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.

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
.

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

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

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

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

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.

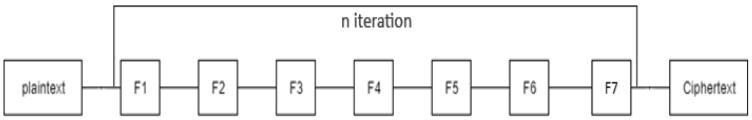
Dalam paper ini, yang digunakan adalah S-Box dengan basis hexadecimal

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 7x loop Feistel dan 7 kali iterasi. Ke tujuh macam algoritma yang digunakan dalam enkripsi akan memperkuat kerahasiaan pesan.



Seperti yang dijelaskan pada gambar diatas, algoritma enkripsi akan menggunakan 7 algoritma, yang direpresentasikan dengan F1 sampai F7. Penjelasan lebih detail mengenai masing masing algoritma Enkripsi adalah sebagai berikut :

- F1
  pada algoritma F1, blok plainteks akan disubstitusikan menggunakan S-box Rijndael berukruan 16x16. Karakter yang dienkripsikan akan disubstitusikan dengan karakter baru sesuai dengan nilai hexadecimal yang bersesuaian. Sebagai contoh jika karakter yang dienkripsikan adalah A. hexadecimal A adalah 41, maka disubstitusikan dengan karakter pada posisi (4,1) yaitu 09 [TAB]

	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

- F2
  Shifting baris. Setiap blok cipher berukuran 128 bit, dibagi kedalam matriks 4x4, 8 bit per sel matriks. Kemudian plainteks pada baris 0-1-2-3 akan disubstitusikan posisinya menjadi 3-2-0-1. Kemudian dilakukan iterasi untuk blok plainteks yang lain.

	0	1	2	3
0	A	B	C	D
1	E	F	G	H
2	I	J	K	L
3	M	N	O	P

	0	1	2	3
3	M	N	O	P
2	I	J	K	L
0	A	B	C	D
1	E	F	G	H

- F3
  invers bit blok pesan. Sebagai contoh jika pesan pada sel (3,4) adalah A, binary dari A adalah 01000001, karakter 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.

	0	1	2	3
0	A	B	C	D
1	E	F	G	H
2	I	J	K	L
3	M	N	O	P

	1	3	0	2
0	B	D	A	C
1	F	H	E	G
2	J	L	I	K
3	N	P	M	O

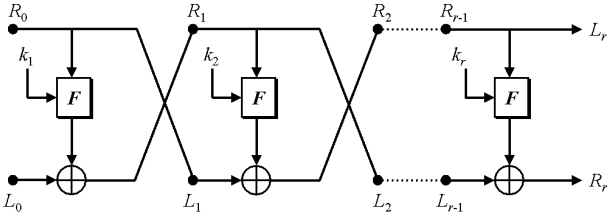
- F5
  diberikan sebuah kunci eksternal, lalu melakukan XOR blok plainteks dengan kunci seperti vigenere cipher.

- F6
  melakukan substitusi sekali lagi, yaitu dengan substitusi byte pada blok cipher (x,y) dengan (y,x).

	0	1	2	3
0	A	B	C	D
1	E	F	G	H
2	I	J	K	L
3	M	N	O	P

	0	1	2	3
0	A	E	I	M
1	B	F	J	N
2	C	G	K	O
3	D	H	L	P

- F7
  melakukan operasi Feistel. Operasi feistel dilakukan



dengan membagi plainteks menjadi dua bagian, yaitu plainteks L dan R, lalu melakukan operasi enkripsi sisi R dengan Caesar cipher, kemudian operasi L⊕R, lalu L ditukar dengan R. operasi feistel dapat dilakukan berulang kali untuk membuat teks semakin rumit dan pada contoh ini dilakukan 7x looping.

- 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 terbalik.

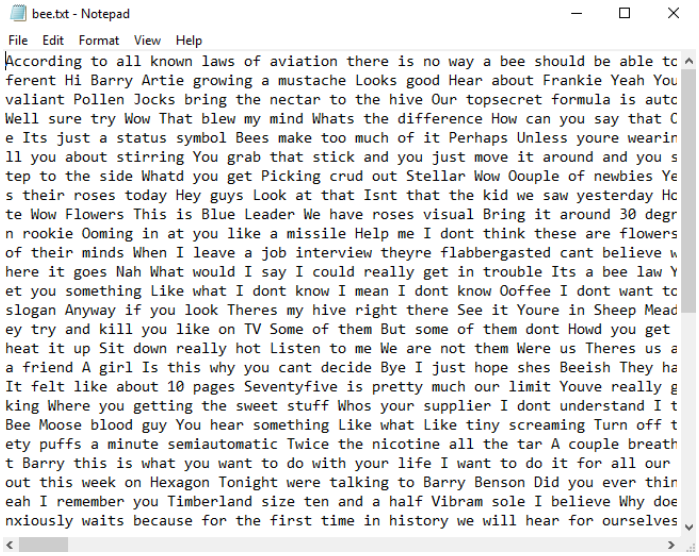
- F7
  tukar sisi L dan R, L⊕R, dekripsi R dengan Caesar cipher, loop proses 7 kali
- F6
  substitusikan sel (x,y) dengan (y,x)
- F5
  dekripsi dengan XOR menggunakan key eksternal
- F4
  substitusikan kolom dari 0-1-2-3 pada cipherteks menjadi 2-0-3-1 agar kembali menjadi posisi 0-1-2-3 dalam plainteks
- F3
  operasi invers bit plainteks
- F2
  substitusikan baris dari 0-1-2-3 pada cipherteks menjadi 2-3-1-0 agar kembali menjadi posisi 0-1-2-3 dalam plainteks
- F1
  substitusikan dengan Inverse S-Box seperti di bawah berikut

	00	01	02	03	04	05	06	07	08	09	0a	0b	0c	0d	0e	0f
00	52	09	6a	d5	30	36	a5	38	bf	40	a3	9e	81	f3	d7	fb
10	7c	e3	39	82	9b	2f	ff	87	34	8e	43	44	c4	de	e9	cb
20	54	7b	94	32	a6	c2	23	3d	ee	4c	95	0b	42	fa	c3	4e
30	08	2e	a1	66	28	d9	24	b2	76	5b	a2	49	6d	8b	d1	25
40	72	f8	f6	64	86	68	98	16	d4	a4	5c	cc	5d	65	b6	92
50	6c	70	48	50	fd	ed	b9	da	5e	15	46	57	a7	8d	9d	84
60	90	d8	ab	00	8c	bc	d3	0a	f7	e4	58	05	b8	b3	45	06
70	d0	2c	1e	8f	ca	3f	0f	02	c1	af	bd	03	01	13	8a	6b
80	3a	91	11	41	4f	67	dc	ea	97	f2	cf	ce	f0	b4	e6	73
90	96	ac	74	22	e7	ad	35	85	e2	f9	37	e8	1c	75	df	6e
a0	47	f1	1a	71	1d	29	c5	89	6f	b7	62	0e	aa	18	be	1b
b0	fc	56	3e	4b	c6	d2	79	20	9a	db	c0	fe	78	cd	5a	f4
c0	1f	dd	a8	33	88	07	c7	31	b1	12	10	59	27	80	ec	5f
d0	60	51	7f	a9	19	b5	4a	0d	2d	e5	7a	9f	93	c9	9c	ef
e0	a0	e0	3b	4d	ae	2a	f5	b0	c8	eb	bb	3c	83	53	99	61
f0	17	2b	04	7e	ba	77	d6	26	e1	69	14	63	55	21	0c	7d

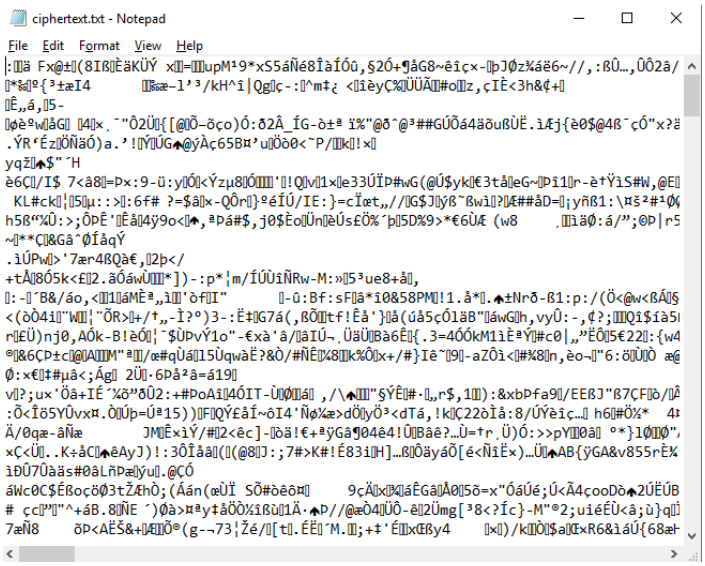
PENGUJIAN DAN ANALISIS

1. Pengujian Frekuensi Karakter

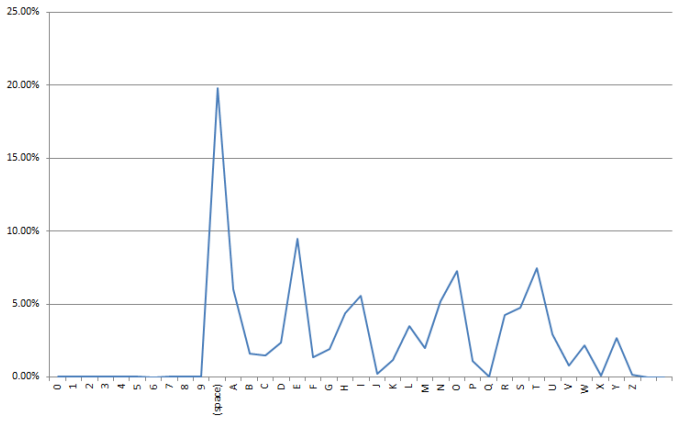
Algoritma diuji dengan pesan teks sepanjang 46211 karakter, di padding dalam algoritma menjadi 46224 agar sesuai jumlah blok, yang kelipatan 256 bit



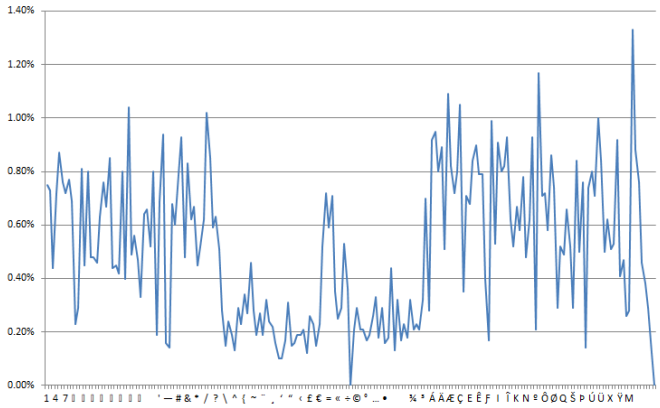
Plainteks demikian didekripsikan menghasilkan cipherteks sebagai berikut



Jika menggunakan penghitungan frekuensi karakter maka plainteks akan menghasilkan grafik frekuensi karakter sebagai berikut



Sedangkan cipherteks akan menghasilkan grafik frekuensi karakter sebagai berikut

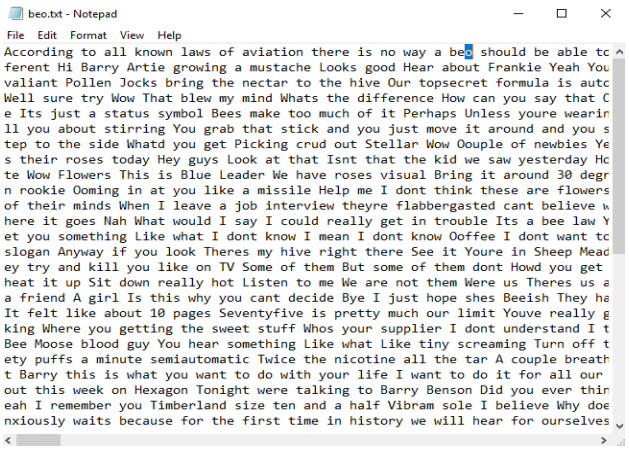


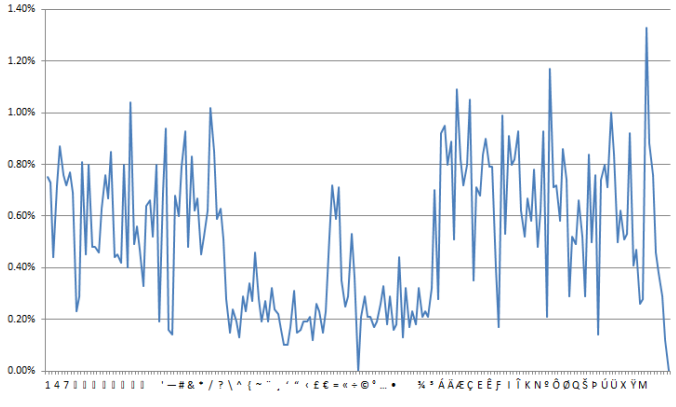
Dengan algoritma yang digunakan, plainteks yang semula terdiri dari 37 karakter (A-Z, 0-9, dan spasi) berubah dan disebarkan menjadi 256 karakter ASCII dengan frekuensi per karakter hanya berkisar pada 1.4%-0% dan frekuensi kemunculan karakter yang diratakan. Dibandingkan dengan plainteks sebelumnya yang menonjolkan banyaknya frekuensi karakter spasi, A, E, I, O, dan T.

Hal ini menyatakan bahwa algoritma memiliki confussion dan diffusion yang kuat

2. Pengujian Pengubahan Karakter

Pada pengujian terhadap pengubahan pesan, semisalnya pesan mengalami hanya satu pengubahan karakter seperti pada contoh mengubahan satu bee menjadi beo

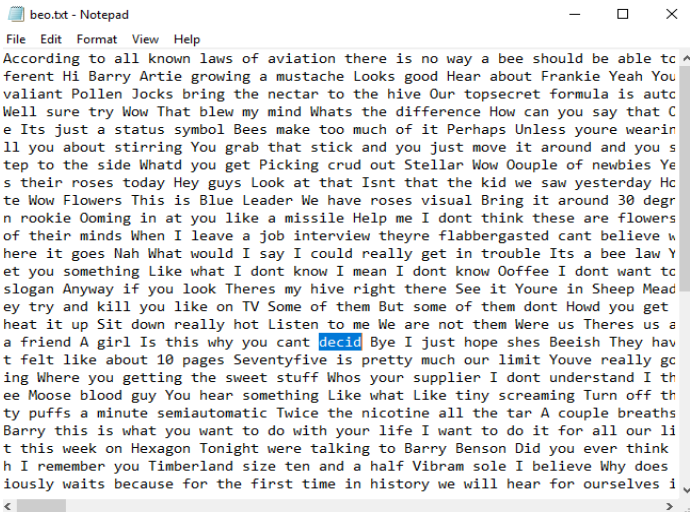


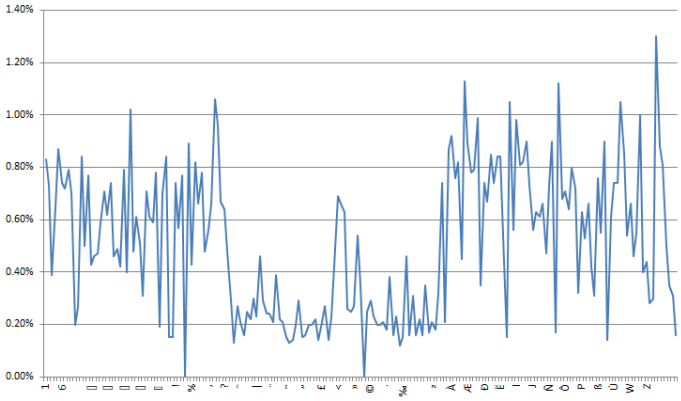


Maka grafik karakter yang dihasilnya tidak akan jauh berbeda dengan grafik karakter tanpa pengubahan. Hal ini menandakan bahwa algoritma kan memiliki celah terhadap pengubahan pesan tanpa mengubah jumlah karakternya.

3. Pengujian Pengurangan Jumlah Karakter

Namun jika dilakukan penambahan atau pengurangan karakter pada pesan, seperti pada contoh menghilangkan satu huruf dari kata dedice





Grafik menghasilkan frekuensi karakter yang memiliki banyak perbedaan dibandingkan dengan plainteks aslinya.

Hal ini menyatakan bahwa algoritma akan sensitive terhadap penambahan atau pengurangan karakter dalam pesan.

KESIMPULAN

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

Algoritma yang dibuat memiliki confussion dan diffusion yang kuat dan cukup sensitif terhadap pengubahan pesan yang sifatnya menambah atau mengurangi jumlah pesan yang dikirim.

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/