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

ANALISIS PERBANDINGAN ALGORITMA KRIPTOGRAFI KLASIK VIGENERE CIPHER DAN ONE TIME PAD

Muhammad Khoiruddin Harahap
Polikteknik Ganesha Medan
Jl.Veteran No. 190 Pasar VI Manunggal
choir.harahap@yahoo.com

***Abstrak*— Kriptografi memiliki peranan yang besar dalam dunia keamanan data. Dengan adanya ilmu yang mempelajari bagaimana menjaga data agar tetap terahasia, diharapkan dapat menciptakan rasa aman bagi siapapun yang ingin menyimpan dan merahasiakan data mereka. Ada beberapa algoritma kriptografi yang tergolong kedalam kriptografi klasik, diantaranya adalah Vigenere Cipher dan One Time Pad. Secara umum proses enkripsi dan dekripsi dari kedua metode ini terlihat sama, namun tetap saja ada perbedaannya. Perbedaan kedua algoritma ini terletak pada kunci yang digunakan, algoritma Vigenere Cipher menggunakan kunci yang sama dan selalu berulang, sedangkan algoritma One Time Pad menggunakan kunci yang selalu berbeda terhadap huruf yang akan dienkripsinya.**

***Keywords*— Kriptografi, Vigenere, One Time Pad.**

I. PENDAHULUAN

A. Latar Belakang

Dalam dunia teknologi informasi, tidak bisa disangkal lagi bahwa data harus diamankan dari pihak-pihak yang tidak berwenang membacanya. Karena adanya pemikiran untuk mengamankan data, maka lahirlah ilmu khusus yang mempelajari tentang kamanan data tersebut. Dalam sejarah terciptanya ilmu ini, ada banyak cara dalam mengamankan data secara tradisional, misalnya saja seperti pesan singkat yang ditulis di kertas panjang yang digulung pada sebuah kayu (scytale), dan apabila gulungan kertas tersebut dibuka, maka pesan akan berbentuk huruf-huruf sandi yang sulit dimengerti.

Pada zaman yang lebih modern, ilmu keamanan data ini sudah dikenal dengan kriptografi. Pada masa data telah diolah dengan komputer (secara komputerisasi), kriptografi juga ikut berkembang. Kriptografi yang sebelumnya hanya diterapkan secara tradisional, kini sudah berkembang dengan melibatkan perhitungan matematika dan teori bilangan dalam pembangkitan kunci, proses enkripsi dan dekripsinya. Walaupun begitu, kriptografi klasik atau yang dikenal dengan kriptografi klasik masih banyak digemari oleh kriptografer karena kesederhanaannya dalam enkripsi dan dekripsi pesan.

Pada penelitian kali ini, penulis ingin meneliti tentang algoritma kriptografi klasik Vigenere Cipher dan algoritma kriptografi klasik One Time Pad.

B. Rumusan Masalah

Berdasarkan latar belakang yang telah dipaparkan sebelumnya, maka yang menjadi rumusan masalah pada penelitian ini adalah bagaimana perbandingan proses penyandian pesan dengan algoritma Vigenere Cipher dan algoritma One Time Pad.

C. Tujuan Penelitian

Tujuan penelitian ini adalah untuk mengetahui lebih detail tentang perbandingan proses enkripsi, dekripsi serta perbandingan keamanan pesan pada algoritma Vigenere Cipher dan algoritma One Time Pad.

D. Manfaat Penelitian

Manfaat penelitian ini adalah untuk menambah pengetahuan tentang kriptografi, khususnya algoritma Vigenere Cipher dan algoritma One Time Pad.

II. TINJAUAN PUSTAKA

A. Sejarah Kriptografi

Sejarah kriptografi ditulis secara lengkap dalam buku David Kahn yang berjudul The Codebreakers pada tahun 1963. David Kahn menceritakan bahwa kriptografi telah digunakan oleh bangsa Mesir sejak 4000 tahun yang lalu, pada masa itu tulisan bangsa Mesir masih berupa hieroglyph yang tidak standard untuk menulis pesan pada piramid. Bangsa Yunani telah menggunakan kriptografi sejak 400 tahun yang lalu sebelum masehi, bangsa Yunani menggunakan alat yang bernama scytale untuk menyampaikan pesan. Scytale adalah kertas panjang yang digulung pada sebuah kayu, pesan ditulis secara horizontal secara baris per baris, apabila kertas dilepaskan, maka pesan akan berubah menjadi huruf-huruf sandi yang sulit untuk diterjemahkan. Dengan cara ini lah bangsa Yunani menyampaikan pesan rahasia kepada pihak-pihak yang bersangkutan.

Gbr.1 Scytale

Setelah abad ke-20 kriptografi bukan lagi hanya sebatas ilmu, kriptografi mulai di teliti dan mulai digunakan untuk keamanan data. Kriptografi sering dipakai pada bidang kemiliteran, contoh dari penerapan yang nyata, kriptografi dipakai dalam Perang Dunia II oleh Pemerintahan Nazi Jerman yang menggunakan mesin Enigma dalam mengubah pesan standart menjadi pesan rahasia.

Gbr.2 Mesin Enigma

B. Pengertian Kriptografi

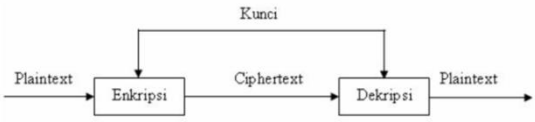
Secara etimologi, kriptografi berasal dari bahasa Yunani yaitu kryptos yang bermakna tersembunyi dan graphein yang bermakna tulisan [2]. Kriptografi adalah ilmu menulis pesan rahasia dengan tujuan menyembunyikan makna pesan tersebut.

C. Istilah-istilah Dalam Kriptografi

Berikut ini adalah lima istilah kriptografi secara umum yaitu [7] :

1. Plaintext
   Pesan asli sebelum diubah menjadi pesan rahasia.
2. Key
   Kunci rahasia yang akan digunakan untuk mengubah pesan asli menjadi pesan rahasia.
3. Ciphertext
   Pesan rahasia yang sudah berbentuk kode-kode yang sulit untuk diterjemahkan.
4. Enkripsi
   Proses mengubah Plaintext menjadi Ciphertext.
5. Dekripsi
   Proses mengubah Ciphertext menjadi Plaintext.

Skema dari sitem kriptografi dapat dilihat pada gambar dibawah ini :



Gbr.3 Skema Sistem Kriptografi

D. Tujuan Kriptografi

Berikut ini adalah empat tujuan kriptografi yang termasuk ke dalam aspek keamanan informasi, yaitu [1] :

1. Kerahasian Data (*Confidentiality*) :
   Menjaga data agar tetap terahasia dari pihak-pihak yang tidak berwenang yang mungkin mencoba membaca data tersebut.
2. Integritas Data (*Integrity*) :
   Memastikan data yang dikirim masih tetap sama dengan data yang diterima tanpa ada perubahan atau modifikasi terhadap data tersebut.
3. Autentikasi (*Authentication*) :
   Memastikan bahwa pengirim dan penerima benar-benar terjamin keasliannya. Dua pihak yang berkomunikasi harus saling mengetahui satu dengan lainnya.
4. Non-Repudiasi (Non-Repudiation) :
   Pengirim tidak bisa menyangkal kalau dia telah mengirim data, karena pengirim akan mendapatkan bukti kalau dia telah mengirim data kepada si penerima.

E. Jenis Kriptografi Berdasarkan Perkembangan

Berdasarkan perkembangan dari tahun ke tahun sejak pertama kali kriptografi ditemukan, ada dua jenis algoritma kriptografi, yaitu :

1. Kriptografi Klasik
   Algoritma kriptografi yang termasuk ke dalam jenis kriptografi klasik ini digunakan pada masa sebelum berlakunya komputarisasi dengan komputer, algoritma kriptografi ini rata-rata masih menggunakan kunci simetris dan menyandikan pesan dengan teknik subtitusi atau transposisi.
2. Kriptografi Modern
   Algoritma kriptografi yang termasuk ke dalam jenis kriptografi modern ini memiliki tingkat kesulitan yang lebih tinggi dan kompleks serta menggunakan pengetahuan matematika dalam penerapan kuncinya. Pada kriptografi modern, kunci yang digunakan untuk menyandikan pesan sudah berupa kunci asimetris.

F. Vigenere Cipher

Algoritma Vigenere Cipher adalah bagian dari kriptografi polialfabetik yang ditemukan pertama kali pada tahun 1586 oleh diplomat Perancis yang bernama Blaise de Vigenere (1523-1596).

Viginere cipher menggunakan tabel vigenere standart dalam mengenkripsi pesan. Tabel yang digunakan merupakan tabel 26 huruf alfabetik standart, yang dimulai dari A sampai Z. Kunci pada Vigenere Cipher dipakai berulang kali sebanyak pesan yang akan dienkripsi. Semakin beragam huruf alfabetik

yang dipakai sebagai kunci, maka semakin kuat juga keamanan algoritma Vigenere Cipher ini. Berikut ini rumus enkripsi dan dekripsi Vigenere Cipher :

Enkripsi : Ci = Pi + ki mod 26
Dekripsi : Pi = Ci - ki mod 26

G. One Time Pad

Algoritma One Pad termasuk salah satu algoritma yang memiliki kesempurnaan saat enkripsi dan dekripsnyai. One Time Pad yang dikenal dengan algoritma Vernam, ditemukan oleh Gillbert Vernam di Major Joseph Mauborge and AT & T's. Konsep dasar algoritma One Time Pad hampir sama dengan algoritma Vigenere, hanya saja pada algoritma ini, kunci dibangkitkan secara acak, dan kecil kemungkinan kunci akan saling sama satu dengan lainnya. Berikut ini rumus enkripsi dan dekripsi Vigenere Cipher :

Enkripsi : Ci = Pi + ki mod 26
Dekripsi : Pi = Ci - ki mod 26

III. PEMBAHASAN

Pada bagian ini, penulis ingin memberikan gambaran tentang cara kerja algoritma Vigenere Cipher dalam menyandikan pesan asli menjadi pesan rahasia (enkripsi) maupun membalikkan pesan rahasia ke dalam bentuk pesan biasa (dekripsi).

A. Vigenere Cipher

Terdapat sebuah plainteks yang akan diubah menjadi ciphertext, yaitu : BESOK SORE KITA PERGI, yang akan diproses dengan kunci VIGENERE.

Kita perlu menyapakati acuan huruf yang akan kita gunakan dalam proses enkripsi pesan, berikut ini tabel alfabeik 26 huruf :

TABEL II
ALFABETIK 26 HURUF

0	1	2	3	4	5	6	7	8
A	B	C	D	E	F	G	H	I
9	10	11	12	13	14	15	16	17
J	K	L	M	N	O	P	Q	R
18	19	20	21	22	23	24	25	
S	T	U	V	W	X	Y	Z	

Dari tabel alfabetik 26 huruf diatas, maka selanjutnya *plaintext* dan kunci akan diubah ke dalam bentuk angka untuk enkripsi dan dekripsi, berikut ini proses enkripsi dan dekripsi pesan :

1) *Enkripsi :*

Ci = Pi + ki mod 26
C1 = B = 1 + 21 mod 26 = 22 = W
C2 = E = 4 + 8 mod 26 = 12 = M
C3 = S = 18 + 6 mod 26 = 24 = Y
C4 = O = 14 + 4 mod 26 = 18 = S
C5 = K = 10 + 13 mod 26 = 23 = X
C6 = S = 18 + 4 mod 26 = 22 = W
C7 = O = 14 + 17 mod 26 = 5 = F
C8 = R = 17 + 4 mod 26 = 21 = V
C9 = E = 4 + 21 mod 26 = 25 = Z
C10 = K = 10 + 8 mod 26 = 18 = S
C11 = I = 8 + 6 mod 26 = 14 = O
C12 = T = 19 + 4 mod 26 = 23 = X
C13 = A = 0 + 13 mod 26 = 13 = N
C14 = P = 15 + 4 mod 26 = 19 = T
C15 = E = 4 + 17 mod 26 = 21 = V
C16 = R = 17 + 4 mod 26 = 21 = V
C17 = G = 6 + 21 mod 26 = 1 = B
C18 = I = 8 + 8 mod 26 = 16 = Q

Dari hasil enkripsi, diperolehlah pesan terahasia ciphertext WMYSX WFVZ SOXN TVVBQ

2) *Dekripsi :*

Pi = Ci - ki mod 26
P1 = W = 22 - 21 mod 26 = 1 = B
P2 = M = 12 - 8 mod 26 = 4 = E
P3 = Y = 24 - 6 mod 26 = 18 = S
P4 = S = 18 - 4 mod 26 = 14 = O
P5 = X = 23 - 13 mod 26 = 10 = K
P6 = W = 22 - 4 mod 26 = 18 = S
P7 = F = 5 - 17 mod 26 = 14 = O
P8 = V = 21 - 4 mod 26 = 17 = R
P9 = Z = 25 - 21 mod 26 = 4 = E
P10 = S = 18 - 8 mod 26 = 10 = K
P11 = O = 14 - 6 mod 26 = 8 = I
P12 = X = 23 - 4 mod 26 = 19 = T
P13 = N = 13 - 13 mod 26 = 0 = A
P14 = T = 19 - 4 mod 26 = 15 = P
P15 = V = 21 - 17 mod 26 = 4 = E
P16 = V = 21 - 4 mod 26 = 17 = R
P17 = B = 1 - 21 mod 26 = 6 = G
P18 = Q = 16 - 8 mod 26 = 8 = I

Dari hasil dekripsi, diperolehlah pesan asli plaintext kembali BESOK SORE KITA PERGI.

B. One Time Pad

Penulis melalukan pengujian dengan pesan yang sama seperti yang dilakukan dengan algoritma Vigenere Cipher, yaitu : BESOK SORE KITA PERGI, dengan kunci ZXCOF GSRL PHNM URFDS. Berikut ini proses enkripsi dan dekripsi pesan :

1) *Enkripsi :*

Ci = Pi + ki mod 26
C1 = B = 1 + 25 mod 26 = 0 = A
C2 = E = 4 + 23 mod 26 = 1 = B
C3 = S = 18 + 2 mod 26 = 20 = U
C4 = O = 14 + 14 mod 26 = 2 = C
C5 = K = 10 + 5 mod 26 = 15 = P
C6 = S = 18 + 6 mod 26 = 24 = Y
C7 = O = 14 + 18 mod 26 = 6 = G
C8 = R = 17 + 17 mod 26 = 8 = I
C9 = E = 4 + 11 mod 26 = 15 = P
C10 = K = 10 + 15 mod 26 = 25 = Z
C11 = I = 8 + 7 mod 26 = 15 = P
C12 = T = 19 + 13 mod 26 = 6 = G

C13 = A = 0 + 12 mod 26 = 12 = M
C14 = P = 15 + 20 mod 26 = 9 = J
C15 = E = 4 + 17 mod 26 = 21= V
C16 = R = 17 + 5 mod 26 = 22 = W
C17 = G = 6 + 3 mod 26 = 9 = J
C18 = I = 8 + 18 mod 26 = 0 = A

Dari hasil enkripsi, diperolehlah pesan terahasia ciphertext ABUCP YGIP ZPGM JVWJA.

2) *Dekripsi :*

Pi = Ci - ki mod 26
P1 = A = 0 - 25 mod 26 = 1 = B
P2 = B = 1 - 23 mod 26 = 4 = E
P3 = U = 20 - 2 mod 26 = 18 = S
P4 = C = 2 - 14 mod 26 = 14 = O
P5 = P = 15 - 5 mod 26 = 10 = K
P6 = Y = 24 - 6 mod 26 = 18 = S
P7 = G = 6 - 18 mod 26 = 14 = O
P8 = I = 8 - 17 mod 26 = 17 = R
P9 = P = 15 - 11 mod 26 = 4 = E
P10 = Z = 25 - 15 mod 26 = 10 = K
P11 = P = 15 - 7 mod 26 = 8 = I
P12 = G = 6 - 13 mod 26 = 19 = T
P13 = M = 12 - 12 mod 26 = 0 = A
P14 = J = 9 - 20 mod 26 = 15 = P
P15 = V = 21 - 17 mod 26 = 4 = E
P16 = W = 22 - 5 mod 26 = 17 = R
P17 = J = 9 - 3 mod 26 = 6 = G
P18 = A = 0 - 18 mod 26 = 8 = I

Dari hasil dekripsi, diperolehlah pesan asli plaintext kembali BESOK SORE KITA PERGI.

IV. KESIMPULAN

Berikut ini adalah kesimpulan terhadap pembahasan algoritma Vigenere Cipher dan algoritma One Time Pad :

1. Algoritma Vigenere Cipher dan algoritma One Time Pad memiliki rumus yang sama dalam enkripsi dan dekripsi. Perbedaan kedua algoritma ini terletak pada deretan kunci yang digunakan.
2. Algoritma Vigenere Cipher menggunakan kunci yang selalu berulang sepanjang pesan yang akan dienkripsi, sedangkan algoritma One Time Pad menggunakan kunci yang benar-benar acak dan tidak memiliki pola tertentu, dimana ukuran panjang kuncinya juga sepanjang pesan yang akan dienkripsi.
3. Dari segi keamanan, algoritma One Time Pad lebih sulit untuk ditembus oleh para kriptanalis. Kunci acak yang digunakan oleh algoritma One Time Pad membuat algoritma ini memiliki tingkat keamanan yang sempurna.

REFERENSI

[1] Abhirama, Dwitiyo. 2013. *Keystream Vigenere Cipher :Modifikasi Vigenere Cipher dengan Pendekatan Keystream Generator*. ITB, Bandung.

[2] Atika Sari, Christy., Hari Rachmawanto, Eko. 2014. *Gabungan Algoritma Vernam Cipher dan End Of File untuk Keamanan Data*. Jurnal. Techno.Com, Vol.13, No.3, Agustus 2014 : 150-157.

[3] Dooley, John F. 2013. *A Brief History of Cryptology and Cryptographic Algorithms*. Springer.

[4] Menezes, Alfred., Van Oorschot, Paul., Vanstone, Scott.1996. *Handbook of Applied Cryptography*. Champan & Hall/ CRC.

[5] Mollin, Richard A. 2007. *An Introduction to Cryptography 2nd Ed*. Champan & Hall/ CRC.

[6] Neuenschwander, Daniel. 2004. *Probabilistic and Statistical Method in Cryptology*. Springer.

[7] Paar, Christof., Pelzi, Jan., dan Preneel, Bart.2010. *Understanding Cryptography*. Springer.

[8] Sadikin, Rifki. 2012. *Kriptografi untuk Keamanan Jaringan dan Implementasinya dalam Bahasa Java*. Penerbit Andi, Yogyakarta.

[9] Sholeh, M., Hamokwarong, J.V. 2011. *Aplikas Kriptografi dengan Metode Vernam Cipher dan Metode Permutasi Biner*. Jurnal. Momentum, Vol.7, No.2, Oktober 2011 : 8-13.

[10] Stinson, D. R. 2002. *Cryptography : Theory and Practice*. Champan & Hall/ CRC.

[11] Wirdasari, Dian. 2008. *Prinsip Kerja Kriptografi dala Mengamankan Informasi*, Jurnal SAINTIKOM Vol.5 No.2.