Subtitusi Abjad

Sindhu Rakasiwi, M.Kom

Objectives

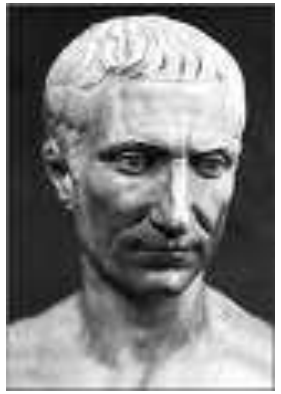
- Mahasiswa mendapatkan penjelasan mengenai pengenalan kriptografi klasik
- Mahasiswa mendapatkan penjelasan mengenai macam-macam teknik subtitusi
  - Cipher abjad-tunggal (monoalphabetic cipher)
  - Cipher substitusi homofonik (Homophonic substitution cipher)
  - Cipher abjad-majemuk (Polyalpabetic substitution cipher)
  - Cipher substitusi poligram (Polygram substitution cipher)

Pengantar

- Algoritma kriptografi klasik berbasis karakter
- Menggunakan pena dan kertas saja, belum ada komputer
- Termasuk ke dalam kriptografi kunci-simetri
- Tiga alasan mempelajari algoritma klasik:
  - 1. Memahami konsep dasar kriptografi.
  - 2. Dasar algoritma kriptografi modern.
  - 3. Memahami kelemahan sistem *cipher*.

Cipher Substitusi

- Caesar Cipher
  - Kriptografi Simetris
  - Merupakan metode enkripsi yang dilakukan pada zaman Julius Caesar.
  - Hanya dipergunakan pada Alfabet baik huruf kapital maupun huruf kecil. Sehingga ketika proses yang dilakukan pada angka maka hal tersebut tidak dapat dilakukan.



Contoh

- Sebuah Chiperteks berbunyi: PWNUYTLWFKN
- Algoritma Caesar Chiper kunci: 5
- Plainteks: ?
- Jawab:

Chipertext	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
Plaintext	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

Contoh

Chiperteks: **PWNUYTLWFKN**

Kunci : Geser 5 huruf

Dari peta huruf di atas, maka

P	→	K
W	→	R
N	→	I
U	→	P
Y	→	T
T	→	O
L	→	G
W	→	R
F	→	A
K	→	F
N	→	I

Plainteks : **KRIPTOGRAFI**

Jenis-jenis Cipher Substitusi

1. Cipher abjad-tunggal (monoalphabetic cipher)
2. Cipher substitusi homofonik (Homophonic substitution cipher)
3. Cipher abjad-majemuk (Polyalpabetic substitution cipher)
4. Cipher substitusi poligram (Polygram substitution cipher)

Cipher Abjad-tunggal (Monoalphabetic Cipher)

- Monoalphabetic cipher (Cipher abjad tunggal) adalah enkripsi metode subtitusi yang memetakan tiap-tiap abjad dengan abjad lain secara random, bukan metode pergeseran seperti Caesar cipher.
- Jumlah kemungkinan susunan huruf-huruf cipherteks yang dapat dibuat pada sembarang cipher abjad-tunggal adalah sebanyak

26! = 403.291.461.126.605.635.584.000.000

Cipher Abjad-tunggal (Monoalphabetic Cipher)

- Tabel substitusi dapat dibentuk secara acak

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

- Atau dengan kalimat yang mudah diingat:

  Contoh: `we hope you enjoy this book`

- Buang duplikasi huruf: `wehopyunjtisbk`
- Sambung dengan huruf lain yang belum ada:

  `wehopyunjtisbkacdfglmqrvxz`

- Tabel substitusi:

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

Cipher Substitusi Homofonik (Homophonic substitution cipher)

- Setiap huruf plainteks dipetakan ke dalam salah satu huruf atau pasangan huruf cipherteks yang mungkin.
- Tujuan: menyembunyikan hubungan statistik antara plainteks dengan cipherteks
- Fungsi ciphering memetakan satu-ke-banyak (one-to-many).

Cipher Substitusi Homofonik (Homophonic substitution cipher)

Huruf Plainteks	Pilihan untuk unit cipherteks												
A	BU	CP	AV	AH	BT	BS	CQ						
B	AT												
C	DL	BK	AU										
D	BV	DY	DM	AI									
E	DK	CO	AW	BL	AA	CR	BM	CS	AF	AG	BO	BN	BE
F	BW	CM	CN										
G	DN	BJ											
H	AS	CL	CK										
I	DJ	BI	AX	CJ	AB	BP	CU	CT					
J	BX												
K	DI												
L	AR	BH	CI	AJ									
M	DH	BG	AY										
N	BY	DG	DF	CH	AC	BR	DU	DT					
O	DZ	BF	DX	AK	CG	BQ	DR						
P	BZ	DE	AZ										
Q	DD												
R	AQ	DC	DQ	AL	CE	CF	CV	DS					
S	AP	AN	AO	CD	DW	DV							
T	CB	DB	DP	CC	AD	CY	CW	CX	AE				
U	CA	AM	BA										
V	BB												
W	CZ												
X	BD												
Y	DO	DA											
Z	BC												

Cipher Substitusi Homofonik (Homophonic substitution cipher)

- Unit cipherteks mana yang dipilih diantara semua homofon ditentukan secara acak.
- Contoh:

  Plainteks: `KRIPTO`

  Cipherteks: **`DI CE AX AZ CC DX`**

- Enkripsi: satu-ke-banyak
- Dekripsi: satu-ke-satu
- Dekripsi menggunakan tabel homofon yang sama.

Cipher Abjad-Majemuk (Polyalpabetic substitution cipher)

- Cipher abjad-tunggal: satu kunci untuk semua huruf plainteks
- Cipher abjad-majemuk: setiap huruf menggunakan kunci berbeda.
- Cipher abjad-majemuk dibuat dari sejumlah cipher abjad-tunggal, masing-masing dengan kunci yang berbeda.
- Contoh: Vigenere Cipher (akan dijelaskan pada kuliah selanjutnya)

Cipher Abjad-Majemuk (Polyalpabetic substitution cipher)

- Contoh: (spasi dibuang)

  P = KRIPTOGRAFIKLASIKDENGANCIPHERALFABETMAJEMUK

  K = LAMPIONLAMPIONLAMPIONLAMPIONLAMPIONLAMPIONL

  C = VRUEBCTCARXSZNDIWSMBTLNOXXVRCAXUIPREMMYMAHV

- Perhitungan:

  (K + L) mod 26 = (10 + 11) mod 26 = 21 = V

  (R + A) mod 26 = (17 + 0) mod 26 = 17 = R

  (I + M) mod 26 = (8 + 12) mod 26 = 20 = U

  dst

- Contoh 2: (dengan spasi)

  P = SHE SELLS SEA SHELLS BY THE SEASHORE

  K = KEY KEYKE YKE YKEYKE YK EYK EYKEYKEY

  C = CLC CIJVW QOE QRIJVW ZI XFO WCKWFYVC

Cipher substitusi poligram (Polygram substitution cipher)

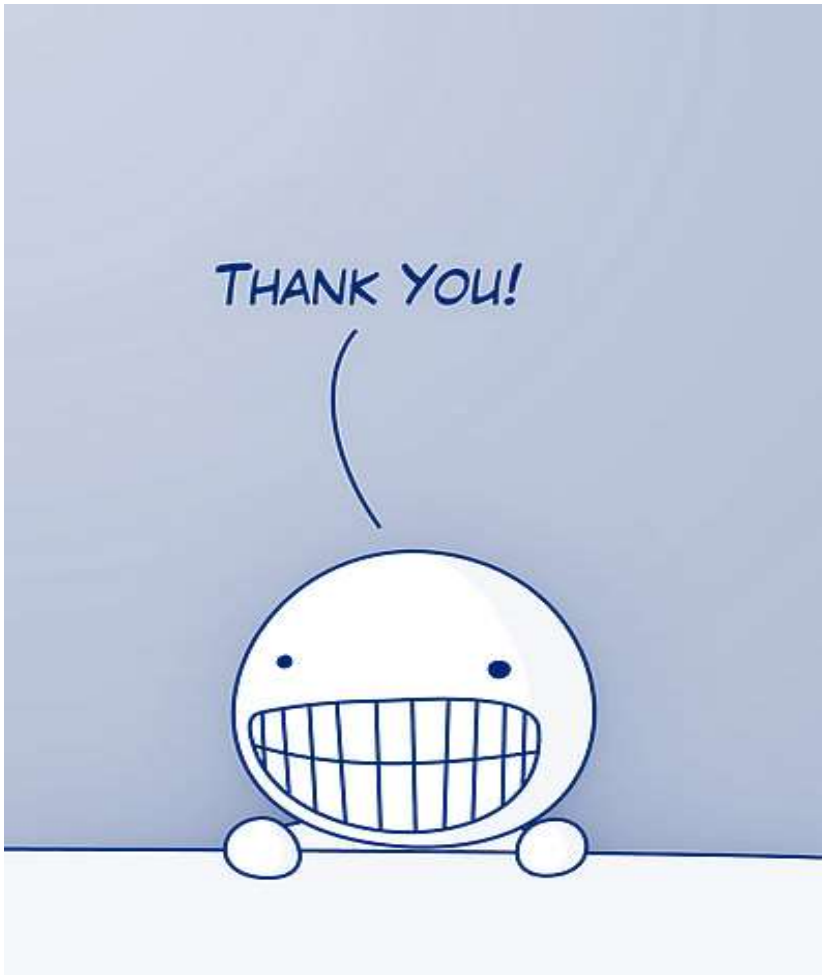
- Blok huruf plainteks disubstitusi dengan blok cipherteks.
- Misalnya `AS` diganti dengan `RT`, `BY` diganti dengan `SL`
- Jika unit huruf plainteks/cipherteks panjangnya 2 huruf, maka ia disebut digram (biigram), jika 3 huruf disebut ternari-gram, dst
- Tujuannya: distribusi kemunculan poligram menjadi flat (datar), dan hal ini menyulitkan analisis frekuensi.
- Contoh: Playfair cipher (akan dijelaskan pada kuliah selanjutnya)

Sumber

- Rinaldi Munir, ITB
- Aisyatul Karima, UDINUS
- Bruce Scheier, (2001), Applied Cryptography, John Willey & Sons Inc, Canada
- Cobb, Chey, (2004), Cryptography for Dummies, John Willey & Sons Inc, Canada
- Stalling William, (2003), Cryptography and Network Security, Prentice Hall, USA

QUIZ

- 1. Plainteks : Nama panjang mahasiswa (point 30)
  - Algoritma Caesar Chiper kunci: 4
  - Chiperteks?
- 2. Plainteks : Belajar (point 30)
  - Algoritma Cipher Substitusi Homofonik
  - Chiperteks?
- 3. Plainteks : Saya suka belajar kriptografi dengan menggunakan Algoritma Cipher Abjad Majemuk (point 40)
  - Algoritma Cipher Abjad Majemuk
  - Kunci : Semangat
  - Chiperteks ?


THANK YOU!