KRIPTOGRAFI KLASIK 2
SANDI AFFINE, HILL, ONE-TIME PAD, dan ROTOR

Dr. R. Rizal Isnanto, S.T., M.M., M.T.

Computer-Electrical Engineering
Diponegoro University

Konsep Modulo (1)

- Konsep Modulo merupakan bagian yang dibahas pada Matematika Diskret. Sangat sering dipakai dlm alg. modern
- Operasi modulo, misal: $a \bmod b = c$ mempersyaratkan nilai-nilai *a, b,* dan *c* harus integer (bulat), dengan *c* merupakan sisa hasil-bagi bulat dari a/b → div (a/b)
- Contoh: $10/3 = 3$, sisa 1 → maka $10 \bmod 3 = 1$
- Penggunaan kalkulator yang tidak ada fungsi **mod**-nya

  contoh: Berapa 124 mod 5?

  cara: 124 : 5 = 24.8

  24

  0.8

  0.8*5 = 4

  Sehingga, $124 \bmod 5 = 4$, atau bisa ditulis: $124 \equiv 4 \bmod 5$

Konsep Modulo (2)

- Jika a mod b, dengan $a < b$, maka a mod $b = a$
- Jika a mod b, dengan $a > b/2$ dan $a < b$ maka a mod $b = a\text{-}b = -(b\text{-}a)$

Contoh: berapakah 31 mod 33?

Jawab: $a = 31$, $b = 33$, dengan $a < b$ ($=31 < 33$), sekaligus

$a > b/2$ ($= 31 > 33/2 = 16{,}5$), maka dapat dituliskan:

$31 \bmod 33 = 31 \equiv 31\text{-}33 \equiv -2 \bmod 33$

atau dapat ditulis: $31 \equiv 31\text{-}33 \equiv -2 \bmod 33$

yang merupakan cara penulisan cepat.

Angka hasil modulo yang kecil lebih disukai → lebih mudah penghitungannya pada *fast exponentiation* (dibahas nanti)

Model penulisan lain (lebih panjang):

$31 \bmod 33 = (31\text{-}33) \bmod 33 = -2 \bmod 33 = -2$

SANDI AFFINE (1)

$e_1 = (a\,p_1 + b) \bmod 26$ | Kunci (a, b)

$e_2 = (a\,p_2 + b) \bmod 26$

Contoh : BIMA SAKTI. ; dg. kunci (15, 7)

Tabel Konversi :

	A	B	C	D	E	F	G	H	I	. . .	W	X	Y	Z
	0	1	2	3	4	5	6	7	8	.	22	23	24	25

B $e(0) = (15 \times 1) + 7 = 22$ → = 'W'

I $e(1) = (15 \times 8) + 7 = 23$ → = 'X'

M $e(2) =$ → 127 =

$e(3) =$

$e(4) =$

SANDI AFFINE (2)

Enkripsi → jelas.

Dekripsi → utk. mencari kunci (a, b) cukup dg. ~~brute force~~ attack dari 2 known plaintext attack.

$W \rightarrow e(0) = a p_0 + b$

$X \rightarrow e(1) = a p_1 + b$

B

$22 = a(1) + b \rightarrow a + b = 22$

$23 = a(8) + b \rightarrow 8a + b = 23$

$7a = 1 \mod 26$

$\uparrow_I$

SANDI AFFINE (3)

Enkripsi → jelas?

Dekripsi → utk. mencari kunci (a, b) cukup dg. ~~brute force~~ attack dari 2 known plaintext attack.

$W \rightarrow e(0) = a p_0 + b$.

$X \rightarrow e(1) = a p_1 + b$.

B

$22 = a(1) + b \rightarrow a + b = 22$.

$23 = a(8) + b \rightarrow 8a + b = 23$

$7a = 1 \mod 26$.

$\uparrow_I$

SANDI AFFINE (4)

Gunakan Trial & Error!

a	$7a \bmod 26 \stackrel{?}{=} 1$.	
0	0.	bukan
1	7.	bukan
2	14.	bukan
3	21	bukan
⋮	⋮	
15	1	ya. ✓
⋮	⋮	
25	19.	

Shg $a = 15$.

$22 = a + b$

$15 + b = 22 \rightarrow b = 7$.

SANDI HILL (1)

Sandi polyalphabet dg. perkalian matriks.

Contoh : Teks "MATAHARI"

Huruf ke.	0	1	2	3	4	5	6	...
Plaintext.	A	B	C	D	E	F	G	H.

"MATAHARI" = {12, 0, 19, 0, 7, 0, 17, 8}.

Kunci

$$K = \begin{bmatrix} 10 & 7 \\ 5 & 21 \end{bmatrix}$$

$$\begin{bmatrix} C(0) & C(2) & C(4) & C(6) \\ C(1) & C(3) & C(5) & C(7) \end{bmatrix} = \begin{bmatrix} 10 & 7 \\ 5 & 21 \end{bmatrix} \begin{bmatrix} 12 & 19 & 7 & 17 \\ 0 & 0 & 0 & 8 \end{bmatrix}$$

$$= \begin{bmatrix} 120 & 190 & 70 & 170+56 \\ 60 & 95 & 35 & 253 \end{bmatrix} \begin{matrix} \\ \\ \end{matrix} \begin{matrix} =226 \\ \\ \end{matrix} \bmod 26.$$

SANDI HILL (2)

$$= \begin{bmatrix} 120 & 190 & 70 & 170+56 \\ 60 & 95 & 35 & 253 \end{bmatrix} \quad \begin{matrix} = 226 \\ \text{mod } 26. \end{matrix}$$

$$= \begin{bmatrix} 16 & 8 & 18 & 18 \\ 8 & 17 & 9 & 19 \end{bmatrix} = \begin{bmatrix} 'Q' & 'I' & 'S' & 'S' \\ 'I' & 'R' & 'J' & 'T' \end{bmatrix}$$

Shy. Ciphertext = "QII RSJST".

SANDI HILL (3)

$$= \begin{bmatrix} 120 & 190 & 70 & 170+56 \\ 60 & 95 & 35 & 253 \end{bmatrix} \quad \begin{matrix} = 226 \\ \text{mod } 26. \end{matrix}$$

$$= \begin{bmatrix} 16 & 8 & 18 & 18 \\ 8 & 17 & 9 & 19 \end{bmatrix} = \begin{bmatrix} 'Q' & 'I' & 'S' & 'S' \\ 'I' & 'R' & 'J' & 'T' \end{bmatrix}$$

shy. Ciphertext = "QII RSJST".

SANDI ONE-TIME PAD (1)

SANDI ONE TIME PAD

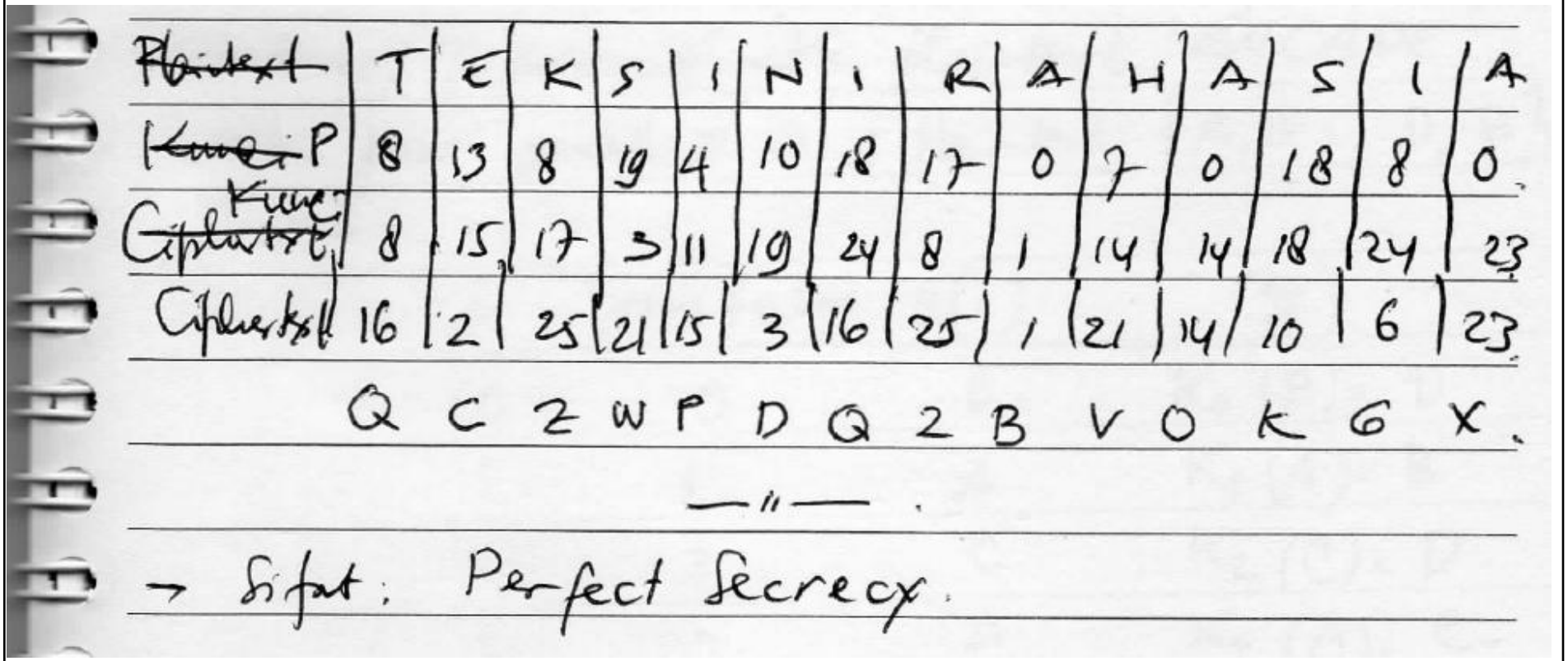
Setiap karakter / blok karakter, kuncinya dibangkitkan secara acak utk. seluruh plaintext. dan hanya digunakan sekali

Contoh: One Time Pad dg Sandi Caesar.

Plaintext = ~~TEKNIS~~ TEKSINIRAHASIA.

Kunci = {8, 15, 17, 3, 11, 19, 24, 8, 1, 14, 14, 18, 24, 23}

SANDI ONE-TIME PAD (2)



~~Plaintext~~	T	E	K	S	I	N	I	R	A	H	A	S	I	A
~~Key~~ P	8	13	8	19	4	10	18	17	0	7	0	18	8	0
Key														
~~Ciphertext~~	8	15	17	3	11	19	24	8	1	14	14	18	24	23
Ciphertext	16	2	25	21	15	3	16	25	1	21	14	10	6	23

Q C Z W P D Q Z B V O K G X.

— " —

→ Sifat: Perfect Secrecy.

SANDI ROTOR (1)

Kunci berubah setiap saat dg. menggunakan rotor.
Misal Rotor dg. 4 posisi. Rotor berputar pada
posisi 0, 1, 2, ~~dan~~ 3, 0, 1, 2, 3 ...
Kalau rotor di posisi 0, gunakan kunci 0
dst

Contoh : Mesin Rotor 3 posisi, dg 3 kunci
substitusi: $K_0 = \{C, D, E, A, B\}$
$K_1 = \{B, E, A, C, D\}$
$K_2 = \{E, A, D, B, C\}$
Tentukan Teks sandi utk plaintext "BACADE"
Jika posisi awal = 0 ; plaintext $\{A, B, C, D, E\}$

SANDI ROTOR (2)

substitusi: $K_0 = \{C, D, E, A, B\}$

$K_1 = \{B, E, A, C, D\}$

$K_2 = \{E, A, D, B, C\}$

Tentukan Teks sandi untuk plaintext "BACADE"

Jika posisi awal = 0 ; plaintext {A, B, C, D, E}

Jawab :

i	posisi Rotor	p(i)	C(i)
0	0	B	$K_0(B) = D$
1	1	A	$K_1(A) = B$
2	2	C	$K_2(C) = D$
3	0	A	$K_0(A) = C$
4	1	D	$K_1(D) = C$
5	2	E	$K_2(E) = C$

shg. ciphertext: "D B D C C C"

Ada pertanyaan?

- Terima kasih