Jurnal Matematika Vol.17 No.1 Mei 2018
ISSN: 1412-5056 / 2598-8980
http://ejournal.unisba.ac.id

Diterima: 10/11/2017
Disetujui: 14/02/2018
Publikasi Online: 26/05/2018

Kriptografi Polyalphabetic

Yurika Permanasari, Erwin Harahap

Program Studi Matematika, FMIPA, Universitas Islam Bandung

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

Abstrak. Kriptografi polyalphabetic merupakan improvisasi dari teknik substitusi monoalphabetic. Polyalphabetic substitution chiper melakukan teknik kriptografi monoalphabetic satu kali proses untuk suatu plainteks pesan. Algoritma polyalphabetic cipher membuat ciperteks lebih kuat untuk dapat dipecahkan karena karakter plainteks yang sama tidak dienkripsi dengan cipherteks yang sama. Kunci enkripsi polyalphabetic cipher dapat berbeda sehingga mempunyai kemungkinan kombinasi yang lebih bervariasi dan lebih sulit dipecahkan. Metode Vigenere cipher menjadi dasar dari polyalphabetic substitution cipher. Teknik enkripsi Vigenere cipher menggunakan tabel yang dikenal dengan tabel Vigenere yang digunakan dan menjadi acuan dibeberapa algoritma pengembangan metode polyalphabetic cipher. Metode polyalphabetic cipher lain adalah playfair cipher, menggunakan tabel kunci berupa matriks 5x5 untuk proses enkripsi sehingga memiliki 25! kemungkinan kunci yang cukup sulit dipecahkan.

Kata kunci : polyalphabetic cipher, vigenre cipher, playfair cipher

Abstract. (*Polyalphabetic Cryptography*) Polyalphabetic cryptography is an improvisation of monoalphabetic substitution techniques. Polyalphabetic substitution cipher performs one-time monoalphabetic cryptographic technique for a message text message. The polyalphabetic cipher algorithm makes cipertext stronger to be solved because the same plaintext character is not encrypted with the same ciphertext. The key to polyalphabetic cipher encryption can be different so that it has a more varied and more difficult to solve combination possibilities. The Vigenere cipher method is the basis of polyalphabetic substitution cipher. Vigenere cipher encryption techniques use tables known as Vigenere tables which are used and become references in several algorithms for developing polyalphabetic cipher methods. Another polyalphabetic cipher method is playfair cipher, using a key table in the form of a 5x5 matrix for the encryption process so that it has 25! Possible keys that are quite difficult to solve.

Keywords: polyalphabetic cipher, vigenere cipher, playfair cipher

1. Pendahuluan

Monoalphabetic Cipher mengenkripsi setiap karakter dalam pesan. Huruf yang sama di-enkripsi menjadi huruf cipherteks yang sama, sehingga huruf yang sering muncul di dalam plainteks, sering muncul pula di dalam cipherteks-nya. Oleh karena itu monoalphabetic chiper akan mudah dipecahkan dengan menggunakan analisis frekuensi kemunculan huruf. Teknik monoalphabetic chiper juga tidak dapat menyembunyikan hubungan antara plainteks dengan cipherteks, sehingga mudah didekripsi mengunakan metode terkaan. Karena itu, untuk membuat cipher supaya lebih aman, cryptographer tertarik dalam pengembangan teknik enciphering yang kebal dari analisis frekuensi.

Salah satu pendekatan teknik penyandian untuk membuat cipher lebih aman adalah dengan menggunakan lebih dari satu alphabet dalam melakukan encrypt pesan, lebih umum dikenal dengan Polyalphabetic Cipher. Polyalphabetic Cipher ditemukan pertama kali oleh Leon Battista pada tahun 1568. Metode ini digunakan sebagai pengembangan dari metode substitusi monoalphabetic. Sesuai dengan namanya, algoritma polyalphabetic cipher meng-enkripsi sekelompok karakter atau string dengan melibatkan penggunaan kunci berbeda.

Penerapan polyalphabetic cipher pada umumnya adalah mengulang kunci monoalphabetic selama *n* periode. Dimana jumlah periode tersebut sama dengan panjang plainteks. Dengan kata lain, panjang

kunci sama dengan panjang palinteks, seperti dicontohkan sebagai berikut : Misal, diketahui kunci = KUNCI, sehingga kunci diperluas menjadi KUNCIKUNCI... sampai ukurannya sama dengan plain text. Jika setiap hurup diberi bobot A = 0, B = 1, …, Z = 25.

Plainteks : SERANGMIPA
Kunci : KUNCIKUNCI
Cipherteks : DY…….

(S + K) mod 26 = (18 + 11) mod 26 = 3 = D
(U + E) mod 26 = (20 + 4) mod 26 = 24 = Y

Metode polyalphabetic juga menghasilkan pola enkripsi yang lebih acak karena tiap huruf yang sama, menghasilkan enkripsi yang berbeda. Plainteks diatas memiliki dua huruf A yang dienkripsi berbeda menjadi huruf C dan I.

2. Vigenere Cipher

Metode ini diperkenalkan oleh Balise de vigenere pada tahun 1585 sebagai bentuk pengembangan dari metode monoalphabethic. Metode ini juga 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. Vigenere Cipher menggunakan tabel berikut yang dikenal kemudian sebagai Tabel Vigenere:

Tabel 1. Tabel Vigenere

	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

Huruf plainteks berada pada kolom teratas, dan key diindikasi oleh baris. Berikut contoh penggunaan Vigenere cipher dengan kata kunci : **deceptive**

Key	d e c e p t i v e w e a r e d i s c o v e r e d s a v
Plaintext	We a r e d i s c o v e r e d s a v e y o u r s e l f
Ciphertext	Z I CVTWQNGRZ GVTWAVZHCQYGLMGJ

3. Playfair Chiper

Playfair Cipher ditemukan oleh Sir Charles Wheatstone (1802-1875) pada tahun 1854, dan dipopulerkan oleh Baron Lyon Playfair (1819-1898). Playfair Cipher merupakan suatu algoritma kriptografi klasik yang termasuk ke dalam polyalphabetic cipher, dimana plainteks diubah menjadi bentuk poligram dan proses enkripsi dekripsi dilakukan untuk poligram tersebut. Algoritma enkripsi berdasarkan matriks huruf 5x5 yang yang dibentuk dari kata kunci dengan tak ada duplikasi huruf. Matriks diisi dari kiri ke kanan, dari atas ke bawah. Elemen matriks yang masih kosong diisi huruf-huruf dalam urutan alpfabet yang tersisa. Plainteks dienkripsi dua huruf-dua huruf (bigram). Jika jumlah huruf ganjil, maka tambahkanhuruf X atau Z. Tidak ada huruf yang terulang pada bigram, jika ada yang berulang, pisahkan dan tambahkan huruf lain, misalnya X, BALLOON : BA LX LO ON.

Algoritma enkripsi sebagai berikut:

1. Jika dua huruf plainteks terdapat pada baris kunci yang sama maka tiap huruf diganti dengan huruf di kanannya (pada matriks)
2. Jika dua huruf terdapat pada kolom kunci yang sama maka tiap huruf diganti dengan huruf di bawahnya
3. Jika dua huruf tidak pada baris yang sama atau kolom yang sama, maka huruf plainteks akan diganti menjadi huruf yang berada pada kolom yang sama dengan huruf lainnya dan baris yang sama dengan huruf tersebut

Berikut adalah implementasi dari algoritma Playfair cipher , kata kunci YURIKAP maka dapat dibentuk matriks kunci seperti dibawah ini :

U	**R**	**I/J**	**K**
P	**B**	**C**	**D**
F	**G**	**H**	**L**
N	**O**	**Q**	**S**
V	**W**	**X**	**Z**

Maka jika plainteks : **MATEMATIKA**, menjadi sekelompok bigram MA TE MA TI KA , masing masing akan diekripsi menjadi : TE YM TE XY YD

4. Penutup

Polyalphabetic Cipher mengenkripsi sekumpulan karakter dalam pesan dalam satu proses. Teknik polyalphabetic chiper dapat menyembunyikan hubungan antara plainteks dengan cipherteks, karena huruf yang sama dienkripsi menjadi huruf cipherteks yang berbeda, sehingga menyulitkan menterjemahkan pesan dengan metode terkaan ataupun analisis frekuesi jika tidak mengetahui kunci. Algoritma polyalphabetic cipher memungkinkan penggunaan kunci yang berbeda, oleh karena itu polyalphabetic chiper akan lebih sulit dipecahkan karena selain algoritmanya lebih panjang dari algoritma monoalphabetic, plainteks yang sama didekripsi dengan kunci yang berbeda akan menghasilkan cipherteks yang berbeda.

Referensi

[1] Munir, Rinaldi. *Kriptografi*. Informatika, Bandung, 2009

[2] Menezes, Alfred J., Paul C. van Oorschot and Scott A.Vanstone, *Handbook of Applied Cryptography*, 5th printing,CRC Press, 2001

[3] Schenier, Bruce. *Applied Cryptography (Protocol, Algorithm, and Source Code in C)*, 2nd edition, John Wiley & Sons, New York, 1996.

[4] Stallings, William. *Cryptography and Network Security Principles and Practices*. International Edition 3rd edition, Prentice Hall USA, 2003.

[5] Y. Permanasari, E. Harahap. *Algoritma Data Encryption Standard (DES) Pada Electronic Code Book (ECB)*. Jurnal Matematika UNISBA, Vol. 6, No. 1. 2007. pp. 77-84.

[6] A. Priatmoko, E. Harahap. *Implementasi Algoritma DES Menggunakan MATLAB*. Jurnal Matematika UNISBA, Vol. 16, No. 1. 2017.

[7] Y. Permanasari. *Kriptografi Klasik Monoalphabetic*. Jurnal Matematika UNISBA, Vol. 16, No. 1. 2017.

[8] R. Tennekoon, J. Wijekoon, E. Harahap, dan H. Nishi. *Per-hop data encryption protocol for transmitting data securely over public netrwork*. Procedia Computer Science. Volume. 32. 2014. pp. 965-972. DOI: 10.1016/i.procs.2014.05.519

[9] R. Tennekoon, J. Wijekoon, E. Harahap, H. Nishi, E. Saito, S *Katsura. Per hop data encryption protocol for transmission of motion control data over public networks*. Proceeding Advanced Motion Control (AMC) on IEEE 13th International Workshop, Yokohama, Japan. 2014. pp.128-133.

[10] A. Tulloh, Y. Permanasari, E. Harahap. 2016. *Kriptografi Advanced Encryption Standard (AES) Untuk Penyandian File Dokumen*. Jurnal Matematika UNISBA. Vol. 15 No 1, Mei 2016. pp. 7-14.