Jurnal Matematika Vol.17 No. 2 November 2018
ISSN: 1412-5056 / 2598-8980
http://ejournal.unisba.ac.id

Diterima: 20/09/2018
Disetujui: 03/11/2018
Publikasi Online: 26/11/2018

Kriptografi *Polyalphabetic One-Time Pad*

Cryptography Polyalphabetic One-Time Pad

Yurika Permanasari, Erwin Harahap

Program Studi Matematika, FMIPA, Universitas Islam Bandung

yurikape@unisba.ac.id, erwin2h@unisba.ac.id

Abstrak. Kriptografi *Polyalphabetic substitution chiper* melakukan teknik kriptografi *monoalphabetic* satu kali proses untuk suatu plainteks pesan. Algoritma polialphabetic cipher membuat ciperteks lebih kuat untuk dapat dipecahkan karena karakter plainteks yang sama tidak dienkripsi dengan cipherteks yang sama. One-Time Pad cipher adalah salah satu metoda ciphering polyalphabetic yang menggunakan tabel Vigenre. Kelebihan metoda *One-Time Pad* dibandingkan *polyalphabetic* lain adalah, kunci yang dibangkitkan secara acak sehingga tidak membentuk suatu kalimat berarti, menyebabkan metoda ini sulit dipecahkan secara terkaan maupun analisis frekuensi. Kelebihan lain adalah cipherteks yang sama didekripsi menggunakan kunci yang berbeda, menghasilkan plainteks yang berbeda.

Kata kunci : Polyalphabetic Cipher, Tabel Vigenre, One-Time Pad Cipher

Abstract. Cryptography Polyalphabetic substitution chipers perform monoalphabetic cryptographic techniques once for a plaintext message. The polialphabetic cipher algorithm makes ciperteks stronger to be solved because the same plainteks character is not encrypted with the same ciphertext. One-Time Pad cipher is one of the polyalphabetic ciphering methods that uses Vigenre tables. The advantages of the One-Time Pad method compared to other polyalphabetic methods are that keys that are generated randomly so that they do not form a meaningful sentence, cause this method to be difficult to solve by guessing or frequency analysis. Another advantage is that the same ciphertext is decrypted using a different key, resulting in a different plaintext.

Keywords: Polyalphabetic Cipher, Vigenre Table, One-Time Pad Cipher

1. Pendahuluan

Polyalphabetic Cipher merupakan pengembangan dari metode substitusi monoalphabetic [1]. Algoritma polyalphabetic cipher mengenkripsi sekelompok karakter atau string dengan melibatkan penggunaan kunci berbeda. Penerapan polyalphabetic cipher pada umumnya adalah mengulang kunci monoalphabetic selama *n* periode [5]. Dimana jumlah periode tersebut sama dengan panjang plainteks.

Vigenere Cipher adalah metode yang merupakan dasar dari *polyalphabetic substitution cipher*. Beberapa ketentuan dalam dalam metode ini antara lain: Kata kunci digunakan untuk menentukan enkrispsi setiap alphabet dalam plainteks, setiap kunci dapat disubstitusi dengan bermacam-macam kunci yang lain dan dapat digunakan secara berulang, huruf ke-i dalam plainteks di spesifikasikan oleh alphabet yang digunakan dalam kunci [2]. *Vigenere Cipher* menggunakan tabel berikut yang dikenal kemudian sebagai Tabel *Vigenere* sebagaimana ditunjukkan pada Gambar 1. Huruf plainteks berada pada kolom teratas, dan *key* diindikasi oleh baris.

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

Gambar 1. Tabel Vigenere

Algoritma kriptografi *Vigenere* memiliki tiga metode dalam teknik penyandiannya, yaitu Metode Vigenere, Metode Polyalphabetic, dan One-Time Pad. Perbedaan dari ketiganya metode adalah pada saat padding kata kunci agar sama panjang dengan plainteks. Metode Vigenere melakukan padding dengan menambahkan karakter plainteks, metode *Polyalphabetic* melakukan padding dengan menambahkan karakter kunci, sedangkan metode One-Time Pad menggunakan karakter random yang tidak bermakna sepanjang plainteks.

2. One-Time Pad Chiper

Algotritma One-Time Pad adalah salah satu algoritma kriptografi simetri (kunci sama untuk enkripsi dan dekripsi) dan merupakan *polyalphabetic cipher*. One-Time Pad merupakan bagian dari teknik ciphering dengan menggunakan tabel Vigenre. Algoritma One-Time Pad seperti pada polyalphabetic cipher umumnya, menggunakan kunci yang sama panjang dengan panjang plainteks. Pemakaian algoritma menggunakan sederetan abjad dari A ... Z, dengan memberikan nilai pada tiap-tiap abjad yaitu A = 0, B = 1, C = 2, ..., Z = 25. Sehingga rumus yang berlaku adalah sebagai berikut [3] :

Enkripsi : $C_i = (P_i + K_i)\ mod\ 26$

$C_i = (P_i + K_i) - 26$ jika $(P_i + K_i) > 26$

Dekripsi : $P_i = (C_i - K_i) mod\ 26$

$P_i = (C_i - K_i) + 26$ jika $(C_i - K_i)$ negatif

One-Time Pad dijelaskan pertama kali oleh Frank Miller pada tahun 1882 dan dimunculkan kembali oleh Gilbert Vernam (dari AT &T Corporation yang kemudian mematenkannya pada tahun 1919 bersama-sama dengan seorang kapten di Angkatan Darat AS Joseph Maugborgne yang menyatakan bahwa algoritma One-Time Pad adalah kriptografi yang sulit dipecahkan [4]. Tingkat keamanan tinggi yang diberikan oleh algoritma ini adalah dari penggunaan kunci acak sepanjang palinteks.

Berikut proses metode One-Time Pad :

Plainteks	**G**	**A**	**N**	**T**	**I**	**P**	**R**	**E**	**S**	**I**	**D**	**E**	**N**
Kunci	H	O	I	B	C	J	C	X	Y	J	Q	F	H
Cipherteks	N	O	V	U	K	Y	T	B	Q	R	T	J	U

Gambar 2. Proses One-Time Pad

One-Time Pad atau penggunaan sekali kunci merupakan gagasan yang sangat kuat tentang keamanan pesan. Kekuatan terletak pada penggunaan kunci random sekali pakai (Gambar 2). Hal ini tidak memberikan informasi tambahan tentang plainteks selain panjang plainteks itu sendiri.

3. Penutup

One-Time Pad Cipher mengenkripsi sekumpulan karakter dalam pesan dalam satu proses dan dapat menyembunyikan hubungan antara plainteks dengan cipherteks, karena huruf yang sama di-enkripsi menjadi huruf cipherteks yang berbeda, sehingga menyulitkan menterjemahkan pesan dengan metode terkaan ataupun analisis frekuesi jika tidak mengetahui kunci. Keunggulan lain dari One-Time Pad adalah kunci yang dibangkitkan secara acak dan digunakan sekali pakai, sehingga metode dapat merahasiakan pesan dengan kemanan kuat karena cipherteks tidak memberikan informasi lain selain panjang plainteks.

Daftar Pustaka

[1] Y Permanasari, "Kriptografi Klasik Monoalphabetic", *Jurnal Matematika*, Vol 16 No 1, Mei 2016. h. 7-10.

[2] R Munir, "Kriptografi", *Bandung: Informatika*, 2009.

[3] W. Stallings, "Cryptography and Network Security Principles and Practices", *USA: Prentice Hall*, 2003.

[4] S M Bellovin, "Frank Miller: Inventor of the One-Time Pad", *Cryptologia*, Vol 35 No 3, 2011. pp. 203–222.

[5] Y. Permanasari, E Harahap, "Kriptografi Polyalphabetic", *Jurnal Matematika*, Vol 17 No 1, Mei 2017. h. 31-34.

(halaman ini sengaja dikosongkan)