). Setiap putaran menggunakan kunci internal yang berbeda
3. Hasil enciphering kemudian dipermutasi dengan matriks permutasi balikan (invers initial permutation atau IP-1) menjadi blok cipherteks.



Gbr.1 Skema global algoritma DES

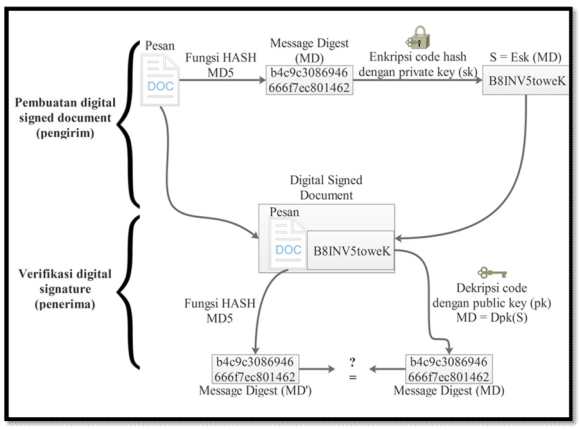
Didalam proses enciphering, blok plainteks akan dibagi menjadi dua bagian, bagian kiri (L) dan kanan (R), yang masing-masing panjangnya 32bit. Kedua bagian ini masuk kedalam 16 putaran DES.

B. Digital Signature Algorithm (DSA)

Tanda tangan digital (digital signature) adalah suatu mekanisme untuk menggantikan tanda tangan secara manual pada dokumen kertas [2]. Tanda tangan pesan dapat dilakukan dengan dua cara yaitu:

1. Enkripsi pesan
   Mengenkripsi pesan dengan sendirinya serta menyediakan ukuran otentikasi, pesan yang terenkripsi sudah menytakan pesan tersebut telah ditandatangani.
2. Tanda tangan digital dengan fungsi hash (hash function).

Tanda tangan digital dibangkitkan dari hash terhadap pesan. Nilai hash adalah kode ringkas dari pesan. Tanda tangan digital berlaku seperti tanda tangan dokumen kertas, tanda tangan digital ditambahkan (append) pada pesan.

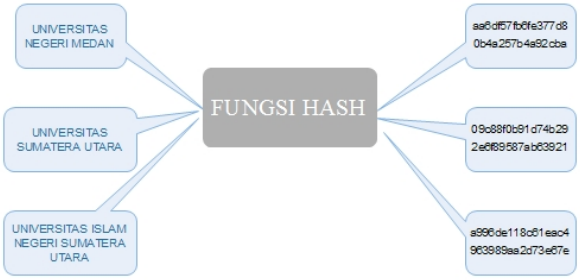


Gbr.2 Proses pemberian tanda tangan digital

Pada Gambar tersebut apabila pesan yang diterima sudah berubah, maka MD' yang dihasilkan dari fungsi hash berbeda dari MD semula yang berarti pesan tersebut sudah tidak asli lagi. Apabila pesan M tidak berasal dari orang yang sebenarnya, maka message digest (MD) yang dihasilkan berbeda dengan message digest (MD') yang dihasilkan pada proses verifikasi karena kunci public yang digunakan oleh penerima pesan tidak berkoresponden dengan kunci privat pengirim. Bila MD = MD' maka pesan yang diterima adalah pesan asli (message authentication) dan orang yang mengirim merupakan orang yang sebenarnya (user authentication).

C. Fungsi Hash MD5

Fungsi hash merupakan fungsi yang menerima masukkan string yang panjangnya sembarang dan mengkonversinya menjadi string keluaran yang panjangnya tetap (fixed), umumnya berukuran jauh lebih kecil daripada ukuran string semula [2].

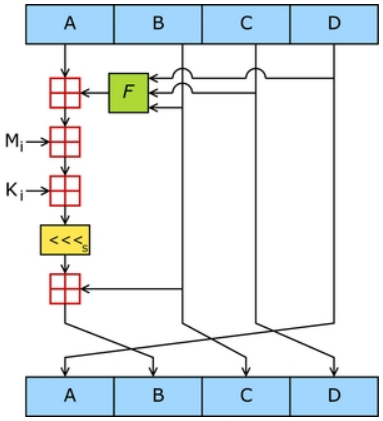


Gbr.3 Contoh hashing beberapa pesan

MD5 merupakan perbaikan dari MD4, algoritma ini menerima masukan berupa pesan dengan ukuran sembarang dan menghasilkan message digest yang panjangnya 128 bit.

Langkah-langkah pembuatan message digest secara garis besar adalah sebagai berikut:

- Penambahan bit-bit pengganjal (padding bits)
- Penambahan nilai panjang pesan semula
- Inisialisasi penyangga (buffer) MD
- Pengolahan pesan dalam blok berukuran 512bit



Gbr.4 Operasi dasar MD5

Operasi dasar MD5 dapat ditulis dengan sebuah persamaan sebagai berikut:

A⟵B + <<<S (A+F (B,C,D) + Mi + Ki

Penjelasan gambar

A,B,C,D = Empat buah peubah penyangga 32-bit (berisi nilai penyangga ABCD)

F = Salah satu fungsi F, G, H,I

<<<S = Circular left shift sebanyak s bit

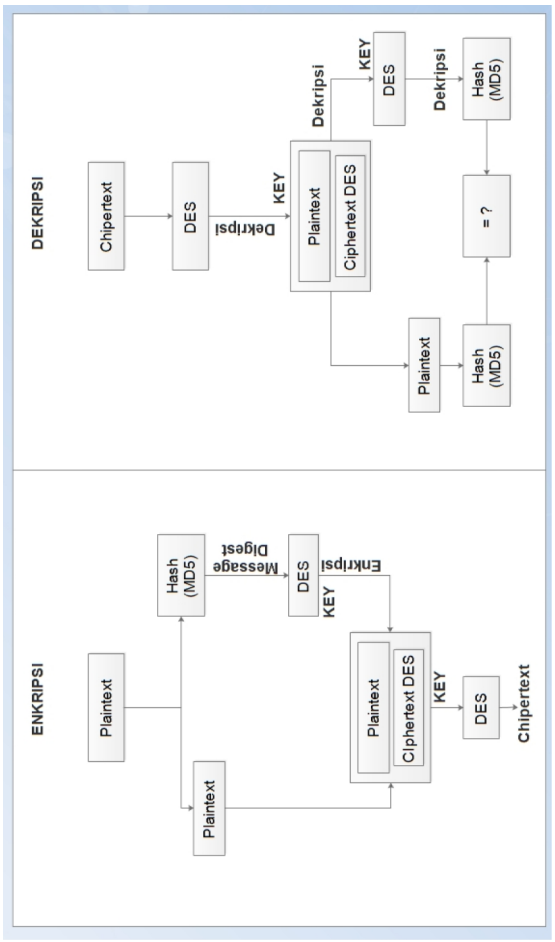
Mi = Kelompok 32-bit ke-i dari blok 512 bit message ke q (pengolahan blok 512- bit), nilai i=0 sampai 15

Ki = Elemen tabel K ke-I (32 bit)

\+ = Operasi penjumlahan modulo 232.

III. METODE PENELITIAN

Adapun skema alur dari model kemanan ini dapat dilihat pada gambar dibawah ini:



Gbr.5 Rancangan model kemanan informasi

Untuk memudahkan dalam hal pembahasan, gambar diatas dapat dibagi menjadi beberapa bagian, diantaranya adalah:

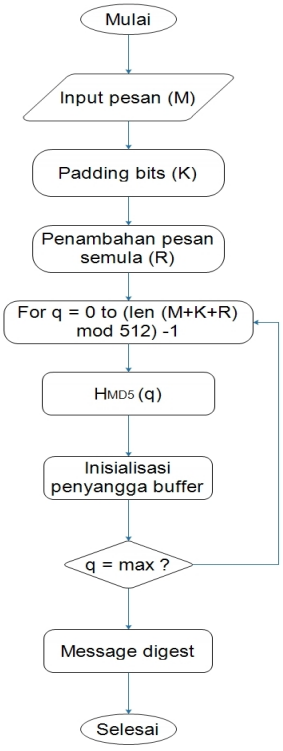
Proses enkripsi

1. Plainteks yang di bagi menjadi 2 bagian yaitu bagian plainteks asli dan bagian plainteks yang diubah menjadi message digest dengan menggunakan hashing MD5.
2. Proses enkripsi message digest dengan menggunakan algoritma DES
3. Proses enkripsi plainteks asli dan cipherteks DES dengan menggunakan algoritma DES sehingga menghasilkan sebuat cipherteks baru.

Proses dekripsi

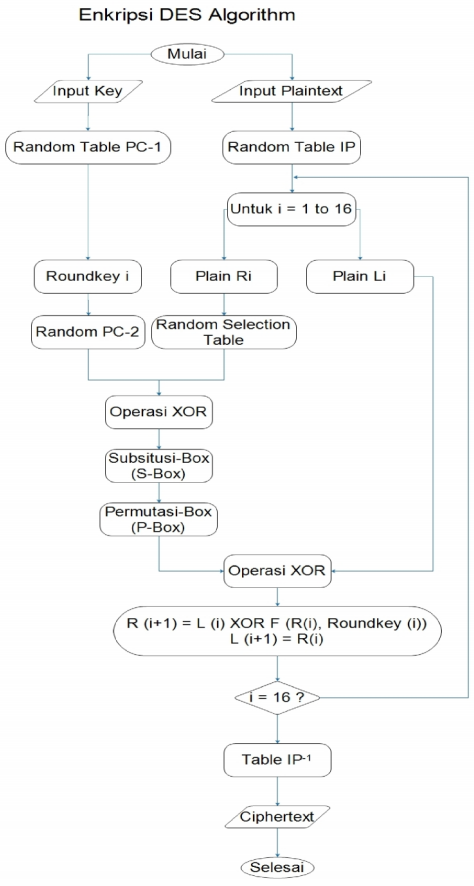
1. Cipherteks yang dihasilkan oleh algoritma DES akan di dekripsi menggunakan kunci sehingga menghasilkan plainteks asli dan cipherteks DES awal
2. Cipherteks DES akan didekripsikan sehingga menghasilkan message digest yang diperoleh dari hasil hashing MD5.
3. Plainteks asli akan dijadikan message digest dengan MD5 dan akan dicocokkan dengan hasil message digest dari dekripsi DES.

A. Proses peubah plainteks dengan MD5

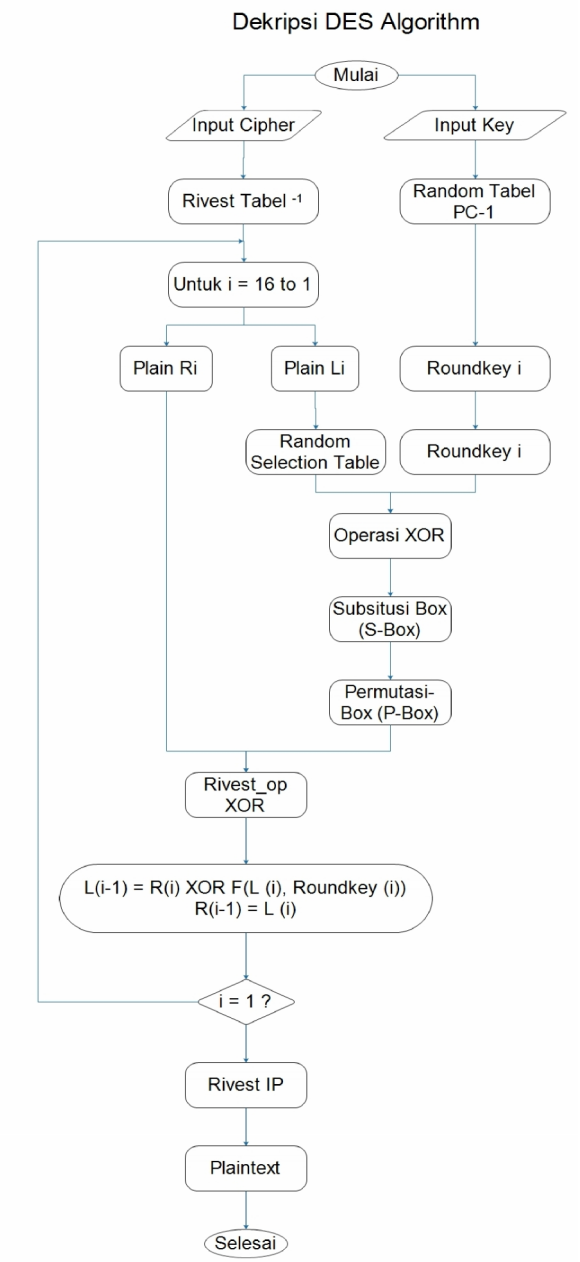


Gbr.6 Proses Peubah MD5

B. Proses enkripsi dan dekripsi DES algorithm



Gbr.7 Proses enkripsi algoritma DES



Gbr. 8 Proses dekripsi alogritma DES

IV. HASIL DAN PEMBAHASAN

Pada percobaan ini akan dilakukan proses enkripsi pesan dan dekripsi pesan dengan menggunakan model kemanan yang telah dirancang.

Pengujian dilakukan terhadap

Plaintext = COMPUTER

Hash MD5 = d19cbc472227d1e3d1d276c2cbc0e513

Plaintext akan diubah kedalam bentuk hashin (message digest) dengan menggunakan MD5, fungsi hash disini adalah sebagai media untuk validasi (tanda tangan digital).

Enkripsi DES akan dilakukan dengan menggunakan plaintext dan kunci

Plaintext = COMPUTER

Kunci = MUPERCOT

Konversi ke bilangan binner

TABEL I
KONVERSI BINNER

Plain Text	Bit	Kunci	Bit
C	01001100	**M**	00101100
O	00101001	**U**	00011001
M	00101100	**P**	00100110
P	00100110	**E**	01001001
U	00011001	**R**	00100011
T	00011010	**C**	01001100
E	01001001	**O**	00101001
R	00100011	**T**	00011010

PlainBit =
[0100110000101001001011000010011000011001000110100100100100011]

KunciBit =
[0010110000011001001001100100100100100011010011000010100100011010]

Sebelum putaran pertama terhadap blok plainteks akan dilakukan permutasi awal (initial permutation atau IP), tujuannya adalah mengacak plainteks sehingga urutan bit-bit didalamnya berubah, pengacakan dilakukan dengan menggunakan matriks permutasi awal berikut:

TABEL II
INITIAL PERMUTATION

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

Proses pengacakan ini akan menghasilkan plainbitIP

PlainBitIP =
0100000100110000000011011101001000000000100011110011101111010100 0

PlainBitIP memiliki bit sebanyak 64bit, bit-bit ini akan dipecah menjadi 2 bagian, masing-masing bagian memiliki bit sebanyak 32bit.

$$Lo = \begin{matrix}0100000100110000\\0000110111010010\end{matrix}$$

$$Ro = \begin{matrix}0000000010001110\\0111011110101000\end{matrix}$$

Pembangkit kunci menggunakan matriks permutasi kompresi PC-1 sebagai berikut

TABEL III
PC-1

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	46	38	30	22
14	6	61	53	45	37	29	21	13	5	28	20	12	4

Dalam permutasi ini tiap bit kedelapan (parity bit) dari delapan byte kunci diabaikan, sehingga menghasilkan permutasi sebanyak 56bit, dapat dikatakan panjang kunci DES 56bit.

KunciBitPC-1 =
00000000001010000101010110001001010000100101 11010110010

56bit ini kemudian dibagi menjadi 2 bagian kiri dan kanan yang masing-masing panjangnya 28bit.
KeyL0 = 00000000001010000101010110000
KeyR0 = 10010100001001011111010110010

Kedua bagian digeser kekiri (left shift) sepanjang satu atau dua bit tergantung pada tiap putaran, operasi pergeseran bersifat round-shift, jumlah pergeseran pada setiap putaran ditunjukkan pada table-tabel berikut:

TABEL IV
ROUND TABLE

r1	r2	r3	r4	r5	r6	r7	r8	r9	r10	r11	r12	r13	r14	r15	r16
1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

Enciphering putaran 1

Geser KeyLo dan KeyRo Ke kiri 1 Kolom sesuai dengan round table
KeyL1 = 00000000010100001010101100000
KeyR1 = 00101000010010111101011001010
Gabungkan KeyL1 dan KeyR1 menjadi Key1
Key1 =
000000000101000010101011000000101000010010111101011001010

TABEL V
PC-2

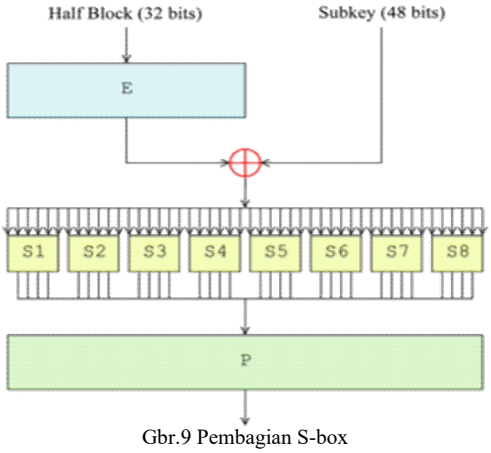
14	17	11	24	1	5	3	28	15	6	21	10
23	19	12	4	26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40	51	45	33	48
44	49	39	56	34	53	46	42	50	36	29	32

Key1PC-2 =
010100000011111000000000101000001111110010010 1000
Mengacak R0 Dengan Tabel seleksi E menjadi 48 bit

TABEL VI
E-SELECTION

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

R048bit =
000000000001010001011100001110101111111010101 0000
Operasi XOR antara Key1PC2 dengan R048bit
Key1PC2xorR048bit =
010100000010101001011100100110100000010001111 000
Membagi 8 hasil operasi xor
Bag1=010100, Bag2=000010,
Bag3=101001, Bag4=011100,
Bag5=100110, Bag6= 100000,
Bag7=010001, Bag8=111000.



Gbr.9 Pembagian S-box

Setiap kotak-S menerima masukan dengan menggunakan delapan buah kotak-S (S-box), S1 sampai S8. Setiap korak-S menerima masukan 6 bit dan menghasilkan keluaran 4 bit.
Hasil dari seluruh nilai substitusi ini adalah 32bit disebut dengan diefunction.
diefunction =01100001011001001011100111101111
Keluaran proses substitusi ini adalah diefunction. diefunction menjadi masukkan untuk proses permutasi. Tujuan permutasi adalah mengacak hasil proses S-box, permutasi dilakukan dengan menggunakan matriks permutasi P (P-box).

TABEL VII
PERMUTASI BOX

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

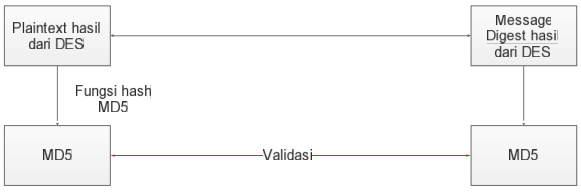
Hasil dari permutasi
diefunctionp =
00111001000100111111111010100101
XOR antara L0 dengan DieFunction Permutasi Sebagai R1 Dan R0 sebagai L1
R1 = L0xor*diefunctionp* =
01111000001000111111001101110111
L1 = R0 = 00000000100011100111011110101000
Proses enciphering akan terus dilakukan hingga 16 putaran.
Enciphering putaran akhir adalah sebagai berikut
Operasi XOR L15 dengan DieFunction Permutasi Sebagai R16 dan R15 sebagai L16
R16 = L15 XOR diefunctionP =
00001011110111101100110110100101
L16 = R15 =
10001100110000001111110000110100
L16 dan R16 Cipher =
1000110011000000111111000011010000001011110111101100110100101
Menggacak Cipher dengan table IP Invers
Cipher=
1000101010100000011011111110110000100101000001110011100011111 0

Membagi Cipher menjadi 8 bagian
Cipher[1]=10001010, Cipher[2]=10100000,
Cipher[3]=01101111, Cipher[4]=11101100,
Cipher[5]=00100101, Cipher[6]=00000111,
Cipher[7]=00111100, Cipher[8]=01111110.

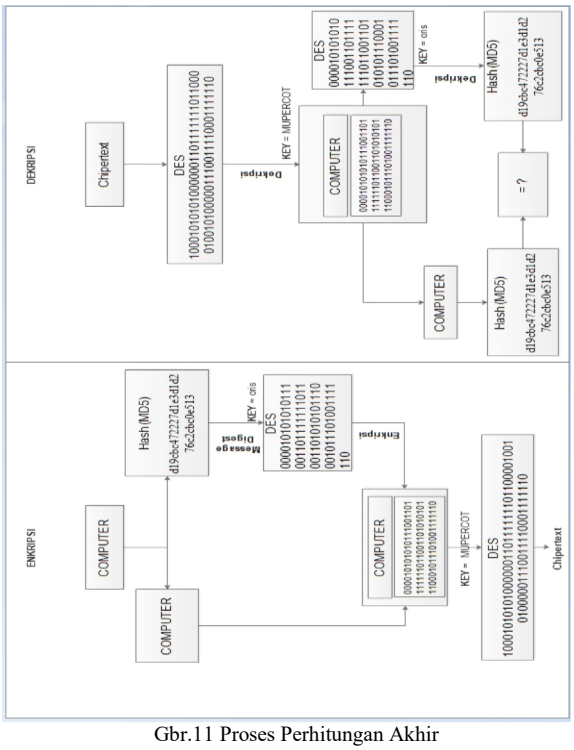
konversi Tiap Cipher menjadi ASCII
Cipher[1]=5
Cipher[2]=
Cipher[3]=ô
Cipher[4]=§
Cipher[5]=Q
Cipher[6]=\
Cipher[7]=”
Cipher[8]=ð

Proses dekripsi akan menggunakan
Ciphertext = 5 §Q\”ð
Kunci = MUPERCOT

Pada proses ini merupakan kebalikan dari round 16 ke 1. Proses ini akan menghasilkan plain teks asli dan akan menghasilkan hashing dari dekripsi DES, plain teks asli akan di ubah menjadi hashing , dan hashing sebagai tanda tangan digital akan mencocokkan dengan hashing dari hasil dekripsi DES, gambar dibawah untuk mempermudah memahami alur proses model enkripsi:



Gbr.10 Proses Validasi



Gbr.11 Proses Perhitungan Akhir

V. KESIMPULAN DAN SARAN

A. Kesimpulan

Model kemanan informasi ini memenuhi 2 kriteria kriptografi yaitu yaitu kerahasian (confidentiality) dan Nirpenyangkalan (non-repudiation).
Proses tanda tangan digital dilakukan oleh hashing (MD5) yang dihasilkan dari DES algorithm.

B. Saran

Perlu diteliti model yang mencakup 4 aspek kriptorafi yaitu : Kerahasiaan (confidentiality), Integritas data (data integrity), Otentikasi (authentication), Nirpenyangkalan (non-repudiation).

REFERENSI

[1] Kromodimoeljo, S. 2009. Teori dan Aplikasi Kriptografi. SPK IT Consulting.
[2] Munir, R, 2006. “Belajar Ilmu Kriptografi” Penerbit Andi, Yogyakarta.
[3] Paramitasari, A.D., Cahyani, N.D. & Wirayuda, T.A.B. 2009. Implementasi Digital Signature Untuk Verifikasi Data Menggunakan Digital Signature Algorithm (DSA), Telkom-U (2009).
[4] Santoso, Fakhrurrazi, 2012, Model Arsitektur Enterprise Untuk Mendukung Sistem Informasi Pada Universitas Gunung Leuser Kutacane Aceh Tenggara, Tesis, Medan, Universitas Sumatera Utara.