Modifikasi Kunci Penyandian Pada Algoritma Alberti Cipher

Mira Yunarti [1)]

1) Program Studi Teknik Informatika ITB, Bandung 40135, email: if14009@students.if.itb.ac.id

Abstract – *Makalah ini membahas mengenai salah satu algoritma kriptografi yang termasuk paling klasik, yaitu Alberti Cipher. Alberti Cipher adalah algoritma pertama yang memperkenalkan polialfabetik, dimana setiap huruf bersesuaian tidak hanya dengan satu huruf lain. Pada makalah ini juga akan dibahas mengenai proses modifikasi yang dilakukan terhadap kunci Alberti Cipher sehingga algoritma menjadi lebih rumit dan kunci tidak mudah ditebak. Proses modifikasi yang dilakukan ialah dengan melakukan sejumlah operasi pada kunci sebelum kunci digunakan dalam proses enkripsi dan dekripsi pesan.*

Kata Kunci*: kriptografi, algoritma kriptografi klasik, Alberti Cipher.*

1. PENDAHULUAN

Sejak dahulu kala data dan informasi sangat penting dijaga keamanannya, karena bagaimanapun juga data atau informasi merupakan benda yang tidak boleh diketahui pihak-pihak tertentu yang tidak memiliki wewenang terhadap data dan informasi tersebut, terutama saat data atau informasi tersebut disampaikan kepada pihak-pihak lain. Sedikit saja pesan yang bocor ke pihak lain, bahkan dapat sangat merugikan pihak yang mengirimkan pesan, misalnya pada saat jaman perang.

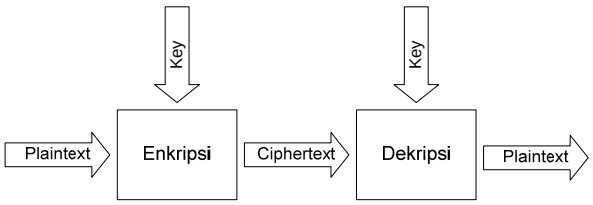
Aspek-aspek keamanan yang dibutuhkan pada saat terjadi transmisi data adalah sebagai berikut :

1. *Confidentiality*, yaitu kemampuan untuk menjaga agar isi pesan yang ditransmisikan tidak diketahui oleh pihak-pihak yang tidak berhak untuk mengetahuinya.
2. *Data integrity*, yaitu kemampuan untuk menjamin bahwa pesan masih utuh saat sampai ke penerima, atau dengan kata lain pesan tidak dimanipulasi saat di perjalanan.
3. *Authentication*, yaitu kemampuan untuk mengidentifikasi kebenaran pihak-pihak yang terlibat dalam komunikasi dan kebenaran sumber pesan.
4. *Non-repudiation*, yaitu kemampuan untuk mencegah pihak-pihak yang terlibat dalam komunikasi melakukan penyangkalan terhadap komunikasi yang dilakukan.

Inti dari keempat aspek di atas adalah bagaimana untuk melakukan komunikasi yang aman. Keempat aspek di atas dapat diselesaikan dengan kriptografi.

Kriptografi berasal dari bahasa Yunani yang terdiri dari 2 kata, yaitu *kryptos* yang berarti menyembunyikan dan *grafi* yang berarti menulis, dan arti seutuhnya adalah seni dan ilmu untuk menyembunyikan pesan menjadi kode-kode yang tidak dapat dibaca oleh pihak yang tidak berhak. Menurut catatan sejarah, kriptografi sudah ada sejak dahulu kala. Kriptografi sudah digunakan oleh bangsa Mesir sejak 4000 tahun yang lalu oleh raja-raja Mesir pada saat perang untuk mengirimkan pesan rahasia kepada panglima perangnya melalui kurir.

Dalam kriptografi, pihak yang saling berkirim pesan akan melakukan dua proses, yaitu proses enkripsi yang dilakukan oleh pengirim pesan dan proses dekripsi yang dilakukan oleh penerima pesan. Proses enkripsi adalah proses penyandian pesan asli (*plainteks*) menjadi pesan rahasia (*ciphertext*). Kemudian cipherteks dikirimkan kepada penerima pesan melalui saluran komunikasi terbuka. Pada saat penerima pesan menerima cipherteks, maka pesan rahasia tersebut diubah lagi menjadi pesan asli melalui proses dekripsi sehingga pesan tadi dapat dibaca kembali oleh penerima pesan. Secara umum, proses enkripsi dan dekripsi dapat dilihat pada Gambar 1.



Gambar-1 Proses Enkripsi dan Dekripsi

Kedua proses tersebut menggunakan kunci dalam pengubahan pesan, dimana kunci tersebut diterapkan menggunakan suatu algoritma. Secara umum terdapat 2 jenis algoritma kriptografi, yaitu algoritma kriptografi klasik dan algoritma kriptografi modern.

1.1 Algoritma Kriptografi Klasik

Algoritma kriptografi klasik adalah algoritma penyandian yang basisnya adalah karakter, yang berarti pesan disandikan per karakter. Karena berbasiskan karakter, maka hanya sedikit operasi yang dapat diterapkan untuk membuat sebuah algoritma cipher. Ada dua macam metode yang

digunakan untuk algoritma kriptografi klasik, yaitu :

1. Substitusi, merupakan penyandian dengan cara mengganti huruf pesan aslinya ke huruf lain sebagai pesan sandinya, baik setiap satu huruf atau setiap kelompok huruf atau bisa juga kombinasi dari itu.

2. Transposisi, merupakan penyandian dengan cara mengubah letak dari huruf-huruf pada pesan yang akan disandikan. Dan untuk membaca pesan aslinya kembali, cukup dengan mengembalikan letak dari huruf-huruf pada pesan tersebut berdasarkan kunci dan algoritma pergeseran huruf yang telah disepakati pihak pengirim dan penerima pesan.

Terdapat beberapa algoritma kriptografi klasik, seperti *Vigenere Cipher*, *Hill Cipher*, *Playfair Cipher*, dan lain-lain, termasuk *Alberti Cipher* yang dibahas dalam makalah ini.

1.2 Algoritma Kriptografi Modern

Algoritma kriptografi modern, basisnya adalah bit, yaitu semua data dan informasi dinyatakan dalam bentuk rangkaian bit, dan algoritma enkripsi-dekripsi memproses data tersebut dalam rangkaian bit. Operator bit yang sering digunakan dalam algoritma kriptografi modern adalah operator XOR.

Algoritma yang beroperasi dalam bentuk bit terdiri dari 2 jenis, yaitu :

1. Cipher Aliran (*Stream Cipher*)

Dalam jenis cipher ini, algoritma kriptografi melakukan operasi terhadap plainteks atau cipherteks dalam bentuk bit tunggal. Atau dengan kata lain plainteks dienkripsikan bit per bit. Contoh dari cipher aliran adalah *Vernam Cipher* dan RS4.

2. Cipher Blok (*Block* Cipher)

Pada cipher ini, bit-bit plainteks dibagi ke dalam blok-blok bit dengan panjang yang sama. Dan proses enkripsi-dekripsi dilakukan terhadap blok bit, bukan terhadap bit tunggal. Contoh dari cipher ini adalah DES, GOST, RC5, dan AES.

Dalam kriptografi, algoritma penyandian yang bagus dan dikatakan aman apabila untuk memecahkannya dibutuhkan waktu yang lama dan biaya yang besar. Alberti Cipher yang merupakan salah satu algoritma kriptografi klasik, memiliki ide yang menarik dalam proses penyandian pesannya. Namun algoritma tersebut kurang cocok digunakan, karena algoritmanya sangat simple dan dapat dipecahkan dengan bantuan komputer pada saat ini. Maka dilakukan modifikasi pada kuncinya, sehingga algoritma menjadi lebih rumit.

2. DESKRIPSI UMUM ALBERTI CIPHER

Menjelang abad ke 15 , kriptografi dan kriptanalis tersebar luas di Eropa. Pada saat itu seluruh teknik enkripsi membutuhkan komputasi manual dengan menuliskan tabel. Seluruh algoritma substitusi adalah monoalfabetik dimana setiap huruf dipetakan ke hanya satu huruf juga. Dan metode ini mudah dipecahkan dengan analisis frekuensi kemunculan huruf.

Keadaan ini berubah sejak Leon Battista Alberti (1404-1472) mengembangkan suatu mesin cipher untuk enkripsi secara mekanik. Mesin ini berdasarkan algoritma Caesar Cipher. Selama tahun 1460an Alberti mengembangkan metode ini dan pada tahun 1467 Alberti mempublikasikan cipher polialfabetik pertama dan mendesain sebuah piringan cipher untuk menyederhanakan proses, seperti yang terlihat pada Gambar 2.

Gambar-2 Piringan Alberti Cipher

Alberti mendeskripsikan penemuannya :

> *"I make two circles out of copper plates. One, the larger, is called stationary, the smaller is called movable. The diameter of the stationary plate is one-ninth greater than that of the movable plate. I divide the circumference of each circle into 24 equal parts [called] cells. In the various cells of the larger circle I write the capital letters, one at a time in red, in the usual order of the letters [whilst those around the movable circle are] not in regular order like the stationary characters, but scattered at random. [I then] place the smaller circle upon the larger so that a needle driven through the centres of both may serve as the axis of both and the movable plate may be revolved around it." (Alberti, "Trattati in Cifra", 1470, cited in Kahn, 1996, pp127-128.)*

Alat penyandian terdiri dari dua piringan yang terbuat dari metal, disusun sedemikian sehingga piringan yang satu (yang terletak di dalam) dapat bergerak memutar sedangkan yang satu lagi (yang terletak di luar) statis Piringan luar terdiri dari huruf-huruf dalam alfabet Latin yang disusun berurutan melingkar mengikuti

pinggiran piringan, sedangkan piringan dalam terdiri dari huruf-huruf dalam alphabet Latin yang disusun acak melingkar mengikuti pinggiran piringan. Untuk mengenkripsi, cukup dengan memutar piringan dalam sehingga setiap huruf bersesuaian dengan huruf di piringan luar. Sandi adalah kumpulan huruf di piringan dalam yang mengikuti pesan asli. Penerima sandi cukup mengetahui satu pasangan huruf yang bersesuaian, memutar piringan menurut pasangan huruf yang diketahui, dan mencocokkan huruf-huruf lainnya. Agar lebih kompleks, piringan dapat diubah selama proses enkripsi sehingga satu alphabet berbeda digunakan secara periodik.

Pada abad ke 16, Giovanni Battista Porta menggunakan sistem ini untuk mengimplementasikan sebuah algoritma. Teknik ini didasarkan dari teknik *polyalphabetic*, dan dengan menggunakan tabel Porta, seperti terlihat pada Gambar-3, yang berbasis 26 karakter alphabet. Teknik ini menggunakan satu kata kunci yang dituliskan berulang sepanjang teks asli. Lalu kata kunci tersebut diganti dengan angka-angka sesuai urutan abjad (A=0, B=1, C=2, dan seterusnya). Kemudian huruf-huruf pada teks asli disesuaikan dengan angka, dan dicari huruf yang memenuhi keduanya dari tabel Porta (sesuai dengan huruf pada teks asli dan angka kunci). Kumpulan huruf inilah yang merupakan pesan sandi.

		Equivalent to the outer disc																								
		a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
	0	A	L	B	E	R	T	I	C	P	H	D	F	G	H	J	K	M	N	O	S	U	V	W	X	Y	Z
	1	Z	A	L	B	E	R	T	I	C	P	H	D	F	G	H	J	K	M	N	O	S	U	V	W	X	Y
N	2	Y	Z	A	L	B	E	R	T	I	C	P	H	D	F	G	H	J	K	M	N	O	S	U	V	W	X
u	3	X	Y	Z	A	L	B	E	R	T	I	C	P	H	D	F	G	H	J	K	M	N	O	S	U	V	W
m	4	W	X	Y	Z	A	L	B	E	R	T	I	C	P	H	D	F	G	H	J	K	M	N	O	S	U	V
b	5	V	W	X	Y	Z	A	L	B	E	R	T	I	C	P	H	D	F	G	H	J	K	M	N	O	S	U
e	6	U	V	W	X	Y	Z	A	L	B	E	R	T	I	C	P	H	D	F	G	H	J	K	M	N	O	S
r	7	S	U	V	W	X	Y	Z	A	L	B	E	R	T	I	C	P	H	D	F	G	H	J	K	M	N	O
	8	O	S	U	V	W	X	Y	Z	A	L	B	E	R	T	I	C	P	H	D	F	G	H	J	K	M	N
o	9	N	O	S	U	V	W	X	Y	Z	A	L	B	E	R	T	I	C	P	H	D	F	G	H	J	K	M
f	10	M	N	O	S	U	V	W	X	Y	Z	A	L	B	E	R	T	I	C	P	H	D	F	G	H	J	K
	11	K	M	N	O	S	U	V	W	X	Y	Z	A	L	B	E	R	T	I	C	P	H	D	F	G	H	J
S	12	J	K	M	N	O	S	U	V	W	X	Y	Z	A	L	B	E	R	T	I	C	P	H	D	F	G	H
h	13	H	J	K	M	N	O	S	U	V	W	X	Y	Z	A	L	B	E	R	T	I	C	P	H	D	F	G
i	14	G	H	J	K	M	N	O	S	U	V	W	X	Y	Z	A	L	B	E	R	T	I	C	P	H	D	F
f	15	F	G	H	J	K	M	N	O	S	U	V	W	X	Y	Z	A	L	B	E	R	T	I	C	P	H	D
t	16	D	F	G	H	J	K	M	N	O	S	U	V	W	X	Y	Z	A	L	B	E	R	T	I	C	P	H
s	17	H	D	F	G	H	J	K	M	N	O	S	U	V	W	X	Y	Z	A	L	B	E	R	T	I	C	P
	18	P	H	D	F	G	H	J	K	M	N	O	S	U	V	W	X	Y	Z	A	L	B	E	R	T	I	C
	19	C	P	H	D	F	G	H	J	K	M	N	O	S	U	V	W	X	Y	Z	A	L	B	E	R	T	I
	20	I	C	P	H	D	F	G	H	J	K	M	N	O	S	U	V	W	X	Y	Z	A	L	B	E	R	T
	21	T	I	C	P	H	D	F	G	H	J	K	M	N	O	S	U	V	W	X	Y	Z	A	L	B	E	R
	22	R	T	I	C	P	H	D	F	G	H	J	K	M	N	O	S	U	V	W	X	Y	Z	A	L	B	E
	23	E	R	T	I	C	P	H	D	F	G	H	J	K	M	N	O	S	U	V	W	X	Y	Z	A	L	B
	24	B	E	R	T	I	C	P	H	D	F	G	H	J	K	M	N	O	S	U	V	W	X	Y	Z	A	L
	25	L	B	E	R	T	I	C	P	H	D	F	G	H	J	K	M	N	O	S	U	V	W	X	Y	Z	A

Gambar-3 tabel Porta

3. PROSES ENKRIPSI DENGAN ALGORITMA ALBERTI CIPHER

Misalkan teks asli “This is a test of alberti” akan disandikan menggunakan algoritma Alberti Cipher dengan kata kunci CATWALK serta tabel Porta. Proses enkripsi dimulai dengan menuliskan kata kunci secara berulang di bawah pesan asli.

this is a test of alberti
CATW AL K CATW AL KCATWAL

Langkah selanjutnya adalah mengganti huruf-huruf pada kata kunci dengan angka-angka yang ekivalen dengan nomer urutan abjadnya, misalnya A dengan 0, B dengan 1, C dengan 2, dan seterusnya.

T h i s i s a t e s t o f a l b e r t i
2 0 19 22 0 11 10 2 0 19 22 0 11 10 2 0 19 22 0 11

Pasangan tersebut menunjukkan hubungan koordinat pada tabel Porta, dimana setiap pasangan akan digantikan dengan satu karakter sesuai koordinat tersebut. Koordinat didefinisikan dengan karakter pesan asli sebagai identitas kolom dan angka sebagai indeks baris, misalnya (t,2) = N, (h,0) = C, dan seterusnya.

Maka hasilnya adalah sebagai berikut :

this is a test of alberti
NCKW PC M NRZX JU MHLFVSX

Pesan sandi yang dikirimkan adalah NCKW PC M NRZX JU MHLFVSX. Pesan ini tidak akan dapat terbaca, karena huruf yang sama pada pesan sandi belum tentu merupakan huruf yang sama pada pesan asli. Dengan kata lain, metode analisis frekuensi tidak dapat digunakan untuk mendekripsi pesan sandi ini.

4. PROSES DEKRIPSI DENGAN ALGORITMA ALBERTI CIPHER

Untuk mendekripsi pesan sandi, lakukan lagi langkah sebelumnya, yaitu menuliskan kata kunci secara berulang di bawah pesan sandi, lalu ubah kata kunci dengan angka yang bersesuaian dengan nomer urut abjadnya.

N C K W P C M N R Z X J U M H L F V S X
C A T W A L K C A T W A L K C A T W A L
2 0 19 22 0 11 10 2 0 19 22 0 11 10 2 0 19 22 0 11

Karakter-karakter pesan asli dapat dicari dalam tabel dengan cara mencari koordinat yang bersesuaian dengan pasangan huruf pesan sandi dengan angka. Pertama cari baris sesuai angka, lalu telusuri ke kanan hingga menemukan huruf pada pesan sandi, dan dilihat berada pada kolom huruf apa. Huruf tersebut merupakan huruf pesan asli. Contohnya (N,2) = t, (C,0) = h, dan seterusnya.

Dengan cara seperti itu, akan didapatkan pesan asli “this is a test of alberti”. Pesan ini sesuai dengan pesan yang dienkripsi.

5. MODIFIKASI KUNCI ALBERTI CIPHER

Cipher Alberti di atas kurang kuat karena proses penyandiannya sangat sederhana dan dapat dengan mudah dipecahkan dengan bantuan teknologi

komputer jaman sekarang. Proses modifikasi dilakukan terhadap kunci, sehingga enkripsi dan dekripsi menjadi lebih rumit dan kunci tidak dapat ditebaj dengan mudah.

5.1 Proses Enkripsi

Misalkan teks asli adalah “kriptografi”, kata kunci adalah “catwalk”, dan digunakan tabel Porta seperti pada tabel 1. Teknik enkripsi yang dilakukan adalah sebagai berikut :

1. Kata kunci “catwalk” dikonversikan ke bilangan-bilangan sesuai urutan abjad, menjadi : 2 -0-19-22 -0-11- 10.

2. Susunan bilangan kunci ini dibentuk ke matriks persegi yang terdekat yang sesuai dengan jumlah banyaknya bilangan. Misalnya dalam contoh ini ada 9 buah bilangan, maka matriks persegi yang terdekat adalah matriks 3 x 3 (9 buah bilangan). Untuk ruang matriks yang masih kosong diisi dengan perulangan bilangan dari awal. Setelah matriks terbentuk, lalu matriks ini dikalikan dengan matriks yang sama (matriks kuadrat).

$$\begin{bmatrix} 2 & 0 & 19 \\ 22 & 0 & 11 \\ 10 & 2 & 0 \end{bmatrix} X \begin{bmatrix} 2 & 0 & 19 \\ 22 & 0 & 11 \\ 10 & 2 & 0 \end{bmatrix} = \begin{bmatrix} 194 & 38 & 38 \\ 154 & 22 & 418 \\ 64 & 0 & 212 \end{bmatrix}$$

3. Bilangan-bilangan yang didapatkan dari hasil perkalian matriks diurutkan secara unik. Hal ini untuk lebih mengacaukan kunci. Maka untuk contoh ini diperoleh bilangan-bilangan 0-22-38-64-154-194-212

4. Langkah selanjutnya adalah melakukan operasi modulo 26 terhadap bilangan-bilangan hasil pengurutan pada langkah 3. Untuk contoh ini :

   0-22-38-64-154-194-212
   0-22-12-12- 24 -12 - 4,

   Dimana baris pertama adalah bilangan yang dihasilkan pada langkah 3, dan baris kedua merupakan hasil bilangan tersebut dimodulo 26.

5. Hasil operasi modulo adalah kunci yang sebenarnya. Kunci ini disejajarkan dengan teks asli secara berulang. Pada contoh ini :

k	r	i	p	t	o	g	r	a	f	i
0	22	12	12	24	12	4	0	22	12	12

Teks asli dan kunci yang baru, disesuaikan menggunakan tabel Porta hingga mendapatkan satu huruf baru untuk setiap pasangan. Misalnya huruf yang terdapat di kolom k dan baris 0 adalah huruf d, huruf yang terdapat di kolom r baris 22 adalah huruf v, dan seterusnya hingga didapatkan teks cipher : “dvwevbbnrsw” untuk teks asli “kriptografi”.

5.2 Proses Dekripsi

Untuk mendekripsi pesan, dilakukan langkah-langkah sebagai berikut :

1. Kata kunci “catwalk” dikonversikan ke bilangan-bilangan sesuai urutan abjad, menjadi : 2 -0-19-22 -0-11- 10.

2. Susunan bilangan kunci ini dibentuk ke matriks persegi yang terdekat yang sesuai dengan jumlah banyaknya bilangan. Misalnya dalam contoh ini ada 9 buah bilangan, maka matriks persegi yang terdekat adalah matriks 3 x 3 (9 buah bilangan). Untuk ruang matriks yang masih kosong diisi dengan perulangan bilangan dari awal. Setelah matriks terbentuk, lalu matriks ini dikalikan dengan matriks yang sama (matriks kuadrat).

$$\begin{bmatrix} 2 & 0 & 19 \\ 22 & 0 & 11 \\ 10 & 2 & 0 \end{bmatrix} X \begin{bmatrix} 2 & 0 & 19 \\ 22 & 0 & 11 \\ 10 & 2 & 0 \end{bmatrix} = \begin{bmatrix} 194 & 38 & 38 \\ 154 & 22 & 418 \\ 64 & 0 & 212 \end{bmatrix}$$

3. Bilangan-bilangan yang didapatkan dari hasil perkalian matriks diurutkan secara unik. Hal ini untuk lebih mengacaukan kunci. Maka untuk contoh ini diperoleh bilangan-bilangan 0-22-38-64-154-194-212

4. Langkah selanjutnya adalah melakukan operasi modulo 26 terhadap bilangan-bilangan hasil pengurutan pada langkah 3. Untuk contoh ini :

   0-22-38-64-154-194-212
   0-22-12-12- 24 -12 - 4,

   Dimana baris pertama adalah bilangan yang dihasilkan pada langkah 3, dan baris kedua merupakan hasil bilangan tersebut dimodulo 26.

5. Hasil operasi modulo adalah kunci yang sebenarnya. Kunci ini disejajarkan dengan pesan sandi secara berulang. Pada contoh ini :

d	v	w	e	v	b	b	n	r	s	w
0	22	12	12	24	12	4	0	22	12	12

6. Selanjutnya, dicari baris sesuai angka, dan ditelusuri hingga menemukan huruf sesuai pesan sandi. Kolom tempat huruf tersebut berada merupakan huruf pesan asli. Maka akan didapatkan pesan “kriptografi” yang sesuai dengan pesan asli yang dienkripsi.

6. ANALISA

Modifikasi kunci penyandian pada algoritma ALberti Cipher ini memperumit proses penyandian, karena kunci sudah dikacaukan dan tidka akan mudah ditebak oleh kriptanalis.Algoritma ini kuat, bahkan untuk beberapa jenis serangan, seperti :

a. *Chipertext-only attack*, bila hanya dengan cipherteks, kriptanalis tidak akan dapat menebak kunci. Hal ini dikarenakan setiap huruf dapat digantikan oleh beberapa huruf, dan sebaliknya. Juga diperkuat oleh kunci yang sudah dikacaukan, jadi akan lebih sulit untuk mencari kunci yang sebenarnya.
b. *Known-plaintext attack*, kriptanalis tidak akan dapat menebak struktur pada pesan asli, karena sifat polialfabetiknya.
c. *Chosen-plaintext attack*, beberapa pesan asli yang diketahui tidak akan mempermudah kriptanalis untuk menemukan kunci, dengan alas an yang sama seperti yang telah dijelaskan di atas.

Kekurangan pada modifikasi algoritma ini, operasi matematika yang dilakukan kurang kompleks, yaitu hanya perkalian matriks, maka kompleksitasnya hanya n^3. Namun dengan kompleksitas ini sudah cukup untuk memperumit proses enkripsi dan dekripsi, terutama untuk mengaburkan kunci.

7. KESIMPULAN

- Kompleksitas algoritma Alberti Cipher yang telah dimodifikasi ini kurang karena hanya n^3.
- Algoritma ini kuat terhadap serangan *chipertext-only attack, known-plaintext attack, chosen-plaintext attack*, terutama untuk penerkaan dan metode analisis frekuensi.
- Algoritma Alberti Cipher yang telah dimodifikasi lebih baik dari algoritma biasa karena proses penyandiannya menjadi lebih rumit dan mengaburkan kunci sebenarnya yang digunakan.

DAFTAR REFERENSI

[1] Munir, Rinaldi, *Diktat Kuliah IF5054 Kriptografi*, Departemen Teknik Informatika Institut Teknologi Bandung, 2006.

[2] Stallings, William, *Classical Cryptography*, http://williamstallings.com/Extras/Security-Notes/lectures/classical.html

[3] Kallis, Jr., Stephen A., *Codes and Ciphers*, http://www.otr.com/ciphers.html.

[3] *Codes and Ciphers in History*, Part 1 - To 1852 http://www.smithsrisca.demon.co.uk/crypto-ancient.html.

[5] Servos, William, *The Alberti Cipher*, http://starbase.cs.trincoll.edu/~crypto/historical/alberti.html.

[6] Schneier, Bruce, *Applied Cryptography 2nd*, John Wiley & Sons, 1996.

[7] Summers, Wayne, *Cipher Machines From Antiquity to the Enigma Machine*, http://csc.colstate.edu/summers/Research/Cipher-Machines.doc.