ANALISIS KEMUNGKINAN PENGGUNAAN PERSAMAAN LINEAR MATEMATIKA SEBAGAI KUNCI PADA MONOALPHABETIC CIPHER

ARIF NANDA ATMAVIDYA (13506083)
Program Studi Informatika, Institut Teknologi Bandung, Jalan Ganesha 10 Bandung 40132
email: 1f16083@students.if.itb.ac.id

Abstraksi *– Monoalphabetic cipher atau biasa disebut sebagai cipher abjad tunggal tergolong dalam algoritma kriptografi klasik dimana setiap huruf dalam plaintext diganti dengan satu huruf lain yang bersesuaian. Untuk menyimpan kunci yang memetakkan huruf dalam plaintext ke ciphertext tersebut dipergunakan suatu tabel yang biasa disebut sebagai tabel substitusi.*
Dalam prakteknya, penggunaan tabel substitusi dipandang kurang praktis dan efisien terkait dengan proses pendistribusian kunci (kunci dikirim bersama dengan ciphertext), dan setiap kali membuat pesan rahasia seringkali orang zaman dahulu membuat tabel substitusi baru. Salah satu contoh dari monoalphabetic cipher yang sudah banyak dikenal ialah Caesar cipher. Algoritma ini telah memanfaatkan persamaan linear matematika sederhana, dan tidak bergantung sepenuhnya terhadap tabel substitusi.
Dalam makalah kriptografi ini, penulis akan menganalisis kemungkinan pemanfaatan persamaan matematika yang lebih kompleks dari persamaan matematika pada Caesar cipher, tetapi tetap pada lingkup persamaan linear, apakah bisa diterapkan sepenuhnya sebagai pengganti tabel substitusi pada monoalphabetic cipher.

Kata kunci : *monoalphabetic cipher, cipher abjad tunggal, persamaan linear, tabel substitusi, enkripsi, dekripsi.*

1. Pendahuluan

Monoalphabetic cipher atau biasa disebut sebagai cipher abjad tunggal tergolong dalam algoritma kriptografi klasik dimana setiap huruf dalam *plaintext* diganti dengan satu huruf lain yang bersesuaian. Untuk menyimpan kunci yang memetakkan huruf dalam *plaintext* ke *ciphertext* tersebut dipergunakan suatu tabel yang biasa disebut sebagai tabel substitusi. Tabel substitusi tersebut biasanya disertakan bersama dengan pesan rahasia, sehingga dapat didekripsi oleh si penerima, atau jika tidak, si penerima telah memiliki salinan tabel substitusi dari pesan terdahulu yang diterima.

Namun demikian, pemanfaatan tabel substitusi tersebut memiliki banyak kendala, antara lain :

- Pengiriman tabel substitusi yang disertakan dengan pesan rahasia tidak efektif dan efisien, bisa saja ketika pesan tersebut disadap oleh pihak tak berkepentingan, pihak tersebut dapat mendekripsi sendiri dengan menggunakan tabel substitusi tersebut.
- Proses pembangkitan kunci secara acak (random) pada tabel substitusi juga membutuhkan waktu.
- Untuk menjamin validitas tabel, sebaiknya setiap kali mengirim pesan digunakan tabel substitusi baru.

Dari kendala-kendala di atas, penulis ingin menganalisis kemungkinan pemanfaatan persamaan linear matematika untuk membangkitkan kunci pada *monoalphabetic cipher* serta bagaimana hubungan persamaan linear matematika tersebut terhadap keberadaan tabel substitusi.

2. Kajian Literatur

a. Tabel Substitusi

Monoalphabetic cipher memanfaatkan tabel substitusi sebagai pengingat padanan huruf pada

plaintext dan ciphertext. Untuk mendapatkan padanan huruf tersebut, biasanya dilakukan pemilihan secara acak terhadap dua puluh enam huruf yang ada, tanpa ada huruf yang mengalami pengulangan.

Contoh tabel substitusi :

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

Dengan demikian, maka jumlah maksimal kunci yang didapatkan dari algoritma *monoalphabetic cipher* ini sebanyak :

26! = 403.291.461.126.605.635.584.000.000

b. Persamaan Matematika

Walaupun begitu, Caesar cipher yang telah dikenal luas yang masih tergolong dalam *monoalphabetic cipher* telah menggunakan persamaan matematika, namun masih sangat sederhana.

$\mathbf{c_i = p_i + k}$

dimana ci = abjad ciphertext
pi = abjad plaintext
k = konstanta $\neq 0$

Persamaan matematika tersebut di atas hanya melakukan pergeseran abjad *plaintext* sebesar konstanta, dimana konstanta berlaku untuk semua huruf pada *plaintext*. Akibatnya, jika nilai konstanta diketemukan oleh kriptanalis, maka semua huruf *ciphertext* dapat dengan mudah didekripsi.
Dalam ilmu matematika, terdapat dua buah persamaan yang penting, yaitu persamaan linear dan persamaan kuadrat, perbedaannya terletak pada bilangan pangkat tertinggi (orde) variabel peubah.

y = ax + b (persamaan linear)

contoh : y = x + 4;
y = 2x + 6;
y = 3x – 1;

$\mathbf{y = ax^2 + bx + c}$ (persamaan kuadrat)

contoh : $y = x^2 + 2x - 1$;
$y = x^2 - 9$;
$y = 2x^2 - 3x + 5$;

Dalam pengujian dan analisis makalah ini, persamaan linear lah yang akan diuji coba untuk diterapkan pada algoritma *monoalphabetic cipher*, serta dianalisis lebih lanjut apakah dapat menghasilkan kunci yang lebih efektif dan efisien atau tidak.

3. Pengujian

Persamaan linear : **y = ax + b**

Dalam pengujian kali ini, a dan b didefinisikan sebagai konstanta, x adalah variabel huruf (abjad) plain, dan y atau f(x) ialah abjad cipher yang dihasilkan.

a. Pengujian terhadap konstanta a

Dalam pengujian pertama ini, coba digunakan sampel beberapa persamaan linear yang memiliki nilai konstanta a (pada persamaan y = ax + b) yang berbeda, misalnya y = **2**x + 1; y = **3**x + 1; y = **4**x + 1; dan y = **5**x + 1.

Tabel Padanan Abjad dengan Numerik

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

<u>Sampel 1 : y = 2x + 1</u>

- Untuk abjad A :
  y = 2x + 1
  y = 2(1) + 1
  = 3 → C

- Abjad B :
  y = 2x + 1
  y = 2(2) + 1
  = 5 → E

Dengan cara menghitung satu-persatu semua huruf, maka didapatkan abjad cipher yang merupakan padanan huruf plain seperti pada tabel berikut ini :

Substitusi abjad untuk y = 2x + 1

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

Dari pengujian persamaan y = 2x + 1 terlihat bahwa abjad cipher C, E, G, I, K, dan seterusnya muncul sebanyak 2 kali, artinya kunci yang dihasilkan tidak bersifat unik, dan akan sulit jika diterapkan pada *monoalphabetic cipher*.
Kemudian, akan diuji coba kembali untuk beberapa persamaan linear matematika lain dengan nilai a (pada persamaan y = ax + b) yang berbeda.

Sampel 2 : y = 3x + 1

Substitusi abjad untuk y = 3x + 1

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

Dari pengujian terhadap persamaan y = 3x + 1, tidak terjadi satu pun pengulangan abjad cipher, artinya kunci bersifat unik dan dapat diterapkan pada *monoalphabetic cipher*.

Sampel 3 : y = 4x + 1

Substitusi abjad untuk y = 4x + 1

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

Dari pengujian terhadap persamaan y = 4x + 1, terjadi pengulangan abjad cipher sebanyak 2 kali.

Sampel 4 : y = 5x + 1

Substitusi abjad untuk y = 5x + 1

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

Dari pengujian terhadap persamaan y = 5x + 1 tersebut, tidak terjadi satu pun pengulangan abjad cipher.

b. Pengujian Terhadap Konstanta b

Dalam pengujian kedua ini, coba digunakan sampel beberapa persamaan linear yang memiliki nilai konstanta b (pada persamaan y = ax + b) yang berbeda, misalnya y = 3x + **1** (sudah diuji di sampel 2); y = 3x + **2** dan y = 3x + **3**.

Hasil Sampel 2 : y = 3x + 1
(telah diuji sebelumnya)

Substitusi abjad untuk y = 3x + 1

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

G → V	O → T	W → R
H → Y	P → W	X → U

Sampel 5 : y = 3x + 2

Substitusi abjad untuk y = 3x + 2

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

Dari pengujian terhadap persamaan y = 3x + 2 tersbut, tidak terjadi satu pun pengulangan abjad cipher.

Sampel 6 : y = 3x + 3

Substitusi abjad untuk y = 3x + 3

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

Dari pengujian terhadap persamaan y = 3x + 3 tersbut, tidak terjadi satu pun pengulangan abjad cipher.

c. Pengujian Terhadap Caesar Cipher

Telah dijelaskan sebelumnya bahwa Caesar cipher merupakan contoh *monoalphabetic cipher* dengan konstanta a (pada persamaan y = ax + b) bernilai satu. Pengujian ini bertujuan membuktikan kembali validitas Caesar cipher sebagai bagian dari *monoalphabetic cipher* yang menggunakan persamaan linear sederhana.

Caesar cipher **: y = x + b**

Sampel 7 : y = x + 3

Substitusi abjad untuk y = x + 3

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

Dari pengujian terhadap persamaan Caesar cipher y = x + 3, sudah bisa ditebak tidak terjadi satu pun pengulangan abjad cipher.

4. Analisis dan Pembahasan

Setelah melakukan pengujian terhadap ke-6 sampel yang berbeda, maka didapat hasil sebgai berikut :

- Sampel 1 : y = 2x + 1 → gagal
- Sampel 2 : y = 3x + 1 → berhasil
- Sampel 3 : y = 4x + 1 → gagal
- Sampel 4 : y = 3x + 1 → berhasil
- Sampel 5 : y = 3x + 2 → berhasil
- Sampel 6 : y = 3x + 3 → berhasil
- Sampel 7 : y = x + 3 (Caesar cipher) → berhasil

gagal → abjad cipher yang didapatkan tidak bersifat unik (ada pengulangan)

berhasil → abjad cipher yang didapatkan bersifat unik (tidak ada pengulangan)

Setelah diamati dari sampel, jelas terlihat bahwa persamaan linear yang berhasil terdiri dari persamaan-persamaan yang memiliki konstanta a (pada y = ax + b) bernilai ganjil, semisal y = x + 3; y = **3**x + 1; y = **3**x + 2; y = **3**x + 3; dan y = **5**x + 1.

Sedangkan persamaan yang gagal memiliki konstanta a bernilai genap y = **2**x + 1; dan y = **4**x + 1;

Setelah melihat ketercapaian penggunaan persamaan linear sebagai kunci *monoalphabetic cipher*, dimana didapat persamamaan linear dengan konstanta a bernilai genap dianggap valid (sementara), maka timbul permasalahan bagaimanakah cara melakukan enkripsi dan dekripsi.

a. Proses Enkripsi

Jika kita sudah mendapatkan kunci yang bersifat unik, harusnya proses enkripsi bisa dilakukan dengan mudah.

Plaintext :

Aku anak sehat tubuhku kuat

Substitusi abjad untuk y = 3x + 1

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

Dengan melakukan substitusi abjad plain satu-persatu, didapat *ciphertext* :

Dhl dqdh fpydi ilglyhlj hldi

b. Proses Dekripsi

Ciphertext :

Dhl dqdh fpydi ilglyhlj hldi

Dari *ciphertext* di atas, akan coba didekripsi satu-persatu hurufnya.

D : 4 = 3x + 1; x = 1 → A

H : 8 = 3x + 1; x = 7/3 → ?

L : 12 = 3x + 1; x = 11/3 → ?

Q : 17 = 3x + 1; x = 16/3 → ?

Sehingga didapat keseluruhan *plaintext* :

A?? a?a? ?eha? ????h?c ??a?

Tentu saja, *plaintext* yang didapatkan sangat jauh dari harapan. Namun jika setelah mendapatkan kunci yaitu y = 3x + 1, lalu disusun tabel substitusi maka dapat diperoleh hasil yang benar.

Kunci : y = 3x + 1

Substitusi abjad untuk kunci y = 3x + 1

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

Maka dapat diperoleh *plaintext* :

Aku anak sehat tubuhku kuat

5. Kesimpulan

Dari analisis dan pemabahasan yang telah dilakukan, didapat kesimpulan :

a. Persamaan linear dapat dipergunakan sebagai kunci untuk algoritma *monoalphabetic cipher* asalkan memiliki konstanta a bernilai 1.
   y = ax + b; dimana a ∈ bilangan ganjil

b. Proses enkripsi dapat langsung dilakukan tanpa perlu adanya tabel substitusi lagi.
c. Jika proses dekripsi dilakukan secara langsung dari *ciphertext* tanpa tabel substitusi, maka *plaintext* yang didapatkan tidak sesuai harapan.
d. Proses dekripsi harus dilakukan melalui tabel substitusi yang dibangkitkan dari kunci persamaan linear.

e. Persamaan linear tidak dapat digunakan untuk menggantikan tabel substitusi sepenuhnya, namun dapat digunakan untuk memperoleh kunci yang memetakkan dari abjad plain ke abjad cipher.
f. Penggunaan kunci persamaan linear ini dapat mengefisienkan pengiriman pesan rahasia karena tidak butuh menyertakan tabel substitusi, yang diperlukan hanya si penerima mengetahui kuncinya dan menyusun tabel substitusi untuk mendekripsi pesan.

6. Pustaka

[1] Munir, Rinaldi, Ir.,M.T. 2007. *Diktat Kuliah IF-5054 Kriptografi.* Bandung : Informatika ITB
[2] Substitution cipher – Wikipedia. http://en.wikipedia.org/wiki/Substitution_cipher
[3] Monoalphabetic cipher. http://ling.ohio-state.edu/~cbrew/2007/spring/codes