SinkrOn
JURNAL & PENELITIAN TEKNIK INFORMATIKA
Publikasi Jurnal & Penelitian Teknik Informatika
Volume 2 Nomor 2, April 2018
e-ISSN : 2541-2019
p-ISSN : 2541-044X

Analisa Perbandingan Algoritma *Monoalphabetic Cipher* Dengan Algoritma *One Time Pad* Sebagai Pengamanan Pesan Teks

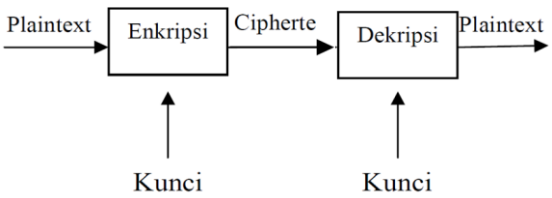
Romindo
Politeknik Ganesha Medan
Jl. Veteran No. 194 Pasar VI Manunggal
romindo4@gmail.com

Abstract — Dalam hal komunikasi data sangatlah diperlukan kerahasiaan data. Untuk menjamin keamanan dan kerahasiaan data, maka diperlukan teknik tertentu dalam penyandian data atau informasi yang disebut kriptografi. Ada berbagai jenis algoritma kriptografi seperti *playfair cipher, blowfish, monoalphabetic cipher, vigenere cipher, des, idea, On Time Pad* (*OTP*) dan sebagainya yang berusaha untuk menciptakan suatu algoritma yang benar-benar dapat mengamankan data. Salah satunya *monoalphabetic cipher* atau disebut juga cipher substitusi sederhana (*simple subsitution cipher*), karena memilki sifat yaitu satu huruf di *plaintext* diganti dengan tepat satu huruf *ciphertext*. Jadi, fungsi *ciphering*-nya adalah satu ke satu, sementara algoritma *One Time Pad* memiliki sifat bahwa panjang plainteks (pesan) harus sama panjang dengan kunci. Algoritma *monoalphabetic chiper* memiliki kelemahan pada *ciphertext*-nya, yaitu beberapa huruf masih sama dengan *plaintext*, sedangkan algoritma *One Time Pad* berbeda dengan *monoalphabetic chiper*.

Kata Kunci − kriptografi, *monoalphabetic cipher, one time pad*

I. PENDAHULUAN

Kriptografi merupakan salah satu ilmu pengetahuan sekaligus seni untuk menjaga kerahasiaan pesan dengan cara merahasiakannya ke dalam bentuk sandi yang tidak mempunyai makna. Pesan yang dirahasiakan dalam kriptografi disebut (*plaintext*) dan hasil penyamaran disebut (*chipertext*). Proses penyamaran dari *plaintext* ke *chipertext* disebut enkripsi (dari kata *encryption*) dan proses pembalikan dari *chipertext* menjadi *plaintext* kembali disebut dekripsi (*decryption*). Baik proses enkripsi maupun proses dekripsi melibatkan satu atau beberapa kunci kriptografi. Dalam suatu system di mana terdapat algoritma kriptografi, ditambah seluruh kemungkinan *plaintext*, *ciphertext* dan kunci-kuncinya disebut kriptosistem. Proses tersebut dapat digambarkan secara sederhana sebagai berikut :



Gambar 1.Enkripsi/Dekripsi

Ada beberapa algoritma dalam penyandian kriptografi yang dapat digunakan untuk mengenkripsi data teks, diantaranya: *Playfair Cipher, Blowfish, Monoalphabetic Cipher, Vigenere Cipher, DES, Idea,*

On Time Pad (OTP) dan sebagainya dengan kelebihan yang berbeda-beda. Dalam hal ini peneliti mengambil algoritma *Monoalphabetic Cipher* dan algoritma *One Time Pad.*

Pada *Monoalphabetic Cipher* atau disebut juga *cipher* substitusi sederhana (*simple subsitution cipher*), satu huruf di *plaintext* diganti dengan tepat satu huruf *ciphertext*. Jadi, fungsi *ciphering*-nya adalah satu ke satu.

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. Implementasi kedua algoritma ini berbeda, maka peneliti mencoba membandingkan algoritma mana yang lebih baik dalam merahasiakan pesan teks.

II. TINJAUAN PUSTAKA

A. Konsep Algoritma

Algoritma adalah jantung ilmu komputer atau informatika. Banyak cabang ilmu computer yang diacu dalam terminologi algoritma. Namun, jangan beranggapan algoritma selalu identik dengan ilmu komputer saja. Dalam kehidupan sehari-haripun banyak terdapat proses yang dinyatakan dalam suatu algoritma. Cara-cara membuat kue atau masakan yang dinyatakan dalam suatu resep juga dapat disebut sebagai algoritma. Pada setiap resep selalu ada urutan langkah-lankah membuat masakan. Bila langkah-langkahnya tidak logis, tidak dapat dihasilkan masakan yang diinginkan. Ibu-ibu yang mencoba suatu resep masakan akan membaca satu per satu langkah-langkah pembuatannya lalu ia mengerjakan proses sesuai yang ia baca. Secara umum, pihak (benda) yang mengerjakan proses disebut pemroses (*processor*). Pemroses tersebut dapat berupa manusia, komputer, robot atau alat alat elektronik lainnya. Pemroses melakukan suatu proses dengan melaksanakan atau "mengeksekusi" algoritma yang menjabarkan proses tersebut.

Melaksanakan Algoritma berarti mengerjakan langkah-langkah di dalam Algoritma tersebut. Pemroses mengerjakan proses sesuai dengan algoritma yang diberikan kepadanya. Juru masak membuat kue berdasarkan resep yang diberikan kepadanya, pianis memainkan lagu berdasarkan papan not balok. Karena itu suatu Algoritma harus dinyatakan dalam bentuk yang dapat dimengerti oleh pemroses. Jadi suatu pemroses harus :

1. Mengerti setiap langkah dalam Algoritma.
2. Mengerjakan operasi yang bersesuaian dengan langkah tersebut.

B. Konsep Kriptografi

Kriptografi (*cryptography*) berasal dari Bahasa Yunani, yaitu *cryptos* dan *graphia* yang berarti 'penulisan rahasia'. Kriptografi adalah ilmu ataupun seni yang mempelajari bagaimana membuat suatu pesan yang dikirim oleh pengirim dapat disampaikan kepada penerima dengan aman. Kriptografi merupakan bagian dari suatu cabang ilmu matematika yang disebut kriptologi (*cryptology*). Kriptografi bertujuan menjaga kerahasian informasi yang terkandung dalam data sehingga informasi tersebut tidak dapat diketahui oleh pihak yang tidak sah. Perancang algoritma kriptografi disebut kriptografer.

C. Tujuan Kriptografi

Kriptografi sesungguhnya merupakan studi tehadap teknik matematis yang terkait dengan aspek keamanan suatu sistem informasi seperti kerahasiaan, integritas data, autentikasi, dan ketiadaaan penyangkalan. Keempat aspek tersebut merupakan tujuan fundamental dari suatu sistem kriptografi).

1. Kerahasian (*confidentiality*)
   Kerahasiaan adalah layanan yang digunakan untuk menjaga informasi dari setiap pihak yang tidak berwenang untuk mengaksesnya. Informasi ini tentunya hanya dapat diakses oleh pihak-pihak yang berhak. Contohnya serangannya adala *sniffing*. Proteksi dilakukan dengan metode enkripsi.
2. Integritas data (*data integrity*)
   Integritas data adalah layanan yang bertujuan untuk menjaga terjadinya pengubahan informasi oleh pihak-pihak yang tidak berwenang. Integritas data harus dipastikan agar sistem informasi mampu mendeteksi terjadinya manipulasi data. Manipulasi data yang dimaksud di sini meliputi penyisipan, penghapusan, ataupun penggantian data. Contoh serangannya adalah *spoofing*, virus, *torjan horse* dan lainnya. Proteksi dilakukan dengan *signature*, *certificate*, dan *hash*.

3. Autentikasi (*authentication*)
   Autentikasi adalah layanan yang terkait dengan identifikasi terhadap pihak-pihak yang ingin mengakses sistem infomasi ataupun keaslian data dari sistem informasi itu sendiri (*data origin authentication*). Contoh serangannya adalah *password* palsu, terminal palsu, atau situs web palsu. Proteksi dilakukan dengan *certificates.*
4. Ketiadaan penyangkalan (*nonrepudiation*)
   Ketiadaan penyangkalan adalah layanan yang berfungsi untuk mencegah terjadinya penyangkalan terhadap suatu aksi yang dilakukan oleh pelaku sistem informasi.

D. *Monoalphabetic Cipher*

Caesar Cipher adalah kasus khusus dari alfabet tunggal di mana susunan huruf *ciphertext* diperoleh dengan menggeser huruf-huruf alfabet sejauh 3 karakter, begitu juga ROT 13. Jika *plaintext* terdiri dari huruf-huruf alfabet, maka jumlah kemungkinan susunan huruf-huruf *ciphertext* yang dapat dibuat adalah sebanyak

26! = 403.291.461.126.605.635.584.000.000

Ini berarti terdapat 26! Buah kunci untuk menyusun huruf-huruf alfabet ke dalam tabel subsitusi. Susunan huruf di dalam tebel subsitusi *Caesar Cipher* adalah salah satunya. Susunan huruf-huruf *ciphertext* juga dapat diperoleh misalnya dengan menyusun huruf-huruf alfebet secara acak seperti tabel subtitusi berikut:

pi : 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
ci : D I Q M T B Z S Y K V O F E R J A U W P X H L C N G

Satu cara untuk membangkitkan tebel subsitusi adalah dengan sebuah kalimat yang mudah diingat. Misalkan kuncinya adalah sebuah kalimat :

we hope you enjoy this book

Dari kunci tersebut, buanglah perulangan huruf sehingga menjadi

wehopyunjtisbk

Lalu sambung dengan huruf-huruf lain yang tidak terdapat di dalam kalimat tersebut sehingga menjadi

w e h o p y u n j t i s b k a c d f g l m q r v x z

Dengan demikian, tabel subsitusi yang diperoleh adalah

pi : 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
ci : W E H O P Y U N J T I S B K A C D F G L M Q R V X Z

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* pada 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 :

$$Ci = (Pi + Ki - 2 \times 64) \bmod 26 + 64$$

dan rumus dekripsi dari *One Time Pad* yaitu :

Pi = (Ci – Ki + 26) mod 26 + 64

Keterangan rumus :

Ci = Cipherteks *(Ciphertext)*,
Pi = Plainteks *(Plaintext)*,
Ki = Kunci *(Key)*.

III. PEMBAHASAN

A. *Monoalphabetic chiper*

Proses enkripsi yang dilakukan pada data teks melalui tahap enkripsi kriptografi *Monoalphabetic Cipher* setelah itu hasil enkripsi dari data teks tersebut di enkripsi dengan *Vigenere Cipher* sehingga data teks yang terenkripsi akan mengalami perubahan menjadi data teks yang tidak dapat dimengerti.

1. Tahap Enkripsi *Monoalphabetic Cipher*

   Seperti sudah disebutkan dalam landasan teori, *Monoalphabetic Cipher* (*cipher* abjad- tunggal) adalah algoritma yang mengganti setiap huruf di dalam abjad dengan sebuah huruf lain dalam abjad yang sama. Jumlah kunci di dalam cipher abjad-tunggal sama dengan jumlah cara menyusun 26 huruf abjad tersebut. Ini berarti terdapat 26 buah kunci untuk menyusun huruf- huruf alfabet ke dalam tabel substitusi. Contohnya, susunan huruf-huruf untuk *ciphertext* diperoleh dengan menyusun huruf-huruf abjad menggunakan metode *Caesar Cipher*, *Rot13*, dan *Simple Subsitution Cipher*, berikut ini adalah tabel substitusi yang disusun bedasarkan ke tiga metode tersebut:

   Tabel substitusi dengan metode *Caesar Cipher* :

   pi : 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
   ci : D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

   Tabel substitusi dengan metode *Rot13* :

   pi : 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
   ci : D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

   membangkitkan tabel subsitusi dengan metode *Simple Subsitution Cipher* adalah dengan sebuah kalimat yang mudah diingat. Misal kuncinya adalah:

   AKU CINTA KAMU

   Dari kunci tersebut, buanglah perulangan huruf sehingga menjadi

   AKUCINTM

   Lalu sambung dengan huruf-huruf lain yang tidak terdapat di dalam kalimat tersebut sehingga menjadi:

   A K U C I N T M B D E F G H J L O P Q R S V W X Y Z

   Dengan demikian, tabel subsitusi yang diperoleh adalah

   Pi : 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
   Ci : A K U C I N T M B D E F G H J L O P Q R S V W X Y Z

2. Tahap Dekripsi *Monoalphabetic Cipher*

   Selanjutnya hasil *plaintext* dekripsi *Monoalphabetic Cipher* dengan menggunakan tabel subsitusi yang sudah di tentukan melalui kunci: AKU CINTA KAMU saat melakukan enkripsi. Proses dekripsi dilakukan dengan cara berikut:

   Tabel substitusi:

   ci : A K U C I N T M B D E F G H J L O P Q R S V W X Y Z

   pi : 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

   Ciphertext : AKUCINTM
   Plaintext : AKU CINTA KAMU

B. *Algoritma One Time Pad*

1. Tahap Enkripsi *Algoritma One Time Pad*

   Berikut ini proses enkripsi algoritma *One Time Pad*, dimana terdapat sebuah *plaintext* “CINTA” dengan *key* = “KASIH”.

   Plaintext = “CINTA”
   Key = “KASIH”

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

   $C_1 = (P_1 + K_1 – 2 \times 64) \bmod 26 + 64$
   $= (67 + 75 – 2 \times 64) \bmod 26 + 64$
   $= (142 – 128) \bmod 26 + 64$
   $= (14) \bmod 26 + 64$
   $= 14 + 64$
   $C_1 = 78$

   Maka C_1**=78** huruf *ciphertext* dengan nilai **78** adalah **N**.

Dengan melakukan konsep yang sama maka didapatkan hasil sebagai berikut :

Plaintext = "CINTA"

Key = "KASIH"

Ciphertext = "NJGCI"

2. Tahap Dekripsi *Algoritma One Time Pad*

Proses dekripsi dapat dilihat pada perhitungan dibawah ini :

Ciphertext = "N"

Key = "K"

Dekripsi :

$P_1 = (C_1 - K_1 + 26) \bmod 26 + 64$

$= (N - K + 26) \bmod 26 + 64$

$= (78 - 75 + 26) \bmod 26 + 64$

$= 29 \bmod 26 + 64$

$= 3 + 64$

$= 67$

huruf *ciphertext* dengan nilai **67** adalah **C**.

IV. KESIMPULAN

Kesimpulan dari suatu penelitian merupakan penjelasan tentang hasil akhir yang menguraikan pencapaian dari tujuan penelitian. Dari hasil penelitian dan analisa yang dilakukan, maka dapat diambil kesimpulan-kesimpulan. Adapun kesimpulan-kesimpulan tersebut adalah sebagai berikut :

1. Pada algoritma *Monoalphabetic chipper* menggunakan 3 metode, yaitu : *Caesar Cipher, Rot13, Simple Subsitution Cipher.* Masing-masing metode memliki sifat-sifat yang berbeda, akan tetapi tidaklah menjamin apakah algoritma *Monoalphabetic chipper* lebih baik daripada algoritma *One Time Pad.*
2. Pada algoritma *One Time Pad* bersifat panjang plainteks (pesan) harus sama panjang dengan kunci, penelitian dengan menggunakan tabel ASCII dan panjang *key* tidak harus sama dengan panjang plainteks. Akan tetapi, kunci yang tidak sama harus mengulang kata sehingga panjang *key* sama dengan panjang pesan.
3. *Monoalphabetic Cipher* atau disebut juga *cipher* substitusi sederhana (*simple subsitution cipher*), karena memilki sifat yaitu satu huruf di *plaintext* diganti dengan tepat satu huruf *ciphertext*. Jadi, fungsi *ciphering*-nya adalah satu ke satu, sementara algoritma *One Time Pad* memiliki sifat bahwa panjang plainteks (pesan) harus sama panjang dengan kunci.
4. Jika diperhatikan dari algortimanya bahwa kedua algoritma ini baik digunakan, akan tetapi algoritma *monoalphabetic chiper* memiliki kelemahan pada *ciphertext*-nya, yaitu beberapa karakter data masih sama dengan *plaintext*, sedangkan algoritma *One Time Pad* berbanding dengan *monoalphabetic chiper.*

REFERENSI

[1] Munir, Rinaldi. 2006, "*Diktat Kuliah Kritografi"*, Institut Teknologi Bandung, Bandung.

[2] Emy Setyaningsih, S.Si, M.Kom. 2015, "*Kriptografi & Implementasi Menggunakan. MATLAB*", CV. Andi Offset, Yogyakarta.

[3] Sugianto, Teguh Winarto. 2014. *"Kriptografi Gabungan menggunakan Algoritma Mono Alphabetic dan One Time Pad"*, STMIK Pontianak.

[4] Endah Pratiwi Lis. 2014. *"Program Aplikasi Kriptografi Penyandian One Time Pad Menggunakan Sandi Vinegere"*,Universitas Pendidikan Indonesia.

[5] Fransiskus Sarumaha. 2016 *"Implementasi Kriptografi Monoalphabetic Cipher dan Vigenere Cipher untuk Menyandikan data teks",* STMIK Budi Darma. Medan.

[6] Hasrul Hasrul, Lamro Herianto Siregar. 2016 *"Penerapan Teknik Kriptografi Pada Database Menggunakan Algoritma One Time Pad"* STMIK Bina Mulia Palu.

[7] Ariyus, Dony. 2008, *"Pengantar Ilmu Kriptografi Teori, Analisis, dan Implementasi"*, Andi, Yogyakarta.

[8] Sadikin, Rifki. 2012, "*Kriptografi untuk keamanan jaringan"*, Andi, Yogyakarta.