Modifikasi *Ceasar Cipher* menjadi Cipher Abjad-Majemuk dan Menambahkan Kunci berupa Barisan Bilangan

Ari Wardana / 135 06 065
Program Studi Teknik Informatika, Institut Teknologi Bandung
Jl. Ganesha 10, Bandung 40132
e-mail : if16065@students.if.itb.ac.id

Abstract

Salah satu teknik kriptografi klasik paling tua yaitu *Caesar cipher*. Teknik ini telah digunakan pada masa Romawi kuno oleh Julius Caesar. Teknik ini menerapkan teknik *Cipher* Subtitusi. Pada teknik ini dilakukan pergeseran huruf alfabet *plain text* sehingga didapatkan huruf baru yang digunakan pada *cipher text*.

Akan tetapi, teknik *Ceasar Cipher* memiliki banyak kelemahan. Pada teknik ini memiliki jumlah kuncinya sangat sedikit (hanya ada 26 kunci). Teknik *Ceasar Cipher* tidak dapat menyembunyikan hubungan antara *plain text* dan *cipher text.* Pada teknik ini, huruf yang sering muncul di dalam *plain text* juga akan sering muncul di dalam *cipher text*. Hal ini menyebabkan teknik *Ceasar Cipher* mudah dipecahkan dengan *exhaustive key search.*

Oleh karena itu, muncul teknik kriptografi yang sempurna yaitu teknik *One-time Pad*. Pada teknik ini, menggunakan kunci yang benar-benar acak dan panjang kunci sama dengan panjang *plain text*, sehingga teknik ini sangat sulit untuk dipecahkan. Akan tetapi, pada teknik ini, muncul kesulitan karena panjang kuncinya yang harus sama panjang dengan *plain text* dan kuncinya harus benar-benar acak. Hal ini menyebabkan banyak orang lebih memilih menggunakan teknik *vigenere cipher*. Walupun teknik ini tidak sempurna seperti *One-time Pad*, namun kunci yang digunakan cukup pendek dan mudah diingat, sehingga tidak menimbulkan masalah dalam pembuatan, penyimpanan, maupun pendistribusian kunci tersebut seperti yang terjadi pada teknik *One-time Pad.*

Penulis melihat banyak dilemma yang terjadi yang dalam pemilihan teknik kriptografi yang akan digunakan. Oleh karena itu, penulis mencoba mengusulkan sebuah teknik kriptografi yang baru berdasarkan teknik *Ceasar Cipher*. Pada teknik yang baru ini penulis akan melakukan modifikasi teknik *Ceasar Cipher* dengan mengadopsi beberapa teknik kriptografi lain yang lebih baik seperti, *Vigenere Cipher* dan teknik *One-time Pad*. Dalam teknik ini, teknik *Ceasar Cipher* yang merupakan *cipher* abjad tunggal akan dimodifikasi menjadi Cipher abjad-majemuk. Tidak seperti teknik *Ceasar Cipher*, pada teknik ini, penulis akan menggunakan kunci untuk proses enkripsi dan dekripsinya. Dalam proses subtitusi huruf-huruf *plain text*-nya, penulis akan memanfaatkan barisan bilangan sebagai kuncinya. Kunci yang digunakan cukup mudah diingat, misalnya: barisan bilangan prima. Akan tetapi, kunci yang tercipta nantinya akan sama panjangan dengan *plain text*. Sehingga akan jauh lebih baik dari teknik *Caesar Cipher*, walupun tidak sampai sempurna seperti teknik *One-time Pad*.

***Kata kunci* :** *Caesar Cipher, Vigenere Cipher, One-time Pad*, barisan bilangan.

1. Pendahuluan

Sebelum komputer ada, kriptografi dilakukan dengan algoritma berbasis karakter. Algoritmam yang digunakan termasuk ke dalam sistem kriptografi sismetri dan digunakan jauh sebelum sistem kriptografi kunci publik ditemukan. Terdapat sejumlah algoritma yang tercatat dalam sejarah kriptografi sehingga dinamakan algoritma kriptografi klasik.

Salah satu algoritma kriptografi klasik yang terkenal adalah *Ceasar Cipher*. Algoritma ini sangat sederhana, sehingga algoritma ini sekarang dengan mudah dipecahkan.

Akan tetapi, *Ceasar Cipher* dapat menginspirasi terciptanya algoritma (teknik) lain dalam kriptografi. Salah satunya yaitu teknik yang dijelaskan dalam makalah ini.

Ceasar Cipher digunakan karena kepraktisannya, namun algoritma ini jadi sangat jarang digunakan lagi karena sangat buruk dari segi keamanannya. Agar algoritma ini tetap dapat digunakan, *Ceasar Cipher* perlu dimodifikasi.

2. Algoritma Kriptografi Klasik

Algoritma kriptografi klasik dibagi menjadi 2 jenis yaitu:

1. *Cipher* Substitusi (*Substitution Ciphers*)
2. *Cipher* Transposisi (*Transposition Ciphers*)

Pada makalah ini, akan dibahas mengenai *cipher* subtitusi. Berikut ini jenis-jenis *Cipher* Subtitusi.

1. Cipher abjad-tunggal (*monoalphabetic cipher*)
   Satu huruf di plainteks diganti dengan satu huruf yang bersesuaian

2. Cipher subtitusi homofonik (*Homophonic substitution cipher*)
   Setiap huruf plainteks dipetakan ke dalam salah satu huruf cipherteks yang mungkin. Tujuannya untuk menyembunyikan hubungan statistic antara plainteks dengan cipherteks

3. Cipher abjad-majemuk (*polyalphabetic cipher*)
   Satu kunci menggunakan kunci berbeda. Cipher abjad-majemuk dibuat dari sejumlah cipher abjad-tunggal, masing-masing dengan kunci yang berbeda. Kebanyakan cipher abjad-majemuk adalah cipher subtitusi periodic yang berdasarkan pada periode m.

4. Cipher subtitusi poligram (*Poligram substitution cipher*)
   Blok huruf plainteks disubtitusi dengna blok cipherteks. Tujuannya agar distribusi kemunculan poligram menjadi datar dan hal ini menyulitkan analisis frekuensi.

2.1 *Ceasar Cipher* dan analisisnya

Salah satu *cipher* subtitusi yang paling tua dan terkenal yaitu *Caesar Cipher*. *Caesar Cipher* termasuk ke dalam cipher subtitusi tunggal. Pada *Caesar Cipher*, tiap huruf alfabetdigeser 3 huruf ke kanan.

Tabel substitusi:

p_i :	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
c_i :	**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**

Contoh. Pesan

```
AWASI ASTERIX DAN TEMANNYA OBELIX
```

disamarkan (enskripsi) menjadi

```
DZDVL DVWHULA GDQ WHPDQQBA REHOLA
```

Penerima pesan men-dekripsi chiperteks dengan menggunakan tabel substitusi, sehingga chiperteks

```
DZDVL DVWHULA GDQ WHPDQQBA REHOLA
```

dapat dikembalikan menjadi plainteks semula:

```
AWASI ASTERIX DAN TEMANNYA OBELIX
```

Dengan mengkodekan setiap huruf abjad dengan *integer* sebagai berikut: $A = 0$, $B = 1$, …, $Z = 25$, maka secara matematis *caesar chiper* menyandikan plainteks p_i menjadi c_i dengan aturan:

$$c_i = E(p_i) = (p_i + 3) \bmod 26 \qquad (1)$$

dan dekripsi chiperteks c_i menjadi p_i dengan aturan:

$$p_i = D(c_i) = (c_i - 3) \bmod 26 \qquad (2)$$

Karena hanya ada 26 huruf abjad, maka pergeseran huruf yang mungkin dilakukan adalah dari 0 sampai 25. Secara umum, untuk pergeseran huruf sejauh k (dalam hal ini k adalah kunci enkripsi dan deksripsi), fungsi enkripsi adalah

$$c_i = E(p_i) = (p_i + k) \bmod 26 \qquad (3)$$

dan fungsi dekripsi adalah

$$p_i = D(c_i) = (c_i - k) \bmod 26 \qquad (4)$$

Kelemahan

Namun *Caesar Cipher* merupakan teknik kriptografi yang paling lemah. *Caesar Cipher* mudah dipecahkan dengan *exhaustive key search* karena jumlah kuncinya sangat sedikit (hanya 26 kunci).

2.2 *Unbreakable cipher*, keunggulan dan kelemahannya

Unbreakable cipher merupakan klaim yang dibuat oleh kriptografer terhadap algoritma kriptografi yang dirancangnya. Untuk merancang *unbreakable cipher*, ada dua syarat yang harus dipenuhi:

1. Kunci harus dipilih secara acak (yaitu, setiap kunci harus mempunyai peluang yang sama untuk terpilih).
2. Panjang kunci harus sama dengan panjang plainteks yang akan dienkripsikan.

Kedua syarat tersebut dapat menyebabkan *setiap* plainteks yang panjangnya sama akan sama-sama mempunyai kemungkinan menghasilkan cipherteks yang diberikan. Dengan kata lain, kriptanalis mendapatkan hasil bahwa cipherteks yang didekripsikannya menghasilkan beberapa plainteks yang mempunyai makna yang berbeda. Hal ini akan membingungkannya dalam menentukan plainteks yang benar.

Cipher yang tidak dapat dipecahkan dikatakan memiliki tingkat kerahasiaan yang sempurna (*perfect secrecy*). Satu-satunya algoritma kriptografi yang tidak dapat dipecahkan adalah *one-time pad*.

Kelemahan

Meskipun *one-time pad* merupakan *cipher* yang sempurna aman, namun faktanya ia tidak diguanakan secara universal dalam aplikasi kriptografi sebagai satu-satunya sistem *cipher* yang tidak dapat dipecahkan (hanya sedikit sistem komunikasi yang menggunakan *one-time pad*). Malahan orang masih tetap menggunakan sistem *cipher* yang dapat dipecahkan.

Alasannya adalah dari segi kepraktisan, yaitu:

1. Karena panjang kunci harus sama dengan panjang pesan, maka *one-time pad* hanya cocok untuk pesan berukuran kecil. Semakin besar ukuran pesan, semakin besar pula ukuran kunci. Pada aplikasi kriptografi untuk mengenkripsikan data tersimpan, timbul masalah lain dalam penyimpanan kunci.

2. Karena kunci dibangkitkan secara acak, maka 'tidak mungkin' pengirim dan penerima membangkitkan kunci yang sama secara simultan. Jadi, salah seorang dari mereka harus membangkitkan kunci lalu mengirimkannya ke pihak lain.

Mengirimkan barisan kunci melalui saluran komunikasi yang digunakan untuk pengiriman pesan juga tidak praktis karena pertimbangan lalu lintas (*traffic*) pesan yang padat. Oleh karena itu, *one-time pad* hanya dapat digunakan jika tersedia saluran komunikasi kedua yang cukup aman untuk mengirim kunci. Saluran kedua ini umumnya lambat dan mahal. Misalnya pada perang dingin antara AS dan Uni Soviet (dahulu), *one-time pad* dibangkitkan, disimpan, lalu dikirim dengan menggunakan jasa kurir yang aman. Penting diingat bahwa saluran kedua yang aman tersebut umumnya lambat dan mahal.

3. Barisan Bilangan

Barisan bilangan adalah jajaran bilangan yang dibentuk dari rumus tertentu. Notasi yang digunakan adalah U_n untuk suku ke-n. Contohnya: 1, 4, 9, 16, ... adalah barisan bilangan kuadrat dengan rumus $U_n = n_2$. Contoh lain: rumus U_n = 3n+4 akan membentuk barisan 7, 10,13, ...

4. Implementasi

Teknik kriptografi yang diharapkan adalah teknik kriptografi yang tidak dapat dipecahkan. Akan tetapi seperti yang telah dijelaskan di atas, teknik seperti itu sangatlah sulit untuk diimplementasikan karena tidak prakstis dan biayanya mahal. Oleh karena itu dibutuhkan suatu pendekatan di mana diciptakan suatu teknik dengan biaya yang murah dan praktis, namun memiliki kemampuan mendekati *Unbreakable cipher*. Dalam tulisan ini, penulis lebih menekankan terhadap kepraktisan dan biaya yang murah.

Teknik kriptografi yang paling praktis adalah *Ceasar Cipher*. Seperti yang telah dijelaskan sebelumnya, teknik ini sangatlah mudah untuk dipecahkan. Akan tetapi, kita dapat mengembangkan kepraktisan ini, menjadi satu teknik yang lebih baik lagi yang mendekati teknik *Unbreakable cipher*.

Teknik yang ditawarkan

Teknik *Ceasar Cipher* yang sebelumnya adalah cipher subtitusi abjad-tunggal dimodifikasi menjadi cipher subtitusi abjad-majemuk. Tidak seperti *Ceasar Cipher* yang sebenarnya, setiap huruf dalam alfabet akan dipetakan dengan beberapa huruf lain, sesuai dengan urutan kunci yang ada.

Kunci yang dipilih

Kunci yang digunakan adalah barisan bilangan. Hal ini dipilih karena setiap bilangan pada suatu barisan bilangan cenderung berbeda dan jumlahnya bisa mencapai tak terhingga atau bisa mencapai jumlah dari plainteks yang ada, contohnya pada barisan bilangan prima (2,3,5,…). Dengan begitu, kelemahan *Ceaser Cipher* mengenai masalah panjang kunci bisa diatasi. Setiap karakter dalam alfabetis tidak lagi disubtitusi dengan hanya satu karakter yang sama.

Barisan bilangan yang dipilih sebagai kunci merupakan barisan bilangan yang anggotanya(bilangan-bilangan dalam barisan tersebut) adalah bilanga bulat, misalnya barisan bilangan asli, barisan bilangan prima, barisan bilangan fibonacci, dan sebagainya, atau dapat juga barisan tersebut didefinisikan sendiri oleh pembuat proses enkripsi dan dekripsinya.

Dengan kunci yang bisa mencapai panjang plainteks dan setiap kunci bisa berbeda, teknik ini akan semakin dekat dengan teknik *Unbreakable cipher*.

Proses subtitusi yang dilakukan adalah menambahkan karakter plainteks dengan kunci yang ada, sehingga dihasilkan karakter cipherteks.
Misalnya untuk karakter 'A', dengan kunci barisan bilangan prima,

Pada urutan pertama
A = 0
Kunci[1] = 2
Karakter cipherteks yang bersesuaian
= 0 + 2 = 3 = C

Tabel subtitusi selengkapnya dari karakter ‘A’ :

urutan	1	2	3	4	5	6	7	8	9
kunci	2	3	5	7	11	13	17	19	23
cipher	C	D	F	H	L	N	R	T	X

Urutan menunjukan pada urutan ke berapa karakter ‘A’, misalnya pada string “SAYA”, karakter ‘A’ yang pertama berada di urutan ke-2 sehingga disubtitusi dengan karakter ‘D’dan karakter ‘A’ yang kedua berada di urutan ke-4 sehingga disubtitusi dengan karakter ‘H’.

Tabel subtitusi untuk beberapa karakter lain dengan kunci barisan bilangan prima.

		huruf							
		A	B	C	D	E	F	G	….
urutan	1	C	D	E	F	G	H	I	
	2	D	E	F	G	H	I	J	
	3	F	G	H	I	J	K	L	
	4	H	I	J	K	L	M	N	
	5	L	M	N	O	P	Q	R	
	6	N	O	P	Q	R	S	T	
	….								

4.1 Algoritma Enkripsi

Secara umum proses enkripsi yaitu :

$$c[i] = (p[i] + k[i]) \bmod 25$$

di mana:

c[i] adalah karakter dari cipherteks ke-i yang dihasilkan
p[i] adalah karakter dari plainteks ke-i
k[i] adalah kunci ke-i

4.2 Algoritma Dekripsi

Secara umum proses dekripsi yaitu:

$$p[i] = (c[i] - k[i]) \bmod 25$$

di mana:

p[i] adalah karakter dari plainteks ke-i yang dicoba dipecahkan
c[i] adalah karakter dari cipherteks ke-i
k[i] adalah kunci ke-i

Kelemahan

Diluar faktor keamanan, teknik ini memiliki kelemahan, jika barisan bilangan yang digunakan sebagai kunci memiliki nilai yang cukup besar, sehingga dalam diimplementasinya kunci akan sulit dibangkitkan dan disimpan.

Contohnya:

Barisan bilangan yang digunakan adalah barisan bilangan “n pangkat n”,
Hanya untuk n ke-10 nilainya sudah mencapai 10.000.000.000.

Variasi Kunci

Variasi kunci dibutuhkan untuk menangani masalah yang timbul di atas. Salah satu variasi kunci yang mungkin dibuat adalah dengan melakukan perulangan kunci, misalnya jika pada kunci ke-n nilainya sudah mencapai 10.000.000.000, maka kunci selanjutnya akan diulangi dari n ke-1 lagi.

Ada variasi kunci yang lain, tetapi bukan untuk menangani masalah di atas. Variasi kunci digunakan untuk memperkuat enkripsi data. Misalnya kunci berupa barisan bilangan prima, namun tidak dimulai dengan n = 1, tetapi misalnya kunci di mulai dari n=10. Atau misalnya kunci menggunakan barisan bilangan fibonacci dengan bilangan pertama adalah 4 dan bilangan ke-2 adalah 10, sehingga dihasilkan barisan fibonacci yang berbeda dari biasanya.

Keamanan

Jika kunci tidak mengalami perulangan seperti yang dijelaskan di atas, teknik ini cukup sulit untuk dipecahkan dengan cara *known-plaintext attack*. Cara *chipertext-only attack* juga sulit dilakukan selama pola kunci tidak diketahui.

Namun, jika mengalami perulangan kelemahan teknik ini akan sama dengan yang terjadi pada teknik *vigenere cipher*. Akan tetapi, kriptanalis akan lebih sulit untuk memecahkannya karena kunci bukan berupa string yang biasanya dipakai dalam teknik *vigenere cipher*.

Keamanan dapat ditingkatkan dengan mensubtitusikan tidak hanya karakter huruf, tetapi juga karakter-karakter lain. Oleh karena itu, rumus enkripsi berubah menjadi

$$c[i] = (p[i] + k[i]) \bmod 255$$

dan dekripsi menjadi

$$p[i] = (c[i] - k[i]) \bmod 255$$

Nilai 255 merupakan jumlah semua karakter yang ada yaitu 256 (2^8)

Pengiriman Kunci

Kesulitan yang muncul jika panjang kunci sama dengan panjang plainteks adalah pendistribusian kunci. Dengan menggunakan kunci berupa barisan bilangan, kunci tidak perlu dikirim semuanya, hanya perlu dikirimkan petunjuk dari kunci tersebut, misalnya: yang dikirimkan hanya berupa string “prima”, artinya kunci yang dipakai adalah barisan bilangan prima.

5. Pengujian

Untuk pengujian dilakukan mengunakan file teks yang isinya tidak terlalu panjang

1. Enkripsi skenario normal

Pesan :
ARI WARDANA

Kunci barisan prima :
2,3,5,7,11,13,17,…

Hasil :
CUM ELFUTLD

Hasil diperbaiki menjadi:
CUME LFUT LD

2. Dekripsi skenario normal

Pesan :
CUME LFUT LD

Kunci barisan prima :
2,3,5,7,11,13,17,…

Hasil:
ARIW ARDA NA

Hasil setelah diperbaiki:
ARI WARDANA

3. Enkripsi skenario normal dengan kunci yang lain

Pesan :
ARI WARDANA

Kunci barisan prima :
1,1,2,3,5,8,….

Hasil :
BSK ZFZQVVF

Hasil diperbaiki menjadi:
BSKZ FZQV VF

4. Dekripsi skenario normal dengan kunci yang lain

Pesan :
BSKZ FZQV VF

Kunci barisan prima :
1,1,2,3,5,8,….

Hasil :
ARIW ARDA NA

Hasil diperbaiki menjadi:
ARI WARDANA

5. Enkripsi dengan kunci barisan bilangan 0

Pesan :
ARI WARDANA

Kunci:
0,0,0,0,…..

Hasil :
ARI WARDANA

Hasil yang diperoleh sama seperti pesan yang dienkripsi.

6. Enkripsi dengan kunci barisan bilangan 3

Pesan :
ARI WARDANA

Kunci:
3,3,3,3,…..

Hasil :
DUL ZDUGDQD

Hasil setelah diperbaiki:
DULZ DUGD QD

Dengan kunci seperti ini hasilnya sama dengan jika menggunakan *Ceasar Cipher* biasa.

7. Dekripsi dengan kunci yang salah

Pesan :
CUME LFUT LD

Kunci seharusnya barisan prima.
Kunci yang digunakan :
3,3,3,….

Hasil:
FXPH OIXW OG

6. Kesimpulan

Ceaser Cipher merupakan algoritma (tekink) kiptografi yang mudah dipecahkan oleh kriptanalis. Namun dengan sedikit modifikasi algoritma *Ceaser Cipher* bisa menjadi lebih kuat dan tahan terhadap gangguan kriptanalis.

Modifikasi *Ceasar Cipher* menjadi Cipher abjad-majemuk dan menambahkan kunci berupa barisan bilangan membuat proses kriptografi menjadi lebih baik dan mendekati *Unbreakable cipher*.

Daftar Pustaka

[1] Munir, Rinaldi. *Kriptografi*, Penerbit Informatika, 2006.

[2] Purcell, Edwin J. dan Dale Varberg. *Kalkulus dan Geometri Analisis*. Penerbit: Penerbit Erlangga, 1987

Lampiran

Program kecil untuk permasalahan di atas dapat diunduh di:

http://students.itb.ac.id/~a121_w/kriptografi