Analisis Algoritma *One Time Pad* Dengan Algoritma *Cipher* Transposisi Sebagai Pengamanan Pesan Teks

Muhammad Khoiruddin Harahap

Politeknik Ganesha Medan
Jl. Veteran No. 194 Pasar VI Manunggal
choir.harahap@yahoo.com

Nurul Khairina

Politeknik Ganesha Medan
Jl. Veteran No. 194 Pasar VI Manunggal
nurulkhairina27@gmail.com

Abstrak — Konsep Algoritma penting dalam menyelesaikan masalah secara efektif dan efisien, terutama bergelut di dunia *computer programming* untuk menyusun program dan menyelesaikan suatu persoalan. Banyak jenis algoritma kriptografi yang dihasilkan oleh para ilmuwan, namun cara pengimplementasiannya beragam pula (berbeda – beda). Algoritma *One Time Pad* merupakan algoritma yang dipopulerkan oleh Major Josep Mouborgne pada tahun 1917. Algoritma ini merupakan salah satu algoritma kriptografi simetris dengan proses kunci enkripsi sama dengan kunci dekripsi. Algoritma ini menggunakan table ASCII (*American Standart Code for Information Interchange*). Algoritma *Cipher* Transposisi merupakan salah satu algoritma yang menggunakan teknik permutasi atau transposisi untuk mengubah *plaintext* menjadi *ciphertext*. Algoritma *One Time Pad* memiliki kriteria panjang teks harus sama dengan panjang *key*, jika tidak sama, maka karakter pesan pada *key* akan melakukan iterasi sehingga panjang pesan sama dengan panjang *key*. Algoritma *One Time Pad* sangat aman dipakai dalam penyandian, karena memiliki *key* yang berbeda di setiap penyandiannya terhadap pesan asli, namun algoritma ini memiliki kelemahan pada dekripsinya yang terkadang *ciphertext* tidak dapat kembali secara utuh. Algoritma *Cipher* Transposisi membagi pesan ke dalam blok yang panjangnya sesuai dengan panjang *key*, apabila panjang pesan lebih pendek panjang blok, maka setiap blok yang bersisa akan diisi oleh *dummy*. Algoritma ini menerapkan pembacaan pesan secara horizontal pada proses enkripsi dan pembacaan secara vertikal pada dekripsi.

Kata Kunci — kriptografi, *one time pad*, *cipher* transposisi

I. PENDAHULUAN

Kriptografi adalah ilmu yang mempelajari bagaimana menjaga keamanan suatu pesan (*plaintext*). Tugas utama kriptografi adalah untuk menjaga agar pesan atau kunci ataupun keduanya tetap terjaga kerahasiaannya dari penyadap (*attacker*). Penyadap pesan diasumsikan mempunyai akses yang lengkap dalam saluran komunikasi antara pengirim pesan dan penerima pesan. Penyadapan pesan sering terjadi pada komunikasi melalui internet maupun saluran telepon. Pesan-pesan yang dirahasiakan dalam kriptografi biasa disebut *plaintext* dan hasil penyamaran disebut *ciphertext*. Proses penyamaran dari *plaintext* ke *ciphertext* disebut enkripsi dan proses pembalikan dari *ciphertext* menjadi *plaintext* kembali disebut dekripsi[1]

Gambar 1. Skema Enkripsi dan intruder
Sumber : <http://userpages.umbc.edu>

Algoritma *One Time Pad* ditemukan pada tahun 1917 oleh Major Joseph Mauborgne. Algoritma ini termasuk ke dalam kelompok algoritma kriptografi simetri. *One Time Pad* (pad = kertas blok not) berisi barisan karakter - karakter kunci yang dibangkitkan secara acak.

Algoritma *Cipher* Transposisi merupakan salah satu dari jenis algoritma *Cipher* yang memanfaatkan teknik permutasi, algoritma ini melakukan pertukaran posisi karakter (*transpose*). Kedua algoritma ini memiliki pengimplementasian yang berbeda sehingga memiliki perbandingan yang berbeda pula, disini penulis akan mencoba membandingkan kecepatan proses enkripsi dan dekripsi masing-masing algoritma.

II. TINJAUAN PUSTAKA

A. Konsep Algoritma

Konsep algoritma sangat penting dalam menyelesaikan permasalahan. Algoritma merupakan langkah – langkah menyelesaikan suatu masalah yang efektif dan efisien yang merupakan data *input* dan data *output* sehingga mendapatkan suatu informasi yang real.

Algoritma berasal dari kata Al-Khawarizm yaitu nama seorang tokoh ilmuwan Arab. Sehingga kata tersebut diubah orang barat dengan kata "Algorism". Yang dulunya kata algoritma banyak dikenal sebagai proses perhitungan dengan angka Arab.

Gambar 2. Muhammad ibnu Musa Al-khawarizm
sumber : todayifoundout.com

B. Kriteria Algoritma

Donald E. Knuth mengemukakan, Algoritma yang baik memiliki Kriteria sebagai berikut:

1. Input

Dari sisi *Input*, minimal program harus memiliki nol atau lebih pengguna. Program pasti memiliki *input*, Yang dimaksud memiliki nol *input* berarti program tidak mendapatkan masukan data dari pengguna secara langsung, namun semua data yang akan digunakan oleh program sudah di deklarasikan di dalam kode program yang akan dieksekusi.

2. Output

Dari sisi *output*, minimal program harus memiliki 1 *output*. Program pasti menghasilkan output karena program dibuat untuk tujuan tertentu.

3. Finite (terbatas)

Program harus pasti dan berhenti, bukan tak terhingga, suatu program yang dieksekusi haruslah berhenti dan selesai, bukan berjalan terus menerus hingga *hang up* atau *not responding*, dan akhirnya harus di *kill* (dimatikan) dengan paksa.

4. Definite (pasti)

Program harus jelas arah dan tujuannya. Suatu program harus jelas kapan mulai dan kapan berakhir, apa tujuannya, dan memiliki logika yang jelas agar dapat menghasilkan output yang sesuai dengan yang diharapkan.

5. Efisien

Artinya, Program harus efisien, tidak memakan banyak *memory*, tidak melakukan hal – hal yang tidak perlu.

C. Kriptografi

Rinaldi Munir dalam bukunya Pengantar Kriptografi menjelaskan bahwa "Kriptografi (*cryptography*) berasal dari Bahasa Yunani yaitu "*cryptós*" artinya "*secret*" (rahasia), sedangkan "*gráphein*" artinya "*writing*" (tulisan). Jadi, kriptografi berarti "*secret writing*" (tulisan rahasia). Ada beberapa definisi kriptografi yang telah dikemukakan di dalam berbagai literatur. Definisi yang dipakai di dalam buku-buku yang lama (sebelum tahun 1980-an) menyatakan bahwa kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi maknanya. Definisi ini mungkin cocok pada masa lalu di mana kriptografi digunakan untuk keamanan komunikasi penting seperti komunikasi di kalangan militer, diplomat, dan mata-mata. Namun saat ini kriptografi lebih dari sekedar *privacy*, tetapi juga untuk tujuan data integrity, *authentication*, dan *non-repudiation*".

Di dalam kriptografi kita akan sering menemukan berbagai istilah atau terminologi. Beberapa istilah yang penting untuk diketahui yaitu :

1. Plainteks (*plaintext*), adalah data atau informasi yang dapat dibaca dan dimengerti maknanya. Pesan yang tersandi tidak hanya berupa teks, tetapi juga dapat berbentuk citra (*image*), suara/bunyi (*audio*), dan video, atau berkas biner lainnya.
2. Cipherteks (*ciphertext*), adalah bentuk pesan yang tersandi atau hasil dari penyamaran plaintexts.
3. Enkripsi, adalah proses menyandikan *plaintext* menjadi *ciphertext*.
4. Dekripsi, adalah proses mengembalikan *ciphertext* menjadi *plaintext* semula.
5. Kriptosistem, adalah kumpulan yang terdiri dari algoritma kriptografi, semua *plaintext* dan *ciphertext* yang mungkin, dan kunci.
6. Kriptanalisis, adalah ilmu dan seni untuk memecahkan *ciphertext* menjadi *plaintext* tanpa mengetahui kunci yang digunakan. Pelakunya disebut kriptanalisis.
7. Kriptologi, adalah studi mengenai kriptografi dan kriptanalisis.

D. Tujuan Kriptografi

Berikut merupakan tujuan dari Kriptografi yaitu :

1. **Kerahasiaan** (*confidentiality*), adalah layanan yang ditujukan untuk menjaga agar pesan tidak dapat dibaca oleh pihak-pihak yang tidak berhak.

2. **Integritas data** (*data integrity*), adalah layanan yang menjamin bahwa pesan masih asli dan utuh atau belum pernah dimanipulasi selama pengiriman.
3. **Otentikasi** (*authentication*), adalah layanan yang berhubungan dengan identifikasi, baik mengidentifikasi kebenaran pihak - pihak yang berkomunikasi (*user authentication* atau *entity authentication*) maupun mengidentifikasi kebenaran sumber pesan (*data origin authentication*).
4. **Nir penyangkalan** (*non-repudiation*), adalah layanan untuk mencegah entitas yang berkomunikasi melakukan penyangkalan, yaitu pengirim pesan menyangkal melakukan pengiriman atau penerima pesan menyangkal telah menerima pesan.

E. Algoritma One Time Pad

Algoritma *One Time Pad* (OTP) adalah *stream cipher* yang melakukan enkripsi dan dekripsi satu karakter setiap kali. Algoritma ini merupakan perbaikan dari Vernam *cipher* untuk menghasilkan keamanan yang sempurna. *Cipher* ini termasuk ke dalam kelompok algoritma kriptografi simetri. *One Time Pad* (pad = kertas bloknot) berisi barisan karakter-karakter kunci yang dibangkitkan secara acak. Aslinya, satu buah *One Time Pad* adalah sebuah pita (tape) yang berisi barisan karakter-karakter kunci. Satu pad hanya digunakan sekali (*one time*) saja untuk mengenkripsi pesan, setelah itu pad yang telah digunakan dihancurkan supaya tidak dipakai kembali untuk mengenkripsi pesan yang lain.

Penggunaan *One Time Pad* berikut yang digunakan penulis menggunakan tabel ASCII, berikut merupakan table ASCII.

Tabel 1 *One Time Pad* Sesuai Tabel ASCII

KARAKTER	ASCII CODE
A	65
B	66
C	67
D	68
E	69
F	70
G	71
H	72
I	73
J	74

K	75
L	76
M	77
N	78
O	79
P	80
Q	81
R	82
S	83
T	84
U	85
V	86
W	87
X	88
Y	89
Z	90

Rumus dari enkripsi *One Time Pad* yaitu :

$$C_i = (P_i + K_i - 2 \times 64) \bmod 26 + 64$$

dan rumus dekripsi dari *One Time Pad* yaitu :

$$P_i = (C_i - K_i + 26) \bmod 26 + 64$$

Keterangan rumus :

C_i = Cipherteks (*Ciphertext*),

P_i = Plainteks (*Plaintext*),

K_i = kunci (*Key*).

F. Algoritma Cipher Transposisi

Algoritma *Cipher Transposisi* ini merubah *plaintext* menjadi *ciphertext* dengan teknik permutasi atau yang dikenal dengan transposisi (*transpose*).

Pada proses enkripsi, algoritma ini membagi masing-masing karakter *plaintext* menjadi beberapa blok/ kolom, dimana *ciphertext* yang merupakan hasil enkripsi akan dibaca secara vertikal (dari atas ke bawah), sedangkan pada proses dekripsi, *plaintext* akan dibaca secara horizontal (dari kiri ke kanan).

Pada algoritma ini, terdapat sebuah kunci (*key*) yang mengatur berapa banyak pembagian blok/ kolom yang akan dibuat. Dan apabila terdapat blok kosong yang disebabkan oleh jumlah karakter *plaintext* yang lebih sedikit dari jumlah blok, maka blok/ kolom yang kosong tersebut dapat diisi oleh *dummy* [7].

III. PEMBAHASAN

A. *Algoritma One Time Pad*

Berikut ini proses enkripsi algoritma *One Time Pad*, dimana terdapat sebuah *plaintext* "KAMPUS" dengan *key* = "POLGAN".

Plaintext = "KAMPUS"

Key = "POLGAN"

Langkah selanjutnya yaitu *plaintext* dan kunci diubah menjadi angka sesuai dengan tabel yang telah diberikan, berikut ini proses enkripsinya :

$$\begin{aligned} C_1 &= (P_1 + K_1 - 2 \times 64) \bmod 26 + 64 \\ &= (75 + 80 - 2 \times 64) \bmod 26 + 64 \\ &= (155 - 128) \bmod 26 + 64 \\ &= (27) \bmod 26 + 64 \\ &= 1 + 64 \\ C_1 &= 65 \end{aligned}$$

Maka $C_1=65$ huruf *ciphertext* dengan nilai 65 adalah A.

Dengan melakukan konsep yang sama maka didapatkan hasil sebagai berikut :

Plaintext = "POLGAN" *Key*
= "KAMPUS" *Ciphertext*
= "APYWVG"

Proses dekripsi dapat dilihat pada perhitungan dibawah ini :

Ciphertext = "A"
Key = "P"

Dekripsi :

$$\begin{aligned} P_1 &= (C_1 - K_1 + 26) \bmod 26 + 64 \\ &= (A - K + 26) \bmod 26 + 64 \\ &= (65 - 80 + 26) \bmod 26 + 64 \\ &= 11 \bmod 26 + 64 \\ &= 75 \end{aligned}$$

huruf *ciphertext* dengan nilai 75 adalah K.

B. *Algoritma Cipher Transposisi*

Berikut ini proses enkripsi algoritma *Cipher Transposisi*, dimana terdapat sebuah kalimat "POLITEKNIK GANESHA MEDAN" dengan *key* = 5.

Plaintext = "POLITEKNIK GANESHA MEDAN"
Key = 5

Langkah melakukan enkripsi adalah dengan menuliskan *plaintext* satu per satu sebanyak 5 karakter secara horizontal (dari kiri ke kanan) sesuai dengan *key* yang telah diberikan sebelumnya, sehingga susunan *plaintext* menjadi :

Tabel 2 Proses Enkripsi *Cipher* Transposisi Tahap 1

P	O	L	I	T
E	K	N	I	K
G	A	N	E	S
H	A	M	E	D
A	N			

Dari tabel diatas dapat terlihat ada 3 blok/ kolom yang kosong karena jumlah karakter *plaintext* yang akan dituliskan di blok/kolom sudah habis, dalam artian, jumlah karakter *plaintext* lebih sedikit dari jumlah blok/ kolom yang tersedia, maka 3 blok/kolom tersebut diisi oleh *dummy* (misalnya X), sehingga proses enkripsi menjadi :

Tabel 3 Proses Enkripsi *Cipher* Transposisi Tahap 2

P	O	L	I	T
E	K	N	I	K
G	A	N	E	S
H	A	M	E	D
A	N	X	X	X

Setelah melalui tahap pembagian karakter *plaintext* ke dalam blok/ kolom, maka *ciphertext* dapat dengan segera diperoleh dari pembacaan karakter secara vertikal (dari atas ke bawah), sehingga diperoleh hasil *ciphertext* sebagai berikut :

Ciphertext = "PEGHAOKAANLNNMXIIEXTKSDX"

Pada proses dekripsi, kita membagi karakter *ciphertext* secara vertikal (dari atas ke bawah) sebanyak kunci yang telah ditentukan sebelumnya. Dapat dihitung bahwa jumlah karakter *ciphertext* yang diperoleh adalah 25 huruf, dan kunci = 5, maka karakter *ciphertext*

dituliskan dan dibagi ke dalam 5 blok secara vertikal (dari atas ke bawah).

$Ciphertext = \text{"PEGHAOKAANLNNMXIIEEXTKSDX"}$
 $Key = 5$

Tabel 4 Proses Dekripsi Cipher Transposisi Tahap 1

P	O	L	I	T
E	K	N	I	K
G	A	N	E	S
H	A	M	E	D
A	N	X	X	X

Setelah selesai proses dekripsi tahap 1, maka *plaintext* sudah dapat diperoleh kembali dengan membaca tabel secara horizontal (dari kiri ke kanan) seperti pada tabel dibawah ini :

Tabel 5 Proses Dekripsi Cipher Transposisi Tahap 2

P	O	L	I	T
E	K	N	I	K
G	A	N	E	S
H	A	M	E	D
A	N	X	X	X

Dari tabel diatas, dapat diperoleh *plaintext* sebagai berikut :

$Plaintext = \text{"POLITEKNIK GANESHA MEDANXXX"}$

Langkah terakhir adalah menghilangkan *dummy* (huruf X) sebanyak jumlah *dummy* yang ditambahkan saat melakukan proses enkripsi sebelumnya. Sehingga diperoleh *plaintext* sebagai berikut :

$Plaintext = \text{"POLITEKNIK GANESHA MEDAN"}$

IV. KESIMPULAN

Sesuai dengan hasil penelitian dan pembahasan yang telah dilakukan di atas, dapat diambil kesimpulan bahwa :

1. Algoritma *One Time Pad* memiliki sifat bahwa panjang *plaintext* (pesan) harus sama panjang dengan kunci, meneliti dengan table ASCII dan panjang *key* tidak harus sama dengan panjang *plaintext*. Akan tetapi, kunci yang tidak sama harus mengulang kata sehingga panjang *key* sama dengan panjang pesan.
2. Algoritma *One Time Pad* memiliki hasil pendekripsian yang pecah atau melebur jika pesan terlalu panjang.
3. Algoritma *Cipher Transposisi* memiliki hasil yang baik dalam pendekripsian atau *plaintext* (pesan) yang dimasukkan memiliki hasil pendekripsian yang sama walaupun pesan tersebut sangat panjang.
4. Jika dilihat dari cara pengimplementasiannya bahwa kedua Algoritma ini baik digunakan, akan tetapi *One Time Pad* memiliki kelemahan pada pendekripsian, sedangkan *Cipher Transposisi* mampu melakukan pendekripsian dengan utuh.

REFERENSI

- [1] Mulyono, Hengky. 2013. "Implementasi Algoritma *One Time Pad* pada Penyimpanan Data Berbasis Web". Gunadarma,.
- [2] Endah Pratiwi Lis. 2014. "Program Aplikasi Kriptografi Penyandian *One Time Pad* Menggunakan Sandi Vinegere", Universitas Pendidikan Indonesia.
- [3] Sugianto, Teguh Winarto. 2014. "Kriptografi Gabungan menggunakan Algoritma Mono Alphabetic dan *One Time Pad*", STMIK Pontianak.
- [4] Tomoyud S Waruwu, Kristina Telaumbanua. 2016. "Kombinasi Algoritma OTP dan Algoritma BBS dalam Pengamanan File", Mikroskill. Medan.
- [5] Erna Kumalasari Nurnawati. 2008. "Analisis Kriptografi menggunakan Algoritma Vigenere Cipher dengan Mode Operasi Cipher Block Chaining (CBC)", IST Akprind.
- [6] Putuh H. Arjana, Tri Puji Rahayu, Yakub, Hariyanto. 2012. "Implementasi Enkripsi Data dengan Algoritma Vigenere Cipher". STMIK Darma Putra Tangerang.
- [7] Pardede AMH, Maulita Y. PERANCANGAN PERANGKAT LUNAK ENKRIPSI DAN DESKRIPSI FILE DENGAN METODE TRANSPOSISI KOLOM. J KAPUTAMA. 2014;8(1):28-35.