TIS13534P KOMUNIKASI DAN KEAMANAN DATA

Minggu 3 - Kriptografi

Definisi Kriptografi

- Kata ini bisa ditelusuri asal-usulnya yang di mana **kryptos** yang berarti “tersembunyi”, dan **graphein** yang artinya “tulisan”

- Secara istilih berarti **pesan yang disembunyikan** sehingga orang lain yang tidak berkepentingan **tidak bisa membaca** bahkan **mengerti pesan** tersebut

Istilah Umum di Kriptografi

- Plaintext : Pesan yang belum disembunyikan
- Ciphertext : Pesan yang sudah disembunyikan
- Key : Kunci yang digunakan untuk menyembunyikan pesan
- Encryption : Proses penyembunyian pesan
- Decryption : Proses membuka pesan tersembunyi

Sejarah Kriptografi

- Awal 1900SM, Penduduk Mesir menuliskan hieroglyphs dengan tatanan yang tidak biasa. Diperkirakan untuk menyembunyikan pesan. (Whitman, 2005)
- Orang-orang Romawi menemukan metode kriptografi yang dikenal sebagai ***Caesar Shift Cipher*** (menggunakan metode substitusi)
- Orang-orang Yunani menggunakan batang kayu sebagai alat metode kriptografinya

Sejarah Kriptografi

- Kriptografi saat itu tidak ada perkembangannya hingga Abad Pertengahan.
- **Leon Battista Alberti** adalah Bapak Kriptologi Barat dengan pengembangan kriptografi substitusi polyalphabetic
- Kriptografi polyalphabetic mengalami perubahan dan yang paling sering dikenal adalah **Vigenere**

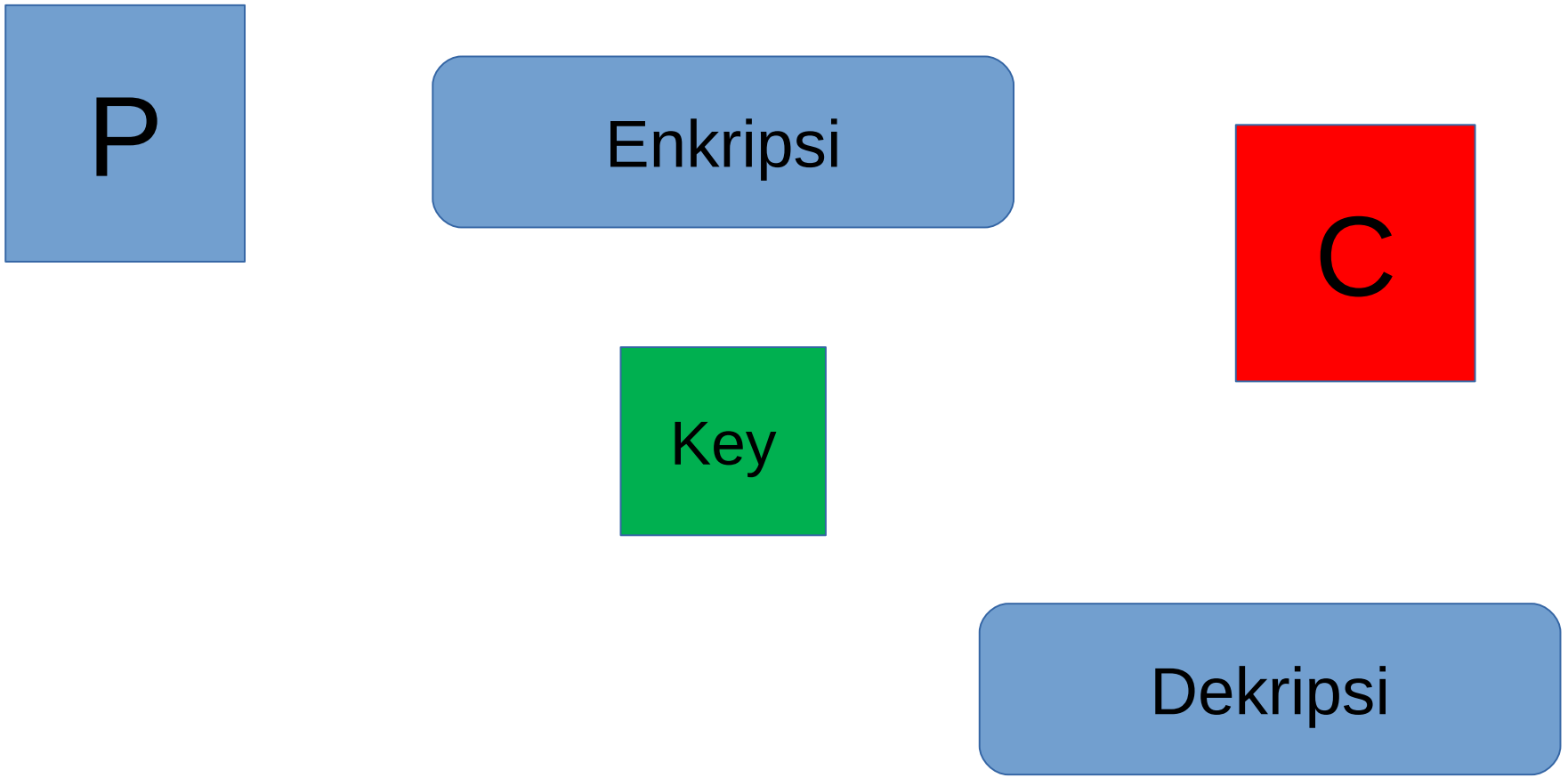
Sejarah Kriptografi

- Kriptografi kini telah diadopsi secara luas, menggunakan teknik yang berbeda-beda, bahkan kunci yang tidak 100% sama (asimetris)
- Penggunaannya sendiri telah menyebarluas dari untuk kepentingan pribadi (penyimpanan data), komunikasi, bahkan hingga kenegaraan.

Jenis Kriptografi

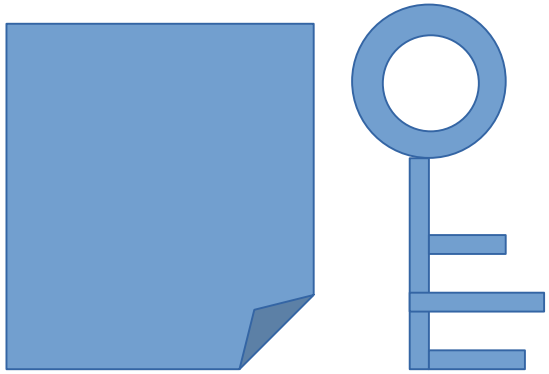
- **Menurut Era**
  - Kriptografi Klasik
  - Kriptografi Modern
- **Menurut Kunci**
  - Kriptografi Simetris
  - Kriptografi Asimetris

Kriptografi Simetris

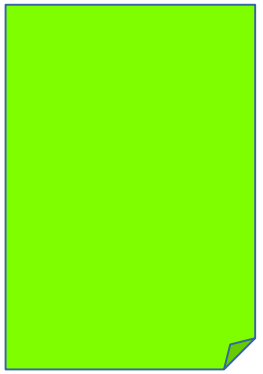


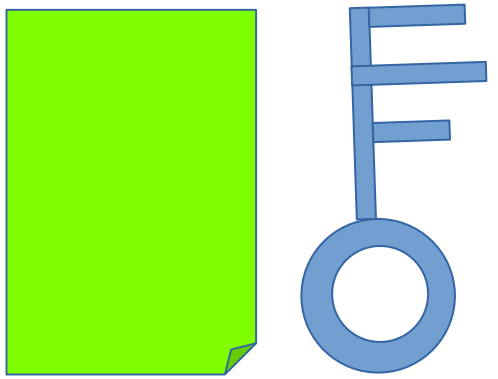
Kriptografi Asimetris

Kriptografi ini menggunakan dua kunci yang berbeda untuk mengakses pesan tersembunyinya

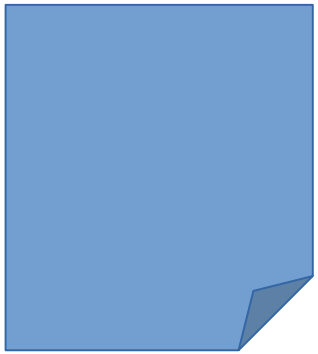


Public Key





Private Key



Kriptografi Klasik

- Kriptografi yang digunakan dijaman-jaman dahulu. Dari awal penggunaannya di kerajaan hingga Perang Dunia
- Algoritma di era ini adalah **substitusi**, yakni menukar karakter/huruf menjadi karakter lain
- Dan juga ada **transposition**, yakni mengubah plaintext dengan menggeser menjadi sebuah pola yang tetap

Caesar Cipher (Substitusi)

A	B	C	D	E	F	G	H	I	J
A	B	C	D	E	F	G	H	I	J

Baris pertama adalah Plaintext yang nantinya menjadi Ciphertext,
Baris kedua harus digeser sehingga pesan dapat tersembunyi

A	B	C	D	E	F	G	H	I	J
D	E	F	G	H	I	J	K	L	M

Baris kedua telah digeser ke kiri sebanyak 3 kali, dan enkripsi bisa dimulai.

Contoh:
P: GIGI ADI -> C: JLJL DGL

Cipher Transposition

- Pola ini merubah pesan menjadi pola yang tetap (memotong kata sesuai ukuran kunci nya)

1	2	3	4	5	6
A	K	U	P	U	N
Y	A	U	A	N	G
L	I	M	A	P	U
L	U	H	R	I	B
U	S	A	J	A	

P: Aku Punya Uang Lima Puluh Ribu Saja
C: AYLL KAIUS UUMHA PAARJ UNPIA NGUB

Vigenere Cipher

- Algoritma ini menggunakan sistem substitusi polyalphabetic.
- Pesan Plaintext ditulis di baris pertama, sedangkan kunci terletak ditulis kolom pertama (kunci ditulis berulang jika panjang kunci < plaintext)

Contoh Vigenere Cipher

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

P: Makan Es

K: LIBUR LI (diulang karena panjangnya berbeda)

C: MKEYW RP

Playfair Cipher

- Algoritma ini mengenkripsi plaintext dengan menghilangkan huruf yang berulang dan “J”.
- Kunci dari kriptografi ini berbentuk bujur sangkar berukuran 5x5.
- Jika plaintext yang sudah dibersihkan dari huruf berulang dan J, ditambah dengan huruf acak yang belum dipakai. Kemudian disusun layaknya Cipher Transposition.

Contoh PlayFair

P: Kucing Kita
Proses 1 -> KucingTa (Huruf Berulang dan J hilang)
Proses 2 -> KucingTaBD EFGHLMOPQR STUVW

C:
KGEMS UTFOT
CAGPU IBHQV
NDLRW

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

Kriptografi Modern

- Sesuai dengan namanya, Kriptografi ini dibuat di masa modern.
- Teknik yang digunakan adalah teknik baru atau campuran sehingga hasil enkripsi menjadi lebih susah dipecahkan.
- Dipakai hingga saat ini di manapun, dan untuk tujuan apapun
- Beroperasi dalam bentu bit biner:
  - 10101111011011100111011110111

Mekanism Simple Enkripsi

- Menggunakan Operator Logic (AND, OR, XOR)
  - A = 20
  - B = A XOR 5
  - C = B XOR 5

Proses

- Proses dilakukan dengan penghitungan jumlah karakter plaintext
- Lalu dilakukan looping sebanyak jumlah karakter tersebut
- Waktu proses looping berjalan karakter dari plaintext akan di-XOR kan dengan jumlah karakter
- Karakter berikutnya akan di-XOR kan dengan hasil sebelumnya. (Pengulangan)
- Hasil dari operasi XOR inilah yang disebut dengan Ciphertext

Contoh

- P: BULSARA, diubah menjadi hexadecimal menurut tabel ASCII
  - b <---- 62h
  - u <---- 75h
  - l <---- 6Ch
  - s <---- 73h
  - a <---- 61h
  - r <---- 72h
  - a <---- 61h

Proses Berlanjut

- 62 XOR 7 = **65**
- 75 XOR **65** = *10*
- 6C XOR *10* = **7C**
- 73 XOR **7C** = *0F*
- 61 XOR *0F* = **6E**
- 72 XOR **6E** = *1C*
- 61 XOR *1C* = 7D
- 65 10 7C 0F 6E 1C 7D → **e † | ☼ n▌}**

Proses Pengembalian

- Menggunakan cara yang sama dan dimulai dengan jumlah karakter plaintext (7)
  - **65 10 7C 0F 6E 1C 7D**
  - 65 XOR 7 = 62 -> b
  - 10 XOR 65 = 75 -> u
  - 7c XOR 10 = 6c -> l

Algoritma-Algoritma Lain

- DES (56-bit) -> Simetris
- 3DES (168-bit, 112-bit atau 56-bit) -> Simetris
- AES (128-bit, 192-bit, 256-bit) -> Simetris
- RSA (512-bit, 1024-bit, 2048-bit, 4096-bit[?])
  - Asimetris -> Public, dan Private Key
- Blowfish (32–448-bit)
  - Dikembangkan menjadi TwoFish

Block Cipher di Kriptografi Modern

- Blok Cipher adalah sebuah algoritma yang bekerja di sebuah blok bit yang berukuran tetap.
- Mode operasi yang adai di blok cipher adalah
  - **Electronic Codebook**, yang di mana blok-blok bit dipecah sesuai ukurannya. Jika terdapat kekurangan di akhir blok akan di tambah dengan padding bit. Dan setiap blok akan di enkripsi maupun di dekripsi sendiri-sendiri

Kriptanalisis

- Sebuah cara untuk mendapatkan Plaintext, dan Kunci tanpa mengetahui algoritmanya.
- Teknik analisis frekuensi
  - Cipherteks substitusi
  - Tidak bisa meyembunyikan hub statistik antara cipherteks dengan plainteks.
  - Huruf yang paling sering muncul di plainteks akan sering muncul juga di cipherteks.

Contoh

- UZ QSO VUOHXMOPV GPOZPEVSG
- ZWSZ OPFPESX UDBMETSX AIZ
- VUEPHZ HMDZSHZO WSFP APPD TSVP
- QUZW YMXUZUHSX EPYEPOPDZSZUPO
- MB ZWP FUPZ HMDJ UD TMOHMQ

Proses Dekripsi #1

- P → E
- Z → T

Hasil Dugaan #1

- UZ QSO VUOHXMOPV GPOZPEVSG
- t e e t
- ZWSZ OPFPESX UDBMETSX AIZ
- t t e e
- VUEPHZ HMDZSHZO WSFP APPD TSVP
- e t t t e ee e
- QUZW YMXUZUHSX EPYEPOPDZSZUPO
- t t e e e t t e
- MB ZWP FUPZ HMDJ UD TMOHMQ
- t e e t

Iterasi #2

- zwp dan zwsz dipetakan menjadi t*e dan t**t
- Menduga w → h dan s → a

Hasil Dugaan #2

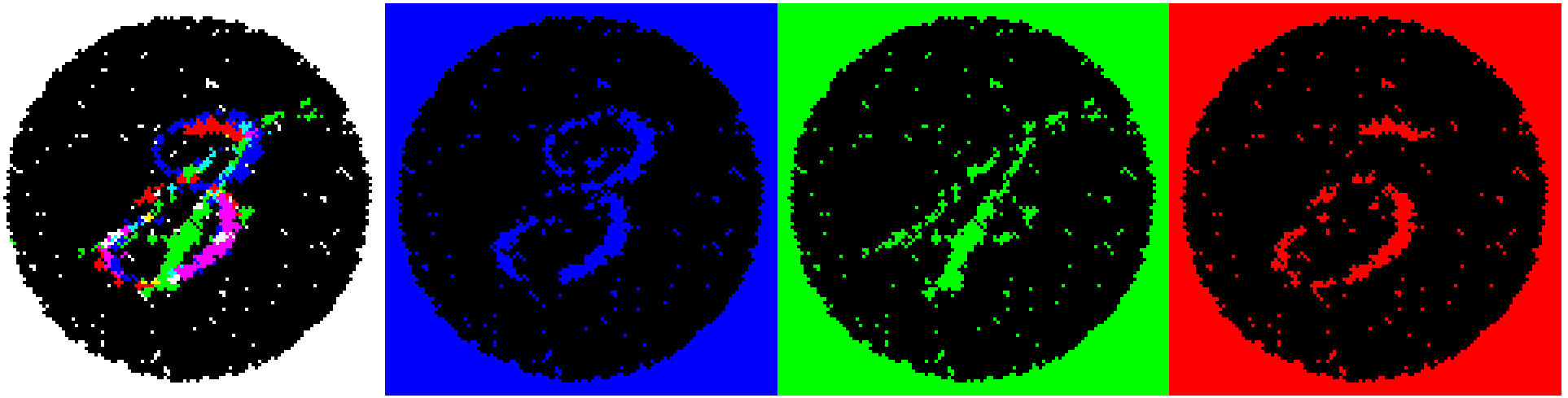
- UZ QSO VUOHXMOPV GPOZPEVSG
- t a e e te a
- ZWSZ OPFPESX UDBMETSX AIZ
- that e e a a t
- VUEPHZ HMDZSHZO WSFP APPD TSVP
- e t t a t ha e ee a e
- QUZW YMXUZUHSX EPYEPOPDZSZUPO
- th a e e e ta t e
- MB ZWP FUPZ HMDJ UD TMOHMQ
- t h e e t

Hasil Dekripsi

- UZ QSO VUOHXMOPV GPOZPEVSG
- IT WAS DISCLOSED YESTERDAY
- ZWSZ OPFPESX UDBMETSX AIZ
- THAT SEVERAL INFORMAL BUT
- VUEPHZ HMDZSHZO WSFP APPD TSVP
- DIRECT CONTACTS HAVE BEEN MADE
- QUZW YMXUZUHSX EPYEPOPDZSZUPO
- WITH POLITICAL REPRESENTATIES
- MB ZWP FUPZ HMDJ UD TMOHMQ
- OF THE VIET CONG IN MOSCOW

Steganografi

- Suatu teknik penyembunyian Gambar, File, Pesan, Audio ke dalam file, video, audio lainnya



Bentuk Penyembunyian

- Secara fisik:
  - Menggunakan tinta tak terlihat
  - Pesan Kode Morse dalam bola wol yang dirajut kedalam kain pakaian sang kurir
  - Pesan yang ditulis di amplop dan tertutupi stempel pos
- Secara digital:
  - Menyembunyikan pesan di bit terendah dari gambar atau file suara yang *noisy*

Bentuk Penyembunyian

- Digital Text
  - Membuat teks memiliki warna yang sama dengan background word editor, e-mail, dan post forum
  - Menggunakan karakter Unicode yang terlihat sama dengan karakter standar ASCII, secara visual tidak ada perbedaan.
- Social Steganography
  - Menyembunyikan pesan di judul, atau konteks dari video/gambar yang dibagikan
  - Kesalahan pengejaan nama atau kata yang populer di media, bisa mensugestikan makna lain

Contoh Stegano Digital

Bersambung....