SYMMETRIC CIPHERS PART 1

--Dr. Mike Yuliana--

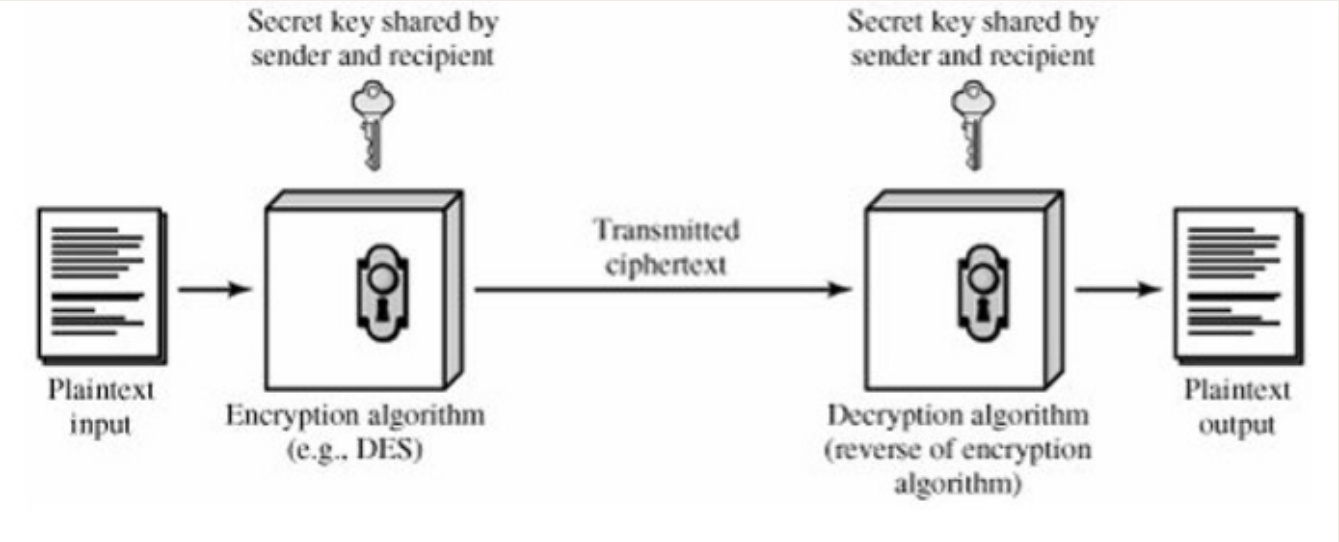
Mata Kuliah : Keamanan Jaringan

Politeknik Elektronika Negeri Surabaya (PENS)

Outline

- Enkripsi simetris
- Cryptanalysis
- Algoritma enkripsi klasik
  - *Teknik Substitusi*
  - *Teknik Transposisi*

Enkripsi Simetris (1)



- Disebut juga dengan enkripsi konvensional atau single key encryption atau private key
- Sender dan recipient melakukan share key
- Semua algoritma enkripsi konvensional menggunakan private key

Enkripsi Simetris (2)

Lima komponen enkripsi simetris :

- Plaintext : pesan atau data asli yang digunakan sebagai input
- Algoritma enkripsi : Algoritma enkripsi melakukan berbagai substitusi dan transformasi pada plaintext
- Secret key : kunci yang digunakan untuk mengacak pesan
- Ciphertext : pesan acak yang dijadikan sebagai output
- Algoritma dekripsi : Algoritma enkripsi yang digunakan secara terbalik dan digunakan untuk menghasilkan pesan atau data asli kembali

Enkripsi Simetris (3)

Keamanan enkripsi simetris tercapai jika :

- Algoritma enkripsi simetris yang digunakan merupakan algoritma yang strong
- Sender dan receiver harus mendapatkan secret key dengan cara yang aman

Kriptografi

studi tentang algoritma ekripsi

Klasifikasi kriptografi:

- Tipe operasi yang digunakan untuk merubah plaintext ke ciphertext
  - *Substitusi*
  - *Transposisi*
  - *Sistem produk*
- Jumlah kunci yang digunakan
  - *Single key*
  - *Two key*
- Mekanisme pemrosesan plaintext
  - *Block cipher*
  - *Stream cipher*

Cryptanalysis

studi tentang metode *deciphering ciphertext* tanpa mengetahui kunci

- Cryptanalytic attack → Jenis serangan ini mengeksploitasi karakteristik algoritma yang akan dicoba atau menyimpulkan kunci yang digunakan
- Brute-force attack → Penyerang mencoba setiap kunci yang mungkin pada ciphertext hingga didapatkan plaintext yang bisa dimengerti

Symmetric Block Cipher Algorithm

studi tentang metode *deciphering ciphertext* tanpa mengetahui kunci

- Cryptanalytic attack → Jenis serangan ini mengeksploitasi karakteristik algoritma yang akan dicoba atau menyimpulkan kunci yang digunakan
- Brute-force attack → Penyerang mencoba setiap kunci yang mungkin pada ciphertext hingga didapatkan plaintext yang bisa dimengerti

Teknik Substitusi (Caesar Cipher) (1)

→ Teknik substitusi : Teknik yang mengganti huruf pada plaintext dengan huruf lain

- Algoritma enkripsi dapat dituliskan sebagai berikut:

$$C = E(p) = (p + k) mod\ 26$$

Dimana p adalah huruf dari plaintext, C adalah huruf dari ciphertext, sedangkan k menunjukkan jumlah pergeseran yang berkisar antara 1 hingga 25

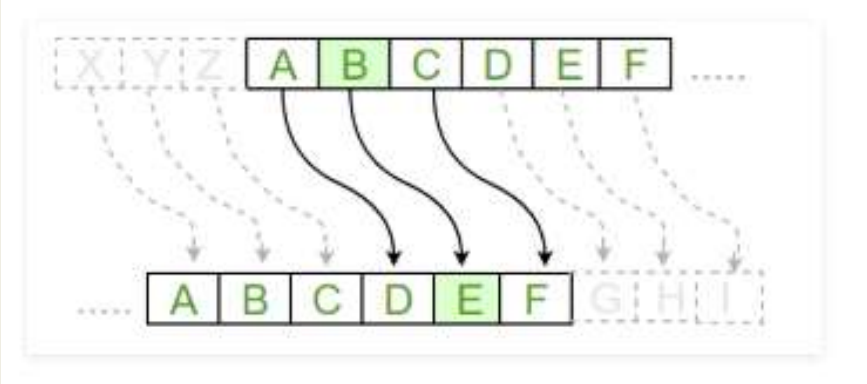
- Algoritma dekripsi dapat dituliskan sebagai berikut:

$$p = D(C) = (C - k) mod\ 26$$

Caesar Cipher

Teknik Substitusi (Caesar Cipher) (2)

k sebesar 3



Contoh :

Text : ABCDEFGHIJKLMNOPQRSTUVWXYZ
Shift: 23
Cipher: XYZABCDEFGHIJKLMNOPQRSTUVW

Text : ATTACKATONCE
Shift: 4
Cipher: EXXEGOEXSRGI

Teknik Substitusi (Caesar Cipher) (3)

Contoh Soal :

1. Dengan menggunakan Caesar cipher,tentukan ciphertext dari

   plain : meet me after the toga party

2. Jelaskan proses enkripsi dan dekripsi dari

   plain : halo apa kabar hari ini

Teknik Substitusi (Hill Cipher) (1)

→ Penerapan Aritmatika Modulo pada kriptografi serta menggunakan sebuah matriks persegi sebagai kunci yang digunakan untuk melakukan enkripsi dan dekripsi.

- Algoritma enkripsi Hill Cipher:
  - *Korespondenkan abjad dengan numerik*

    $$A \rightarrow 1, B \rightarrow 2, \ldots, Z \rightarrow 26$$

  - *Buat matriks kunci berukuran* mxm

    $$K_{mxm} = \begin{bmatrix} k_{11} & k_{12} & \ldots & k_{1m} \\ k_{21} & k_{22} & \ldots & k_{2m} \\ \ldots & \ldots & \ldots & \ldots \\ k_{m1} & k_{m2} & \ldots & k_{mm} \end{bmatrix}$$

  - Matrik K merupakan matriks *yang invertible* yaitu memiliki *multi plicative inverse* $K-1$ sehingga $K.K-1 = 1$

Teknik Substitusi (Hill Cipher) (2)

- Algoritma enkripsi Hill Cipher (lanjutan 1):
  - Plainteks *P* = *p*1 *p*2 ... *pn* , diblok dengan ukuran sama dengan baris atau kolom matrik K, sehingga

$$P_{qxm} = \begin{bmatrix} p_{11} & p_{12} & \cdots & p_{1m} \\ p_{21} & p_{22} & \cdots & p_{2m} \\ \cdots & \cdots & \cdots & \cdots \\ p_{q1} & p_{q2} & \cdots & p_{qm} \end{bmatrix}$$

  - *Matrik P* ditranspose menjadi

$$P^{t}_{mxq} = \begin{bmatrix} p_{11} & p_{21} & \cdots & p_{1q} \\ p_{12} & p_{22} & \cdots & p_{2q} \\ \cdots & \cdots & \cdots & \cdots \\ p_{1m} & p_{2m} & \cdots & p_{qm} \end{bmatrix}$$

  - Kalikan Matrik K dengan Matrik P transpose dalam modulo 26

$$C^{t} = K_{mxm} P^{t}_{mxq}$$

$$\begin{bmatrix} k_{11} & k_{12} & \cdots & k_{1m} \\ k_{21} & k_{22} & \cdots & k_{2m} \end{bmatrix} \begin{bmatrix} p_{11} & p_{21} & \cdots & p_{1q} \\ p_{12} & p_{22} & \cdots & p_{2q} \end{bmatrix} \begin{bmatrix} c_{11} & c_{21} & \cdots & c_{m1} \\ c_{12} & c_{22} & \cdots & c_{m2} \end{bmatrix}$$

Teknik Substitusi (Hill Cipher) (3)

- Algoritma enkripsi Hill Cipher (lanjutan 2):
  - Kemudian ditransposekan

$$C = (C^t)^t = \begin{bmatrix} c_{11} & c_{12} & \dots & c_{1q} \\ c_{21} & c_{22} & \dots & c_{2q} \\ \dots & \dots & \dots & \dots \\ c_{m1} & c_{m2} & \dots & c_{mq} \end{bmatrix}$$

- Algoritma Dekripsi Hill Cipher :
  - Korespondenkan abjad dengan numerik

$$A \rightarrow 1, B \rightarrow 2, \dots, Z \rightarrow 26$$

  - Ubah cipherteks kedalam numerik
  - Kunci yang digunakan untuk mendekrip ciphertext ke plaintext adalah invers dari matrik kunci *K mxm*
  - Menghitung $K-1$

Teknik Substitusi (Hill Cipher) (4)

- Algoritma Dekripsi Hill Cipher (lanjutan):
  - Korespondenkan abjad dengan numerik

    $A \rightarrow 1, B \rightarrow 2,\ldots, Z \rightarrow 26$
  - Ubah cipherteks kedalam numerik
  - Kunci yang digunakan untuk mendekrip ciphertext ke plaintext adalah invers dari matrik kunci *K mxm*
  - Kalikan invers matriks kunci dengan cipherteks transpose dalam modulo 26, diperoleh plainteks transpose $P\,t = K - 1C\,t$
  - Dari langkah ke-5 diperoleh $P = (P\,t)\,t$
  - Korespondensikan abjad dengan numerik hasil langkah 6 diperoleh plainteks

Teknik Substitusi (Hill Cipher) (5)

Korespondenkan abjad :

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	0

Secara matematis proses enkripsi:

$$C = K \cdot P \,(2)$$

Plaintext :

```
P = STRIKE NOW
```

Konversi :

```
P = 19 20 18 9 11 5 14 15 23
```

Blok pertama dari plaintext :

$$P_{1,2} = \begin{bmatrix} 19 \\ 20 \end{bmatrix}$$

Proses Enkripsi:

$$C_{1,2} = \begin{bmatrix} 5 & 6 \\ 2 & 3 \end{bmatrix} \begin{bmatrix} 19 \\ 20 \end{bmatrix} = \begin{bmatrix} 215 \\ 98 \end{bmatrix}$$

$$C_{1,2} = \begin{bmatrix} 215 \\ 98 \end{bmatrix} = \begin{bmatrix} 7 \\ 20 \end{bmatrix} (\text{mod } 26)$$

Ciphertext:

P = STRIKENOW

C = 7 20 14 11 7 11 4 21 19 11

C = GTNKGKDUSK

Teknik Substitusi (Hill Cipher) (6)

Secara matematis proses dekripsi :

$$
\begin{aligned}
C &= K.P \\
K^{-1}.C &= K^{-1}.K.P \\
K^{-1}.C &= I.P \\
P &= K^{-1}.C
\end{aligned}
$$

Proses Dekripsi:

$$P_{1,2} = K^{-1}.C_{1,2}$$

$$P_{1,2} = \begin{bmatrix} 1 & 24 \\ 8 & 19 \end{bmatrix} \cdot \begin{bmatrix} 7 \\ 20 \end{bmatrix} = \begin{bmatrix} 487 \\ 436 \end{bmatrix} = \begin{bmatrix} 19 \\ 20 \end{bmatrix} (\text{mod } 26)$$

Hasil Dekripsi:

P = 19 20 18 9 11 5 14 15 23

P = STRIKENOW

Teknik Transposisi (1) →per rangkaian karakter

→Algoritma ini melakukan transpose terhadap rangkaian karakter didalam teks. Algoritma ini dikenal juga dengan nama permutasi.

1	2	3	4	5	6
3	5	1	6	4	2

⇨ Kunci permutasi (enkripsi)

Plaintext : SAYA SEDANG BELAJAR KEAMANAN KOMPUTER

Pemotongan Plaintext menjadi 6 blok : SAYASE DANGBE LAJARK EAMANA NKOMPU TERXXX

Hasil Enkripsi: YSSEAA NBDEGA JRLKAA MNEAAA OPNUMK RXTXXE

1	2	3	4	5	6
3	6	1	5	2	4

⇨ Kunci permutasi (dekripsi)

Hasil Enkripsi: SAYA SEDANG BELAJAR KEAMANAN KOMPUTER

Teknik Transposisi (2) →segitiga

Plaintext : SAYA SEDANG BELAJAR KEAMANAN KOMPUTER

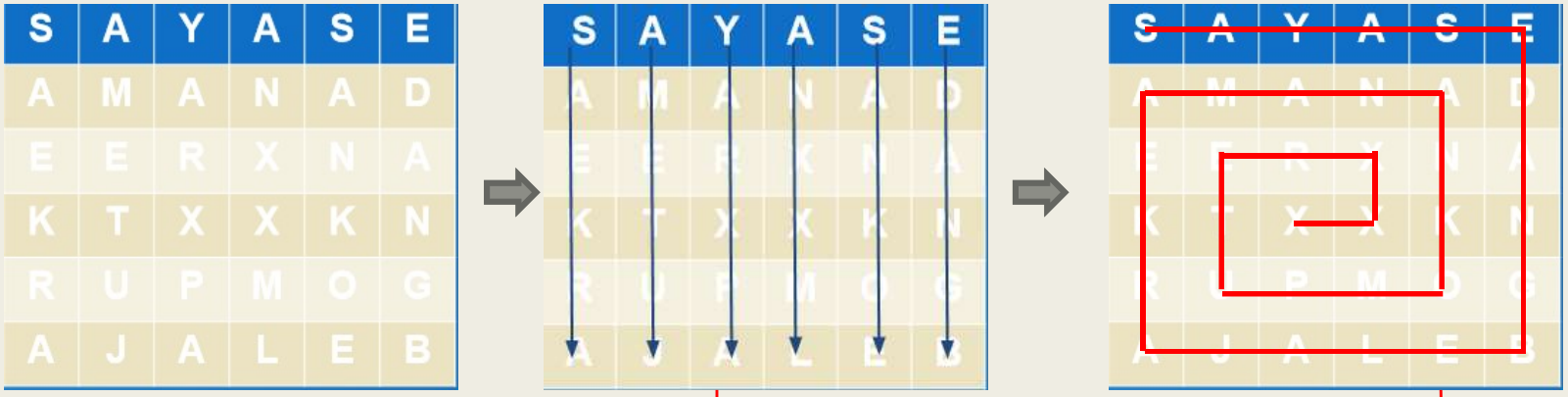
					S					
				A	Y	A				
			S	E	D	A	N			
		G	B	E	L	A	J	A		
	R	K	E	A	M	A	N	A	N	
K	O	M	P	U	T	E	R	X	X	X

Ciphertext : KROGKMSBEPAEEAUSYDLMTAAAAENJNRAAXNXX → Enkripsi

Plaintext: KROGKMSBEPAEEAUSYDLMTAAAAENJNRAAXNXX → Dekripsi

Teknik Transposisi (3) →Spiral

Plaintext : SAYA SEDANG BELAJAR KEAMANAN KOMPUTER

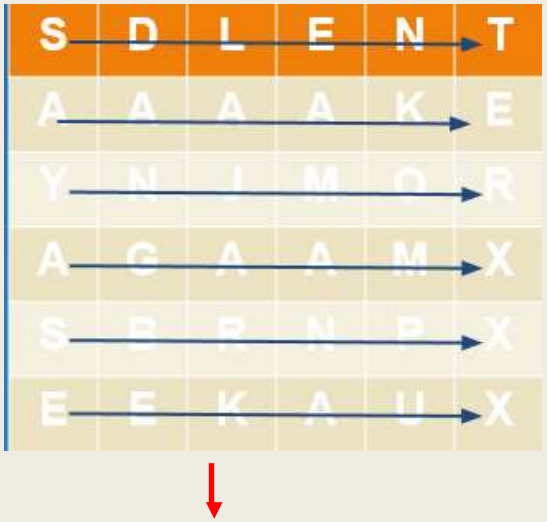


Ciphertext : SAEKRAAMETUJYARXPAANXXMLSANKOEEDANGB

Plaintext : SAYA SEDANG BELAJAR KEAMANAN KOMPUTER

Teknik Transposisi (4) →Diagonal

Plaintext : SAYA SEDANG BELAJAR KEAMANAN KOMPUTER

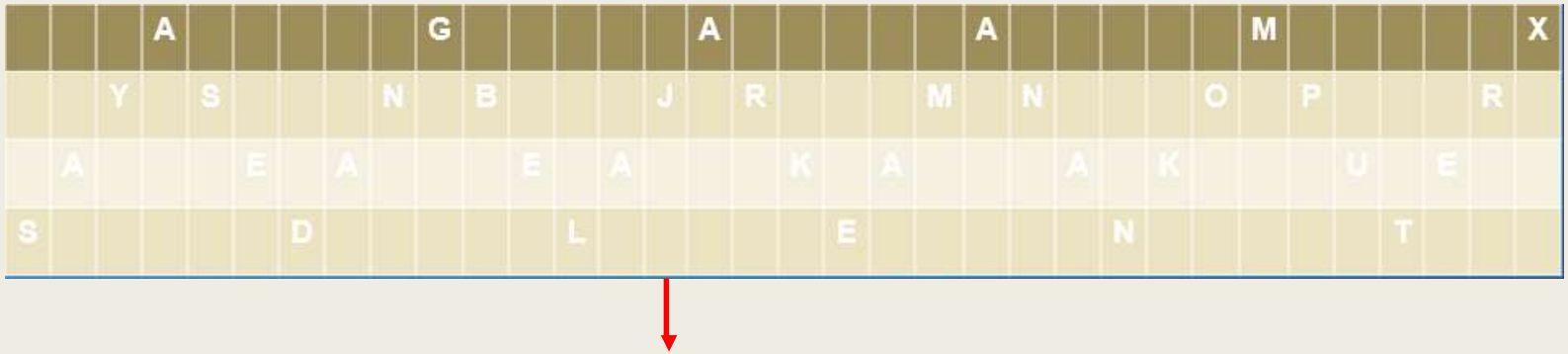


Ciphertext : SDLENTAAAAKEYNJMORAGAAMXSBRNPXEEKAUX

Plaintext : SAYA SEDANG BELAJAR KEAMANAN KOMPUTER

Teknik Transposisi (5) →Zig-zag

Plaintext : SAYA SEDANG BELAJAR KEAMANAN KOMPUTER



Ciphertext : AGAAMXYSNBJRMNORAEAEAKAAKUESDLENT