ANALISIS PENGGUNAAN PERSAMAAN KUADRAT MATEMATIKA SEBAGAI KUNCI PADA MONOALPHABETIC CIPHER

Ikhsani Annisa Khozinati[1], Billy Arifa Tengger[1]
Universitas Nahdlatul Ulama Purwokerto[1], annisakhozinati@gmail.com[1]

Article Info :
Received : 19-09-2020
Revised: 09-10-2020
Accepted : 10-10-2020

Keywords :
1. Monoalphabetic Chiper
2. Quadratic Equation
3. Substitution Table

Kata Kunci :
1. Chiper Abjad Tunggal
2. Persamaan Kuadrat
3. Tabel Substitusi

ABSTRACT
Monoalphabetic cipher is an encryption substitution method that maps each alphabet to another alphabet randomly. This method is different from the Caesar cipher, which only shifts the alphabet. In addition, in monoalphabetic ciphers, substitution tables are used to store keys, where these keys are useful for mapping alphabets from plaintext to ciphertext. However, in reality the use of substitution tables still has difficulties. Based on this, an idea emerged to analyze whether the substitution table could be replaced by a mathematical equation to be used as a key to the monoalphabetic cipher. And in this case, the mathematical equation used is a quadratic equation.

ABSTRAK
Monoalphabetic cipher merupakan enkripsi metode substitusi yang memetakan tiap-tiap abjad dengan abjad lain secara random. Metode ini berbeda dengan Caesar cipher yang hanya melakukan pergeseran abjad. Selain itu, pada monoalphabetic cipher digunakan tabel substitusi untuk menyimpan kunci, dimana kunci tersebut berguna untuk memetakan abjad dari plaintext ke ciphertext. Akan tetapi, pada kenyataanya penggunaan tabel substitusi masih memiliki kesulitan. Berdasarkan hal tersebut, muncul lah sebuah ide untuk menganalisis apakah tabel substitusi dapat diganti oleh persamaan matematika untuk dijadikan kunci pada monoalphabetic cipher. Dan dalam hal ini, persamaan matematika yang digunakan adalah persamaan kuadrat.

I. PENDAHULUAN

Monoalphabetic chiper yang termasuk dalam algoritma kriptografi klasik, diperkenalkan oleh ilmuwan Arab, Abu Alkin, didalam bukunya yang berjudul *"A Manuscript on Deciphering Cryptographic Messages"* yang dipublikasikan pada abad ke-9. Monoalphabetic cipher merupakan enkripsi metode substitusi yang memetakan tiap-tiap abjad dengan abjad lain secara random. Metode ini berbeda dengan Caesar cipher yang hanya melakukan pergeseran abjad. Selain itu, pada monoalphabetic cipher digunakan tabel substitusi untuk menyimpan kunci, dimana kunci tersebut berguna untuk memetakan abjad dari plaintext ke ciphertext. Akan tetapi, pada kenyataanya penggunaan tabel substitusi masih memiliki kesulitan.

Berdasarkan hal tersebut, muncul lah sebuah ide untuk menganalisis apakah tabel substitusi dapat diganti oleh persamaan matematika untuk dijadikan kunci pada monoalphabetic cipher. Dan dalam hal ini, persamaan matematika yang digunakan adalah persamaan kuadrat.

II. METODE PENELITIAN

2.1. Tabel Substitusi (Substitution Table)

Pada Monoalphabetic cipher digunakan tabel substitusi untuk menyimpan kunci, dimana kunci tersebut berguna untuk memetakan abjad dari plaintext ke ciphertext. Selain itu, tabel substitusi juga berguna sebagai pengingat padanan abjad, baik pada plaintext maupun ciphertext. Agar diperoleh padanan abjad, biasanya akan dipilih secara acak dari 26 abjad yang ada dan dengan catatan tidak ada abjad yang berulang.

Contoh Tabel Substitusi

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

2.2. Persamaan Kuadrat Matematika

Ada banyak persamaan yang dikenal dalam ilmu matematika. Seperti persamaan linear, persamaan kuadrat, persamaan lingkaran, persamaan trigonometri dan lainnya. Dari banyaknya persamaan tersebut, terdapat satu persamaan yang sering digunakan dan dipelajari yaitu persamaan kuadrat. Persamaan kuadrat merupakan persamaan dari variabel yang mempunyai pangkat tertinggi dua (orde 2). Adapun bentuk umumnya yaitu **$y = ax^2 + bx + c$,** dengan a,b sebagai koefisien dan c sebagai konstanta.

Persamaan kuadrat sering digunakan dalam menyelesaikan permasalahan sehari-hari seperti menghitung gerak suatu objek, menghitung panjang/lebar suatu bangunan, menghitung jarak tempuh dan sebagainya. Dikarenakan penerapan yang begitu banyak, maka pada analisis dan pengujian ini digunakan lah persamaan kuadrat.

III. HASIL DAN PEMBAHASAN

3.1 Analisis Penggunaan Persamaan Kuadrat sebagai Kunci Pada Monoalphabetic Chiper

Untuk mengetahui apakah persamaan kuadrat dapat digunakan sebagai kunci pada monoalphabetic cipher, maka terlebih dahulu dilakukan pengujian. Pada tahap pengujian ini digunakan persamaan kuadrat dengan bentuk umumnya yaitu **$y = ax^2 + bx + c$,** dimana a , b, dan c merupakan konstanta, sedangkan y merupakan abjad chiper yang dihasilkan dan x merupakan abjad plainnya. Dalam hal ini akan dilakukan 3 jenis pengujian yaitu pengujian terhadap konstanta a, pengujian terhadap konstanta b, dan pengujian terhadap konstanta c.

3.1.1 Uji Coba terhadap konstanta a

Pada tahap pengujian ini, kita memilih beberapa sampel persamaan kuadrat, dimana sampel tersebut memiliki nilai konstanta a yang berbeda (bilangan ganjil dan genap). Misalnya :

$$y = x^2 + x + 1$$
$$y = 2x^2 + x + 1$$
$$y = 3x^2 + x + 1$$
$$y = 4x^2 + x + 1.$$

Sebelum melakukan pengujian perhatikan tabel berikut :

Tabel padanan abjad dengan numerik

A → 1	H → 8	O → 15	V → 22
B → 2	I → 9	P → 16	W → 23
C → 3	J → 10	Q → 17	X → 24
D → 4	K → 11	R → 18	Y → 25
E → 5	L → 12	S → 19	Z → 26
F → 6	M → 13	T → 20	
G → 7	N → 14	U → 21	

→

$y = x^2 + x + 1$

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

$y = 2x^2 + x + 1$

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

$y = 3x^2 + x + 1$

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

$y = 4x^2 + x + 1$

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

Ternyata dari hasil pengujian terhadap sampel-sampel diatas, terdapat beberapa abjad cipher yang muncul lebih dari 1 kali, hal ini menunjukkan bahwa kunci yang dihasilkan tidak memiliki keunikan/mudah diketahui sehingga kurang efektif diterapkan pada monoalphabetic cipher.

3.1.2 Uji coba terhadap konstanta b

Pada tahap pengujian ini, kita memilih beberapa sampel persamaan kuadrat, dimana sampel tersebut memiliki nilai konstanta b yang berbeda (bilangan ganjil dan genap). Misalnya:

$$y = x^2 + 2x + 1$$
$$y = 2x^2 + 2x + 1$$
$$y = 2x^2 + 3x + 1$$
$$y = 3x^2 + 3x + 1$$

Sebelum melakukan pengujian perhatikan tabel berikut :

$y = x^2 + 2x + 1$

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

$y = 2x^2 + 2x + 1$

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

$y = 2x^2 + 3x + 1$

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

$y = 3x^2 + 3x + 1$

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

3.1.3 Uji coba terhadap konstanta c

Pada tahap pengujian ini, kita memilih beberapa sampel persamaan kuadrat, dimana sampel tersebut memiliki nilai konstanta c yang berbeda (bilangan ganjil dan genap). Misalnya:

$$y = x^2 + x + 2$$
$$y = 2x^3 + 3x+3$$
$$y = 3x^2 + 2x + 4$$
$$y = x^2 + 2x + 5$$
$$y = 2x^2 + 4x + 5$$
$$y = 2x^2 + 3x + 4$$

$y = x^2 + x + 2$

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

$= 2x^2 + 3x + 3$

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

$y = 2x^2 + 3x + 3$

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

$y = 3x^2 + 2x + 4$

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

$y = x^2 + 2x + 5$

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

$y = 2x^2 + 4x + 5$

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

$y = 2x^2 + 3x + 4$

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

$y = 2x^2 + 3x + 3$

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

Dari hasil pengujian sampel-sampel diatas, ternyata terdapat beberapa abjad cipher yang muncul lebih dari 1 kali, hal ini menunjukkan bahwa kunci yang dihasilkan tidak memiliki keunikan/mudah diketahui sehingga kurang efektif diterapkan pada monoalphabetic cipher.

IV. KESIMPULAN DAN SARAN

Beberapa uji coba persamaan kuadrat matematika kurang efektif digunakan sebagai kunci pada monoalphabetic cipher. Hal ini dikarenakan kunci yang dihasilkan tidak bersifat unik sehingga dikhawatirkan pesan yang disampaikan akan mudah diketahui. Perlu adanya kajian lebih luas mengenai polinomial dan ruang lingkpupnya.

V. DAFTAR PUSTAKA

[1] Munir, Rinaldi, Dr. 2019. *Kriptografi, edisi kedua.* Bandung : Informatika Bandung

[2] Sandi Substitusi - Wikipedia Diakses dari : https://id.m.wikipedia.org/wiki/Sandi_substitusi

[3] Persamaan Kuadrat - Wikipedia Diakses dari : https://id.m.wikipedia.org/wiki/Persamaan_kuadrat