Triple Seven Block Cipher

Yusak Yuwono Awondatu

Program Studi Teknik Informatika

Institut Teknologi Bandung

Jalan Ganesha 10 Bandung, Indonesia

yusak.awondatu@gmail.com

***Abstract*—Komputer dengan kemajuannya sekarang menjadi alat komunikasi yang sangat cepat dan mudah diakses. Namun dibalik kemudahan tersebut, ada masalah keamanan dalam penyampaian informasi. Kriptografi sebagai salah satu cara untuk mengamankan informasi yang dikirim melalui computer juga berkembang sedemikian hingga untuk menyulitkan penyadap informasi. Salah satu teknik tersebut adalah dengan block cipher. Ada bermacam-macam algoritma block cipher baru yang telah dikembangkan dan salah satunya adalah algoritma (my algorithm name).**

Keywords—Kriptografi, Block Cipher, Feistel, Diffusion dan Confussion

I. PENDAHULUAN

Komunikasi merupakan hal yang sangat penting dalam kehidupan manusia. Namun sebagai manusia yang terbatas oleh ruang dan waktu, hal ini sangatlah menghambat upaya pengiriman pesan tersebut. Manusia ingin pesan yang ingin diberikan bisa dijangkau oleh individu lain pada jarak yang jauh sekalipun dengan waktu yang diharapkan. Oleh karena itu manusia berusaha untuk mengembangkan cara komunikasi yang bisa menembus batas ruang dan waktu tersebut.

cara komunikasi ini tidak lain adalah dengan menggunakan pihak perantara, baik objek maupun makhluk hidup lain. Telah diketahui ada banyak cara yang telah digunakan sejak dahulu kala. Pesan kode asap, kode cahaya, surat burung merpati, kurir, dan banyak cara lainnya.

Salah satu masalah yang muncul dari pengiriman pesan melalui pihak ketiga, adalah adanya interferensi. Ada kemungkinan pesan tidak sampai karena suatu kecelakaan, atau bisa saja karena kesengajaan suatu pihak yang berniat menggagalkan atau mencuri pesan tersebut, terlebih lagi jika pesan tersebut memiliki nilai informasi yang sangat penting / berharga.

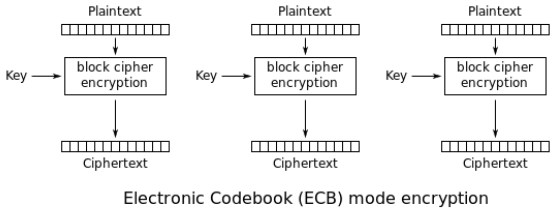
Oleh karena itu berkembanglah Kriptografi, ilmu seni untuk merahasiakan pesan. Pesan yang dikirimkan dikodekan sedemikian hingga agar pesan meskipun dapat dibaca, tidak dapat dimengerti siapapun selain pengirim dan penerima yang tahu cara membacanya. Dari teknik tradisional ribuan tahun yang memanfaatkan operasi operasi sederhana terhadap huruf dan angka dalam pesan, kini telah berkembang sangat drastis. Perkembangan drastis ini juga disebabkan oleh penemuan komputer sebagai alat yang dapat melakukan banyak operasi dengan cepat. Dengan komputer, dapat dikembangkan algoritma algoritma baru, yang meskipun tampak sederhana, namun memiliki tingkat keamanan yang tinggi.

II. DASAR TEORI

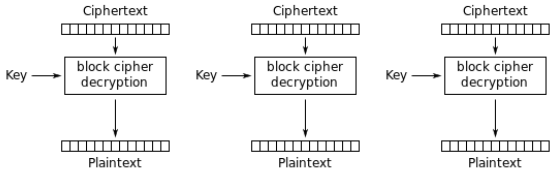
A. *Block Cipher*

Block cipher adalah salah satu teknik kriptografi modern karena operasi yang dilakukan mulai melibatkan elemen bit atau byte data dalam computer. Ada 4 beberapa macam operasi enkripsi-dekripsi dalam block cipher.

ECB(Electronic Codebook) adalah cara paling sederhana, yaitu mengenkripsikan blok plaintext dengan kunci secara konstan, sehingga tergolong kurang aman karena tidak begitu bervariasi.

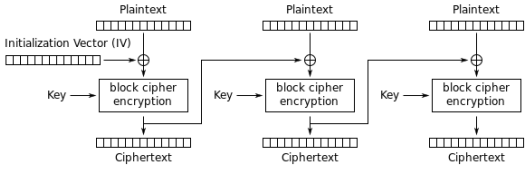


Electronic Codebook (ECB) mode encryption

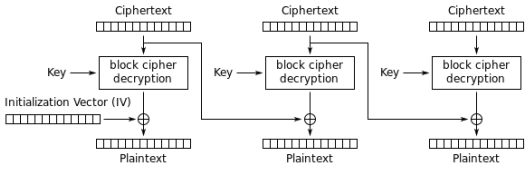


Electronic Codebook (ECB) mode decryption

CBC (Cipher Block Chaining), block plaintext pada iterasi ke n+1 menggunakan plaintext pada blok n dan kemudain di-XOR-kan dan dioperasikan dengan kunci



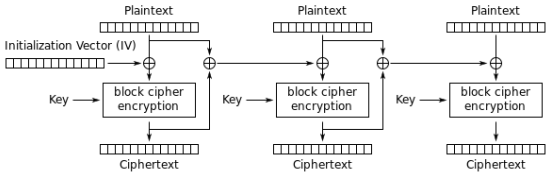
Cipher Block Chaining (CBC) mode encryption



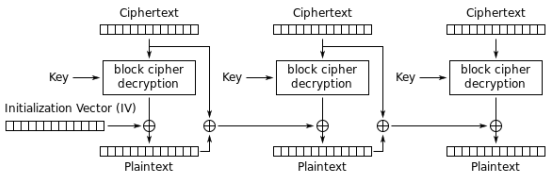
Cipher Block Chaining (CBC) mode decryption

.

PCBC (Propagating Cipher Block Chaining). Block plaintext n+1 diXORkan dengan blok plaintext ke n dan block ciphertext n barulah kemudian dioperasikan dengan key.

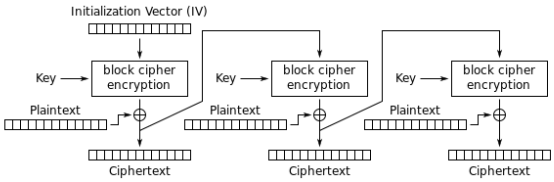


Propagating Cipher Block Chaining (PCBC) mode encryption

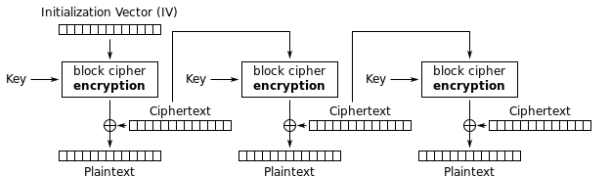


Propagating Cipher Block Chaining (PCBC) mode decryption

CFB(Cipher Feedback). Serupa dengan CBC, namun alur dibalik. Iterasi untuk decipher dilakukan dari belakang.

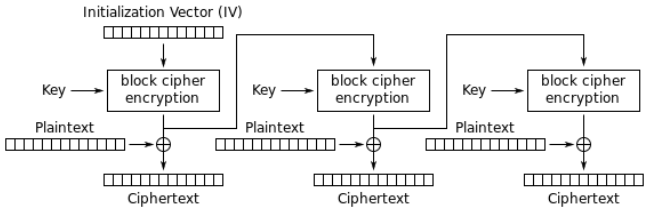


Cipher Feedback (CFB) mode encryption

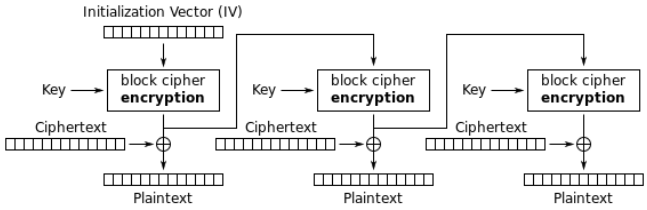


Cipher Feedback (CFB) mode decryption

OFB (Output Feedback). Operasi XOR yang simetris antara plaintext dan ciphertext

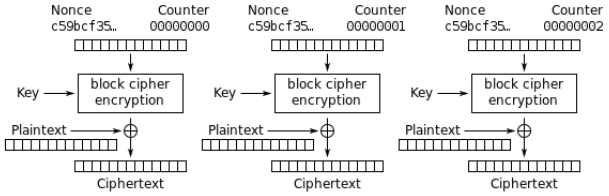


Output Feedback (OFB) mode encryption

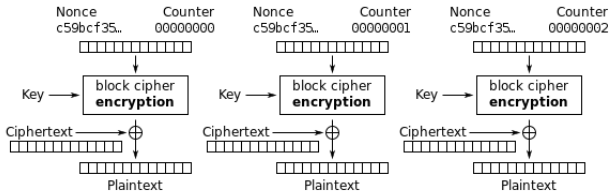


Output Feedback (OFB) mode decryption

Counter. Metode counter menggunakan angka yang dilibatkan dalam kunci enkripsi dan nilainya bertambah seiring banyaknya pesan yang dienkripsikan.



Counter (CTR) mode encryption



Counter (CTR) mode decryption

B. *Shannon's Confusion and Diffusion*

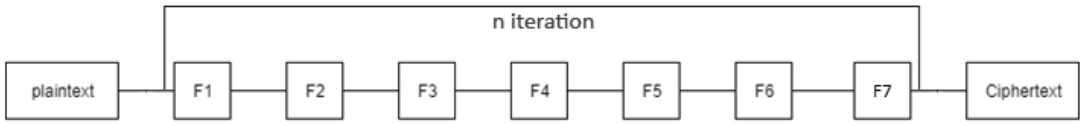
Salah satu prinsip utama dalam kriptografi adalah *Confusion* dan *Diffusion*. *Confusion* berarti membuat *ciphertext* yang cukup rumit, dan *diffusion* adalah mengacaukan struktur *plaintext* terhadap *ciphertext* sehingga menyusahkan teknik prediksi klasik(contohnya seperti prediksi kata dan huruf yang paling banyak digunakan). Salah satu cara untuk mendapatkan hal ini adalah dengan operasi substitusi dan permutasi. Karakter yang ada dalam blok dioperasikan terhadap S-box atau P-box untuk meningkatkan kerumitan ciphertext.

Dalam paper ini, yang digunakan adalah S-Box dengan basis hexadecimal

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
5	53	D1	00	ED	20	FC	B1	5B	6A	CB	BE	39	4A	4C	58	CF
6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

C. *Iterated Cipher*

Iterated Cipher sebenarnya hanyalah metode cipher standard, namun menambah kerumitan dalam algoritma karena melakukan iterasi enkripsi berulang kali.

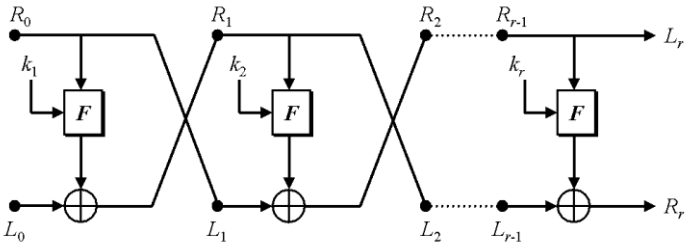


III. RANCANGAN DAN IMLPEMENTASI

Dengan beragamnya algoritma yang ada dalam block cipher, dapat dikembangkan algoritma baru yang beragam, salah satunya adalah dengan mengkombinasikan algoritma-algoritma yang sudah ada dalam teori yang telah disebutkan. Pada algoritma Triple Seven, akan digunakan 7 macam enkripsi yang dikombinasikan dengan 7 loop Feistel dan 7 kali iterasi. Ke tujuh macam algoritma yang digunakan dalam enkripsi akan memperkuat kerahasiaan pesan, namun dengan dekripsi yang tidak begitu rumit.

Seperti yang dijelaskan pada gambar, ke tujuh algoritma yang akan diiterasikan direpresentasi dengan F1, F2, F3 sampai F7. Penjelasan lebih detail mengenai masing masing algoritma Enkripsi adalah sebagai berikut :

- F1
  pada algoritma F1, blok plainteks akan disubstitusikan menggunakan S-box, langkah awal ini akan mengacaukan makna pesan secara langsung karena pesan menjadi tidak dapat diprediksi dengan metode penghitungan huruf dan kata karena pesan kini bercampur dengan karakter ASCII
- F2
  Shift baris. Setiap blok cipher adalah 128 bit, dibagi kedalam matriks 4x4, 8 bit/1 byte per sel matriks. Kemudian plainteks pada baris 0-1-2-3 akan disubstitusikan posisinya menjadi 3-2-0-1. Kemudian dilakukan iterasi untuk plainteks yang lain.
- F3
  invers bit blok pesan. Sebagai contoh jika pesan pada sel (3,4) adalah A, binary dari A adalah 01000001, kemudian di invers menjadi 10111110 sehingga berubah menjadi ¥.
- F4
  Shift kolom, sama halnya dengan Shift baris, pada matriks 4x4, plainteks dalam kolom disubstitusikan dari 0-1-2-3 menjadi 1-3-0-2.
- F5
  diberikan sebuah kunci eksternal, lalu melakukan enkrispi seperti pada ECB.
- F6
  melakukan substitusi sekali lagi, yaitu dengan substitusi byte pada kolom blok cipher x,y menjadi y,x.
- F7
  melakukan operasi Feistel. Operasi feistel dilakukan dengan membagi plainteks menjadi dua sisi kiri kanan, lalu melakukan operasi XOR pada salah satu sisi terhadap sisi lainnya, lalu mengoperasikan suatu kunci kepada sisi yang satunya lagi (atau bisa juga menggunakan blok n dan n+1)

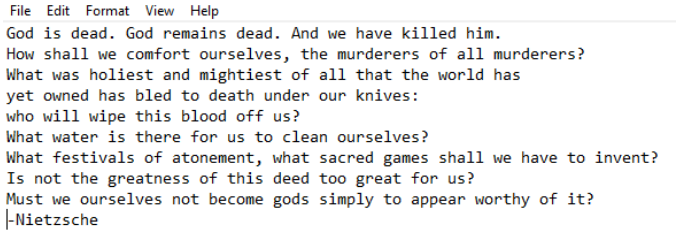


- Pada algoritma yang digunakan dalam paper ini, Feistel cipher digunakan dengan cara membagi plainteks menjadi dua sisi saja. melakukan operasi Caesar cipher terhadap sisi kanan, mengXORkan sisi kiri dengan sisi kanan, lalu menukar sisi kiri dengan sisi kanan. Ketiga proses ini akan dilakukan sebanyak 7 kali
- Setelah melakukan proses F1 sampai F7, proses diulangi sebanyak 7 kali lagi, baru kemudian hasil disimpan sebagai cipherteks.

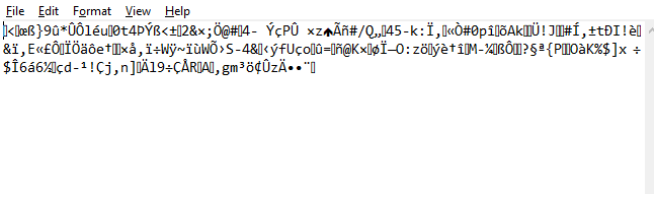
Algoritma untuk dekripsi dapat dilakukan dengan menjalankan proses F1 sampai F7 kembali, namun secara kebalikannya.

- F7
  tukar sisi kiri dan kanan, XORkan, lalu dekripsi Caesar cipher. Ulangi proses 7 kali
- F6
  substitusikan x,y dengan y,x
- F5
  dekripsi dengan XOR menggunakan key eksternal
- F4
  substitusikan kolom dari 0-1-2-3 pada cipherteks menjadi 2-0-3-1
- F3
  invers plainteks
- F2
  substitusikan baris dari 0-1-2-3 pada cipherteks menjadi 2-3-1-0
- F1
  substitusikan dengan Reverse S-Box

PENGUJIAN DAN ANALISIS



Algoritma diuji dengan pesan teks sepanjang 500 karakter, dengan key external adalah abcdefghijklmnop, dan menghasilkan cipherteks sebagai berikut



Dapat dilihat bahwa pesan yang sebelumnya adalah kutipan kalimat Nietzche dienkripsikan menjadi rentetan symbol dan huruf yang tidak memiliki makna. Jika dibandingkan dengan key yang hanyalah 16 huruf a sampai o, akan sulit membandingkan hubungan antara key dengan cipherteks sehingga algoritma memenuhi confusion dan diffusion.

Selain itu karena algoritma yang digunakan pada dasarnya tidak terlalu rumit, maka dapat melakukan enkripsi pada plainteks yang berisi ribuan karakter dengan cepat.

Penggunaan algoritma Triple Seven.dapat menguatkan keamanan pesan meskipun dengan langkah enkripsi yang tergolong *simple*, namun diperkuat dengan banyaknya iterasi dan looping sehingga dapat menguatkan algoritma kali terhadap serangan brute force.

Keuntungan lain dari algoritma ini adalah mudahnya pengembangangan karena penggunaan fungsi yang terstruktur dan memungkinkan adanya penambahan algoritma ke8 dan seterusnya, atau juga penambahan jumlah loop untuk membuat cipherteks yang lebih rumit

KESIMPULAN

Triple Seven adalah salah satu pengembangan algoritma Block Cipher yang memanfaatkan kombinasi algoritma block cipher yang sudah ada

REFERENSI

[1] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38a.pdf

[2] http://www.quadibloc.com/crypto/co040601.htm

[3] https://csrc.nist.gov/projects/block-cipher-techniques

[4] https://en.wikipedia.org/wiki/Rijndael_S-box

[5] http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/

[6] https://en.wikipedia.org/wiki/God_is_dead