Keamanan Sistem Komputer

kρυπτο γραφη

Kriptologi

- Ilmu yang mempelajari tentang menyembunyikan.
- Cruptos (= hidden) & Logos (=study, science)
- Kriptologi mempelajari metode enkripsi dan dekripsi pesan atau sinyal
- Kriptologi terbagi menjadi 2 area :
  - Kriptografi
  - Kriptoanalisis

Kriptografi & Kriptoanalisis

- Kriptografi dapat lebih dispesifikkan sebagai ilmu yang mempelajari teknik penyembunyian pesan atau data dengan sebuah kunci rahasia. Hanya orang yang memiliki hak yang dapat melakukan dekripsi dari pesan tersebut.

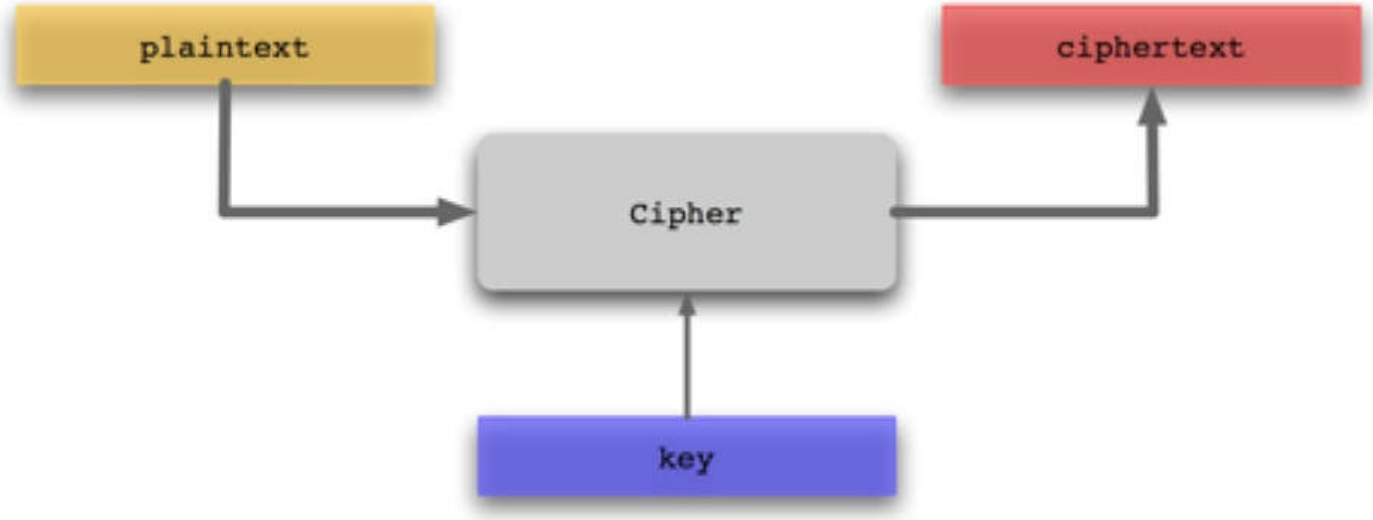
Kriptografi & Kriptoanalisis

- Kriptoanalisis merupakan teknik yang mempelajari dekripsi sebuah data rahasia tanpa mengetahui kunci yang digunakan. Atau sering disebut juga teknik **hacking/cracking**

Kriptografi

- Terdiri dari :
  - Kerahasiaan (Confidentiality)
    - Mencegah penyadapan data
  - Keutuhan (Integrity)
    - Menjamin data tidak diubah
  - Autentifikasi
    - Memeriksa pesan dikirim oleh orang yang benar
  - Non-repudiation
    - Meyakinkan pihak ke-3 akurasi dari pesan

Terminologi



Terminologi

- Cryptographer
  - Menemukan sistem kripto
- Cryptanalyst
  - Memecahkan sistem kripto
- Cryptology
  - Ilmu tentang sistem kripto
- Cipher
  - Cara menenkripsi teks
- Code
  - Terjemahan semantik: “burung” = “pesawat terbang”, “elang”=“pesawat tempur”, “lemper”=“terpedo” dll

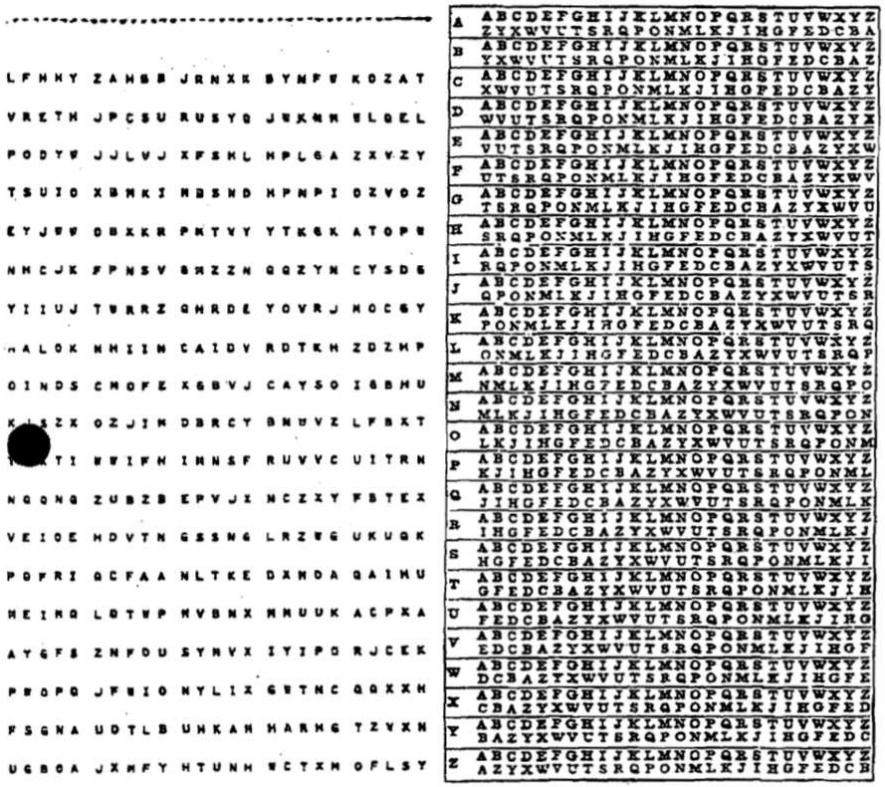
Jenis-jenis Analisis Kripto

- **Tujuan** : mendapatkan kunci (& algoritma)

Jenis Serangan	Yang Diketahui Cryptanalust
Ciphertext only (hanya tau kode rahasianya)	Algoritma Enkripsi Ciphertext yang akan dibaca
Known plaintext (mengetahui plaintext tertentu)	Algoritma Enkripsi Ciphertext yang akan dibaca Sepasang/lebih plaintext – ciphertext yang disusun dengan kunci rahasia tertentu
Chosen plaintext (dapat memilih plaintext)	Algoritma Enkripsi Ciphertext yang akan dibaca Plaintext yang dipilih cryptanalyst, bersama dengan ciphertext pasangannya yang dibangkitkan dengan kunci rahasia tertentu

Jenis Serangan	Yang Diketahui Cryptanalust
Adaptive chosen plaintext attack	Algoritma Enkripsi Ciphertext yang akan dibaca Plaintext dapat dipilih lebih khusus oleh cryptanalyst
Chosen ciphertext (dapat memilih ciphertext tertentu yang diinginkan)	Algoritma Enkripsi Ciphertext yang akan dibaca Ciphertext yang isi pokoknya diketahui, dipilih oleh cryptanalyst, bersama dengan plaintext (terdekrip) pasangannya yang dibangkitkan dengan kunci tertentu
Chosen text	Algoritma Enkripsi Ciphertext yang akan dibaca Plaintext yang dipilih cryptanalyst, bersama dengan ciphertext pasangannya yang dibangkitkan dengan kunci rahasia tertentu Ciphertext yang isi pokoknya diketahui, dipilih oleh cryptanalyst, bersama dengan plaintext (terdekrip) pasangannya yang dibangkitkan dengan kunci tertentu

One Time Pads



- OTP merupakan teknik enkripsi yang tidak dapat dipecahkan jika digunakan dengan cara yang salah
- Contoh OTP yang digunakan di NSA coded name DIANA, digunakan untuk converting plain text menjadi cipher text

OTP Example

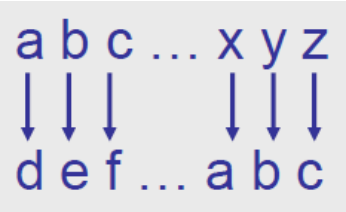
```
      H       E       L       L       O  message
    7 (H)   4 (E)  11 (L)  11 (L)  14 (O) message
+  23 (X)  12 (M)   2 (C)  10 (K)  11 (L) key
=  30      16      13      21      25     message + key
=   4 (E)  16 (Q)  13 (N)  21 (V)  25 (Z) (message + key) mod 26
       E       Q       N       V       Z  → ciphertext
```

```
       E       Q       N       V       Z  ciphertext
     4 (E)  16 (Q)  13 (N)  21 (V)  25 (Z) ciphertext
-   23 (X)  12 (M)   2 (C)  10 (K)  11 (L) key
= -19       4       11      11      14     ciphertext - key
=    7 (H)   4 (E)  11 (L)  11 (L)  14 (O) ciphertext - key (mod 26)
       H       E       L       L       O  → message
```

Model enkripsi seperti ini banyak ditemukan pada metode algoritma enkripsi monoalphabetik dan polyalphabetik

Caesar Cipher

- Digunakan Julius Caesar (sekitar 75 BC)
  - Tambah 3 mod 26 (geser 3)

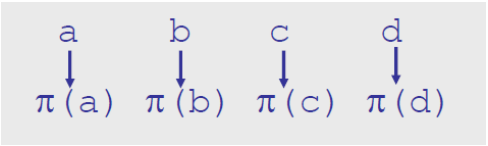


- Kelebihan?
  - Sederhana, digunakan di medan perang, sebagian besar orang pada zaman itu buta huruf
- Kekurangan?
  - Keamanan mengandalkan penyamaran, mudah untuk dipecahkan

Cipher Monoalphabetik

- a.k.a cipher subtitusi

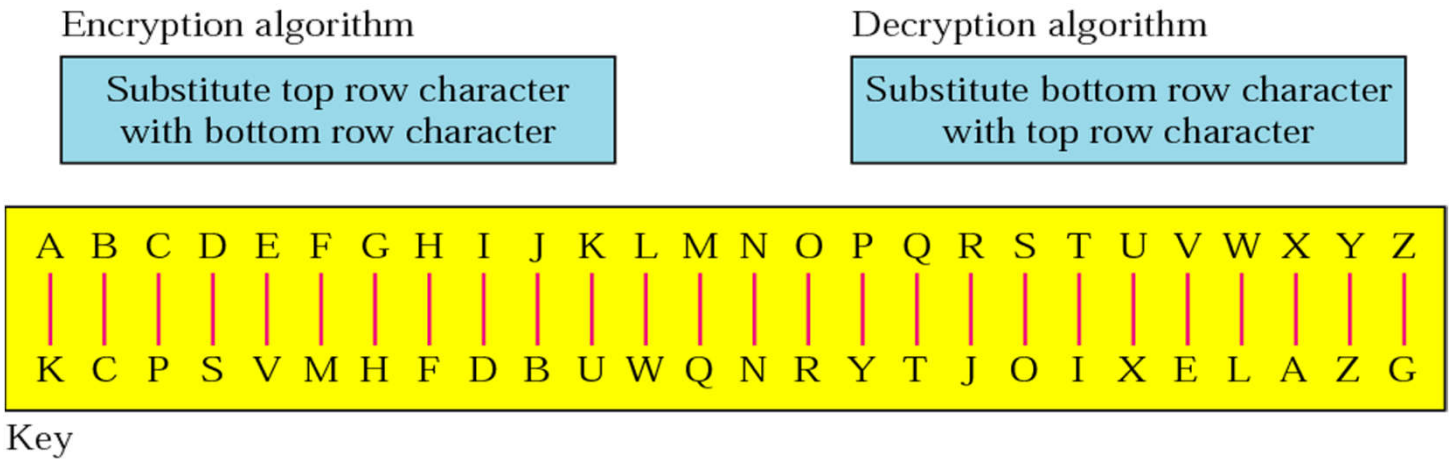
- Cipher monoalphabetik umum
  - Melakukan permutasi dari alphabet
  - Kuncinya di permutasi



- 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. Misal A -> D, B -> I, C -> Q dan seterusnya.

Subtitusi Monoalphabetik

- Plain Text : TELKOM UNIVERSITY
- Cipher Text : IVWURQ XNDEVJODIZ



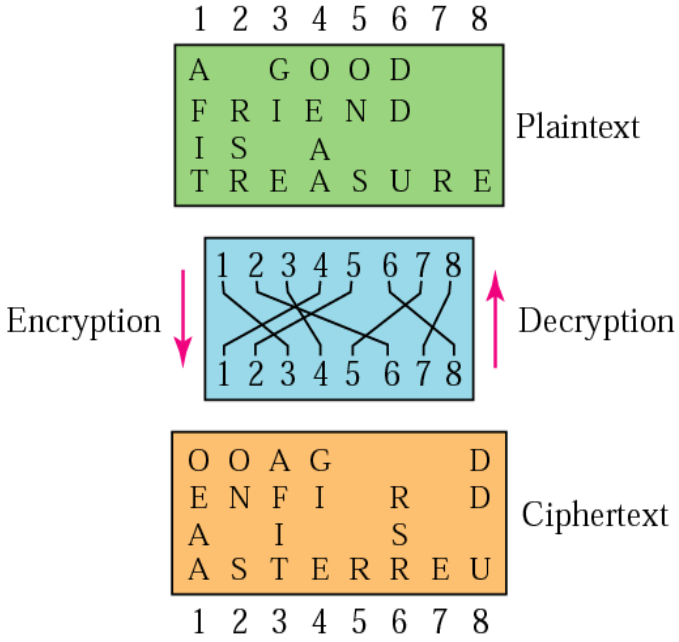
Jogja Cipher

Ha	-----	Pa
Na	-----	Dha
Ca	-----	Ja
Ra	-----	Ya
Ka	-----	Nya
Da	-----	Ma
Ta	-----	Ga
Sa	-----	Ba
Wa	-----	Tha
La	-----	Nga

Jogja Cipher

- DAGADU
- MOTHIG
- DHEPOYAPIBOPOYAHOHO

Cipher Transposisional



- Digunakan pada PD II oleh Jerman dalam mesin Enigma, hanya di Enigma transposisi dilakukan 6 kali dengan 3 mesin rotor

Rail Fence Algorithm

- Plain Text
  - WE ARE DISCOVERED. FLEE AT ONCE

W . . . E . . . C . . . R . . . L . . . T . . . E

. E . R . D . S . O . E . E . F . E . A . O . C .

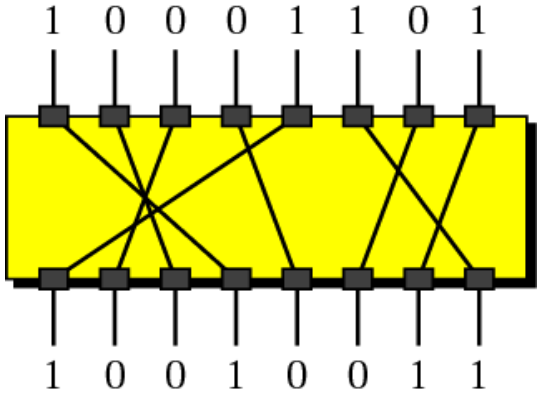
. . A . . . I . . . V . . . D . . . E . . . N . .

- Cipher Text
  - WECRL TEERD SOEEF EAOCA IVDEN

Malang Cipher

- Kera ngalam ----- Arek Malang
- Bojo ----- Ojob
- Mulih ----- Hilum

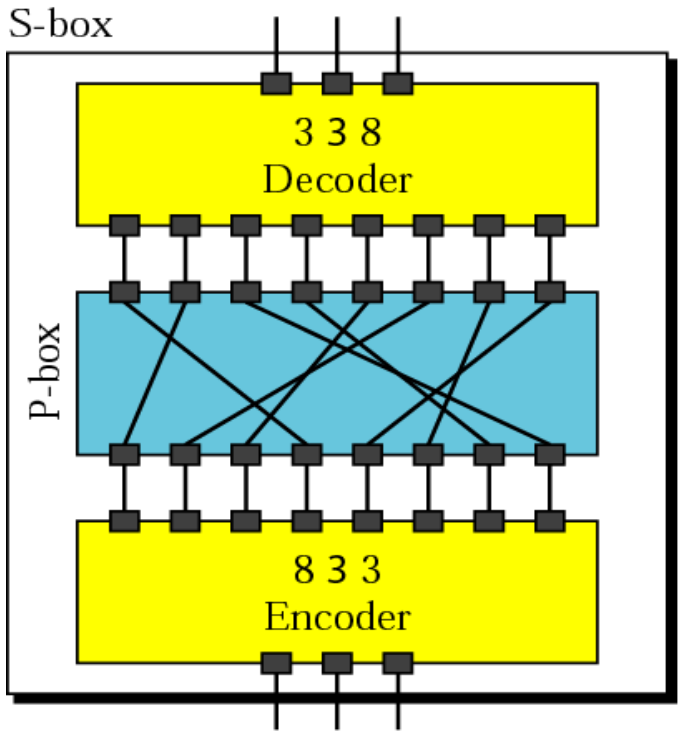
P-Box



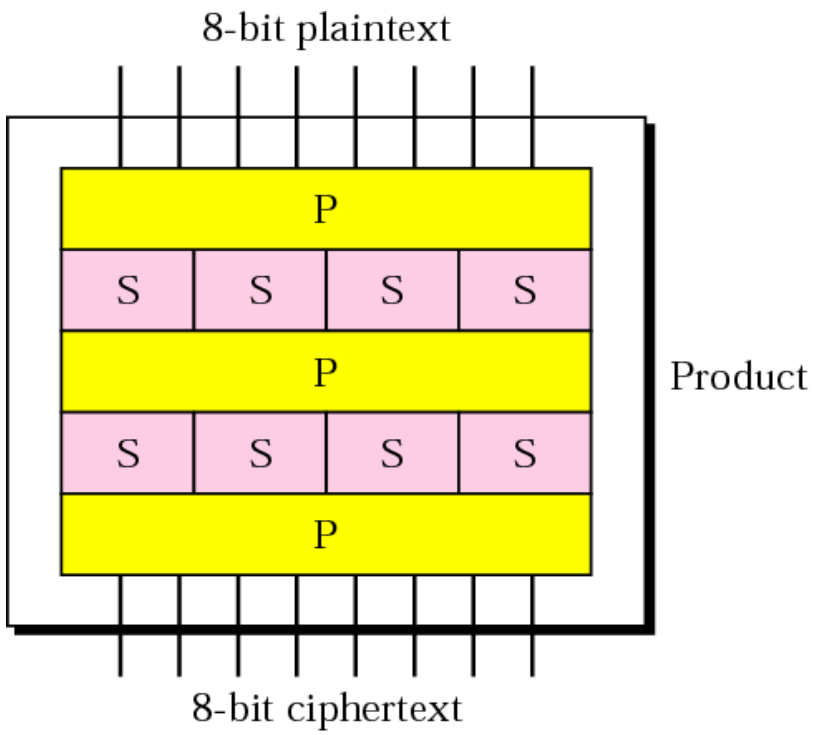
- Permutation Box
- Merupakan hardware yang digunakan untuk menukarkan posisi bit dalam karakter ASCII, sehingga jika dibaca langsung pada output tidak akan membentuk karater yang sesungguhnya
- 1 = 31h menggunakan P-box diatas menjadi 4Ah = J
- Penggunaan P-box hanya satu arah, berarti proses dekripsi harus menggunakan p-box mirrornya

S-Box

- Subtitution Box
- Penggunaan P-box bisa dikembangkan lebih jauh menjadi S-box
- Misal dalam gambar di kanan
  - Input **001** akan menyebabkan output **010**
  - Input **111** akan menyebabkan output **100**



Product Block



- Produk blok akan menenkrip dan mendekrip karakter plainteks menjadi cipherteks
- Setiap S-blox yang digunakan boleh tidak sama, yang akan menyebabkan proses semakin kompleks

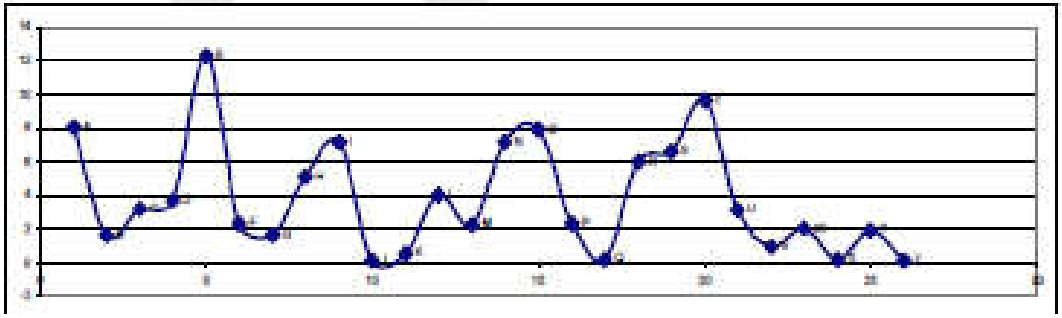
Analisis Kripto Monoalphabetik

- Serangan “brute force” : coba setiap kunci
  - N! kemungkinan permutasi untuk N huruf alphabet
    - $26! \approx 4 \times 10^{28}$ kemungkinan kunci
    - Jika 1 percobaan : 1 us → 10 triliun tahun
    - Coba baca novel Dan Brown “Digital Fortress”

- Tapi ada cara serangan yang lebih cerdas sehingga tidak perlu selama itu
  - Pengamatan pemetaan satu huruf ke satu huruf lain tidak bagus
  - Distrbusi frekuensi huruf umum tetap

Urutan & Frekuensi Huruf Bahasa Inggris

E	12.31%	L	4.03%	B	1.62%
T	9.59	D	3.65	G	1.61
A	8.05	C	3.20	V	0.93
O	7.94	U	3.10	K	0.52
N	7.19	P	2.29	Q	0.20
I	7.18	F	2.28	X	0.20
S	6.59	M	2.25	J	0.10
R	6.03	W	2.03	Z	0.09
H	5.14	Y	1.88		



Analisis Kripto Monoalphabetik

- Hitung frekuensi setiap huruf di ciphertext
- Cocokan dengan statistik huruf Inggris
  - Huruf yang paling sering keluar kemungkinan besar huruf “e”
  - Kedua tersering kemungkinan “t”
  - Dst

- Ciphertext yang lebih panjang membuat teknik ini lebih mungkin berhasil

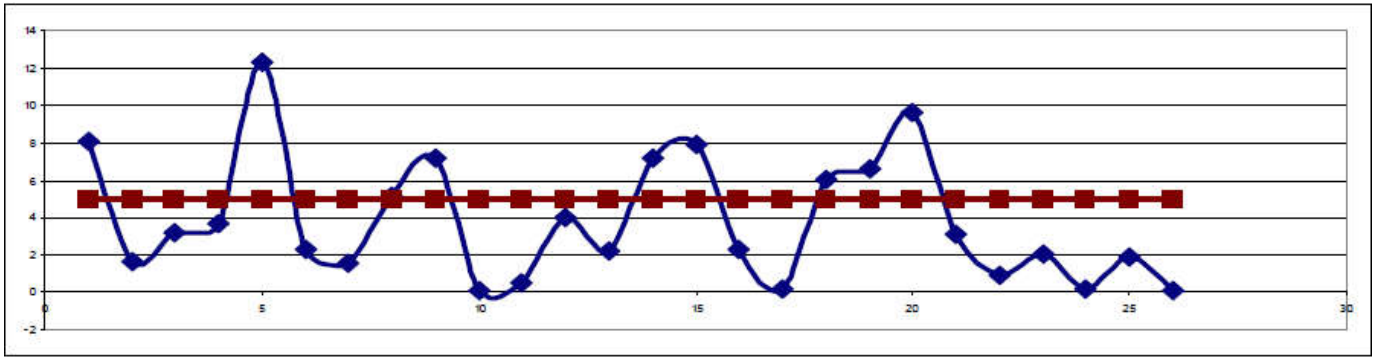
Diagram & Trigram

- Urutan frekuensi diagram
  - TH HE AN IN ER RE ES ON EA TI AT ST EN ND OR

- Urutan frekuensi trigram
  - THE AND THA ENT ION TIO FOR NDE HAS NCE EDT TIS OFT STH MEN

Statistik Yang Diinginkan

- Masalah di cipher monoalphabetik
  - Frekuensi huruf di ciphertext menyatakan frekuensi dari plaintext
- Diinginkan pemetaan satu huruf plaintext ke banyak huruf ciphertext
  - e → x, c, w dst
- Idealnya frekuensi ciphertext ‘rata’



Subtitusi Polyalphabetik

- Ambil k cipher subtitusi
  - 1, 2, 3 … k
- Enkripsi pesan secara berputar melalui k subtitusi

m	e	s	s	a	g	e
$\pi_1(m)$	$\pi_2(e)$	$\pi_3(s)$	$\pi_4(s)$	$\pi_1(a)$	$\pi_2(g)$	$\pi_3(e)$
q	a	x	o	a	u	v

- Huruf yang sama dipetakan ke berbagai huruf ciphertext
  - Meratakan distribusi frekuensi
  - Diffusi

Tabel Vigenere

- Subtitusi Jamak
  - Bisa memilih cipher “complementer” sehingga distribusi frekuensi bisa lebih rata
  - Umum : lebih banyak subtitusi berarti distrbusi lebih rata
- Tabel Vigenere
  - Ditemukan oleh Blaise de Vigenere untuk Henry III raja Prancis sekitar th 1500
  - Kumpulan dari 26 permutasi
  - Biasanya berupa grid 26 x 26
  - Kuncinya sebuah kata

Vigenere

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
0	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
1	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
2	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
3	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
4	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
5	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
6	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
7	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
8	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
9	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
10	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
11	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
12	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
13	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
14	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
15	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
16	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
17	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
18	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
19	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
20	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
21	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
22	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
23	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
24	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
25	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

Enkripsi

1. Buat keyword secara berulang sepanjang plainteks
2. Cari huruf pada tabel yang sesuai dengan kombinasi nomor baris huruf key dan nomor kolom huruf plainteks
3. Secara matematik:

Cipher = plain+key mod 26

Dekripsi

1. Cara huruf pada tabel yang sesuai dengan kombinasi nomor baris huruf key dan nomor kolom huruf cipher
2. Secara matematik

plain = cipher – key mod 26

Plaintext : a bad deed
Kunci ‘bed’ ; B EDB EDBE
Cipertext ; b fde hgfh

Kelemahan Subtitusi Polyalphabetik

- Masalah
  - Jika pola terjadi k kali dan panjang kunci n maka akan dikodekan k/n kali oleh kunci yang sama
- Contoh
  - Plaintext: theboyhasthebag
  - Kunci ‘big’: BIGBIGBIGBIGBIG
  - Ciphertext: OPKWWECIYOPKWIM

- Telihat bahwa OPK terjadi 2 kali, dan berjarak kelipatan kunci (9)

Playfair Cipher

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

- Menggunakan tabel 5x5 yang berisikan alphabet yang akan diisikan dengan kunci
- Memisahkan plaintext menjadi digraf (2 huruf)
- “Hello World” → “HE LL OW OR LD”
- Memiliki 4 aturan utama

Aturan Playfair Cipher

1. Jika terdapat 2 buah huruf yang sama atau sisa 1 huruf, huruf pertama akan diberikan huruf “X” sebagai huruf tambahan
2. Jika terdapat huruf-huruf yang berada pada 1 baris pada tabel, maka subtitusikan dengan huruf-huruf yang berada di sebelah kanan huruf tersebut (wrap ke kiri jika dibutuhkan)
3. Jika terdapat huruf-huruf yang berada pada 1 kolom pada tabel, maka subtitusikan dengan huruf yang berada pada bawah dari huruf tersebut (wrap ke atas jika dibutuhkan
4. Jika terdapat huruf yang berada pada baris dan kolom yang berbeda, subtitusikan dengan huruf yang berada pada baris yang sama dan memiliki posisi kolom yang sama dengan huruf yang lain

Playfair Cipher

- Kunci : PLAYFAIREXAMPLE
- Plain teks : Hide the gold in the tree stump

- Diagraf :

HI DE TH EG OL DI NT HE TR EE ST UM P

HI DE TH EG OL DI NT HE TR EX ES TU MP

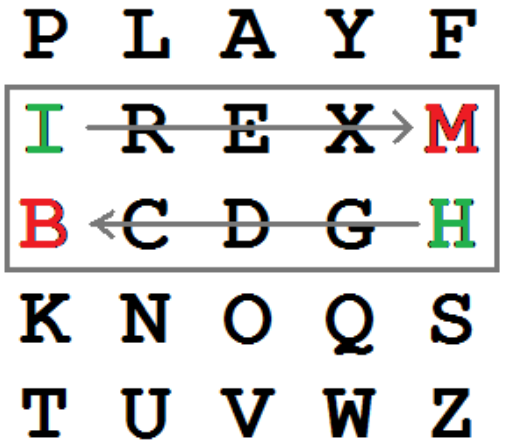
Playfair Cipher Key : “PLAYFAIREXAMPLE”

P	L	A	Y	F a
I	R	E	X a	M ple a
B	C	D ef	G	H i=j
K lm	N	O p	Q r	S
T	U	V	W xy	Z

Playfair Cipher Key : “PLAYFAIREXAMPLE”

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

Playfair Cipher : “HI”

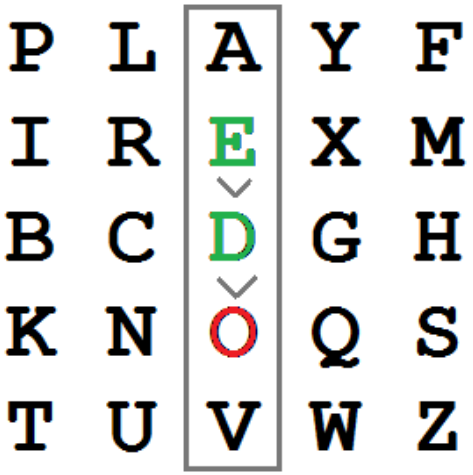


HI

Shape: Rectangle
Rule: Pick Same Rows, Opposite Corners

BM

Playfair Cipher : “DE”

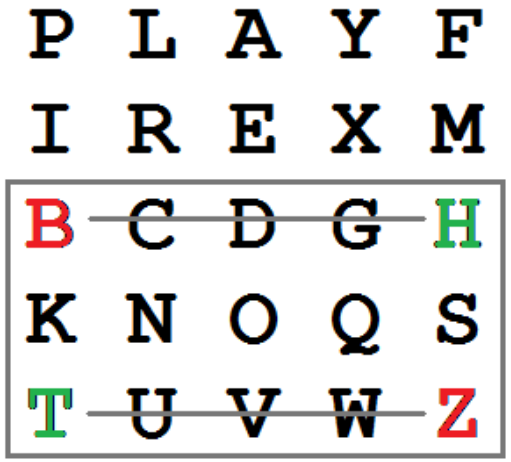


DE

Shape: Column
Rule: Pick Items Below Each Letter, Wrap to Top if Needed

OD

Playfair Cipher : “TH”

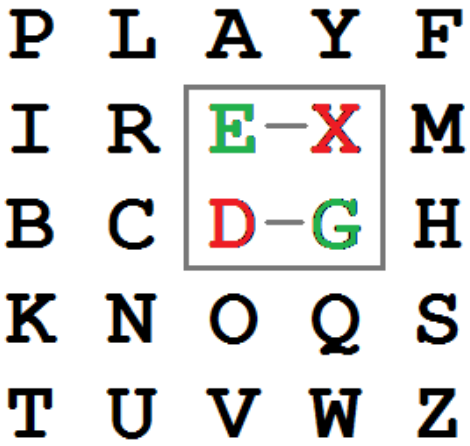


TH

Shape: Rectangle
Rule: Pick Same Rows, Opposite Corners

ZB

Playfair Cipher : “EG”

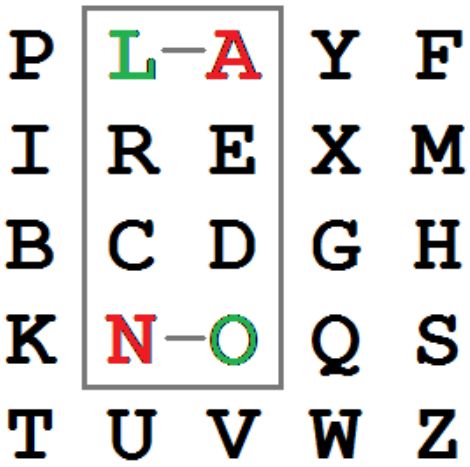


EG

Shape: Rectangle
Rule: Pick Same Rows, Opposite Corners

XD

Playfair Cipher : “OL”

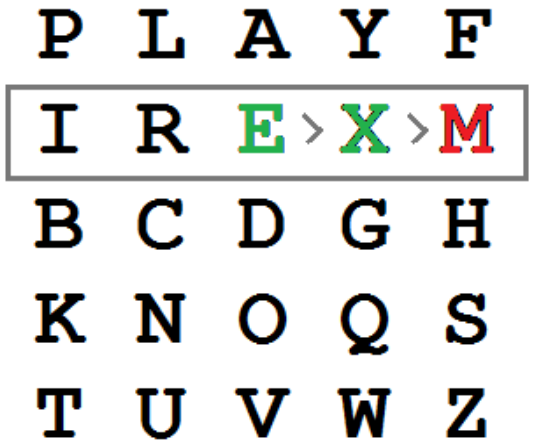


OL

Shape: Rectangle
Rule: Pick Same Rows, Opposite Corners

NA

Playfair Cipher : “EX”



EX

Shape: Row
Rule: Pick Items to Right of Each Letter, Wrap to Left if Needed

XM

Cipher Text

BM OD ZB XD NA BE KU DM UI XM MO UV IF

Enigma…

Kripto Sistem Aman

- Jika ciphertext dicuri, tidak bisa dipecahkan plaintext-nya

- Persisnya :
  - Apa yang diketahui musuh?
    - Jenis enkripsi
    - Pasangan plaintext-ciphertext yang pernah digunakan
    - Informasi tentang kunci yang kita pilih
  - Apa yang dimaksud tidak dapat dipecahkan plaintext-nya?
    - Ciphertext sama sekali **tidak menginformasikan** plaintext atau membutuhkan **waktu yang sangat lama** untuk dipecahkan meskipun menggunakan **komputer tercanggih**

Dalam Kenyataan…

- Keamanan informasi teoritis dimungkinkan
  - Cipher sempurna adalah aman secara teori informasi
- Tapi tidak praktis
  - Kunci harus sepanjang plaintext dan random
  - Sulit untuk dibuat dan berbagi (share)
- Sistem kripto yang digunakan berbasis keamanan komputasional

Keamanan Komputasional

- Idea 10.000 feet: not impossible to crack *cipher*, but very difficult to do so
  - Sehingga penyerang dengan sumberdaya terbatas akan mustahil untuk memecahkannya
- Sehingga : kunci yang dibutuhkan bisa lebih pendek dan mudah dibagi

- Disebut kripto 99%
- Masalah utama: seberapa yakin kita tentang sulit dipecahkan
  - Yakinkah sudah sangat sulit?
  - Bukankah tingkat kesulitan ini semakin lama semakin turun?