

Kriptografi Klasik

Bahan Kuliah Keamanan Data

Sevi Nurafni

Fakultas Sains dan Teknologi

Universitas Koperasi Indonesia 2025

Kenapa perlu belajar?



1. Memahami konsep dasar kriptografi
2. Dasar algoritma kriptografi modern
3. Memahami kelemahan sistem cipher

1. ***Cipher Substitusi***: mengganti huruf plainteks dengan huruf ciperteks
2. ***Cipher Transposisi***: mengubah susunan/posisi huruf plainteks ke posisi lainnya

Cipher Substitusi



- Contoh: Caesar Cipher
- Tiap huruf alfabet digeser 3 huruf ke kanan

P_i : 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
 C_i : **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**

- Contoh:

Plainteks: materinya banyak banget

Cipherteks: PDWHULQBD EDQBDN EDQJHW

Caesar Cipher



- Supaya lebih aman, cipherteks dikelompokkan ke dalam kelompok n-huruf misalnya kelompok 4 huruf

Semula: PDWHULQBD EDQBDN EDQJHW

Menjadi: PDWH ULQB DEDQ BDNE DQJHW

- Atau membuang semua spasi:

PDWHULQBDEDEDQBDNEDQJHW

- Tujuannya agar kriptanalisis menjadi lebih sulit

Caesar Cipher



- Misal kan, $A = 0$,
 $B = 1$,
 $C = 2$,
 $Z = 25$

Maka, Caesar Cipher dirumuskan secara matematis:

Enkripsi: $c = E(p) = (p + 3) \bmod 26$

Dekripsi: $p = D(c) = (c - 3) \bmod 26$

Caesar Cipher



Plainteks: materinya banyak banget

- $p_1 = 'm' = 12 \rightarrow E(12) = (12 + 3) \bmod 26 = 15 = 'P'$
- $p_2 = 'a' = 0 \rightarrow E(0) = (0 + 3) \bmod 26 = 3 = 'D'$
- $p_3 = 't' = 19 \rightarrow E(19) = (19 + 3) \bmod 26 = 22 = 'W'$
- $p_4 = 'e' = 4 \rightarrow E(4) = (4 + 3) \bmod 26 = 7 = 'H'$
- $p_5 = 'r' = 17 \rightarrow E(17) = (17 + 3) \bmod 26 = 20 = 'U'$
- $p_6 = 'i' = 8 \rightarrow E(8) = (8 + 3) \bmod 26 = 11 = 'L'$
- ...

Cipherteks: PDWHULQBD EDQBDN EDQJHW

Caesar Cipher



Cipherteks: PDWHULQBD EDQBDN EDQJHW

- $c_1 = 'P' = 15 \rightarrow D(15) = (15 - 3) \bmod 26 = 12 = 'm'$
- $c_2 = 'D' = 3 \rightarrow D(3) = (3 - 3) \bmod 26 = 0 = 'a'$
- $c_3 = 'W' = 22 \rightarrow D(22) = (22 - 3) \bmod 26 = 19 = 't'$
- $c_4 = 'H' = 7 \rightarrow D(7) = (7 - 3) \bmod 26 = 4 = 'e'$
- $c_5 = 'U' = 20 \rightarrow D(20) = (20 - 3) \bmod 26 = 17 = 'r'$
- $c_6 = 'L' = 11 \rightarrow D(11) = (11 - 3) \bmod 26 = 8 = 'i'$
- ...

Plainteks: materinya banyak banget

Caesar Cipher



- Jika pergeseran huruf sejauh k , maka:

Enkripsi: $c = E(p) = (p + k) \bmod 26$

Dekripsi: $p = D(c) = (c - k) \bmod 26$

- Untuk 256 karakter ASCII, maka:

Enkripsi: $c = E(p) = (p + 3) \bmod 256$

Dekripsi: $p = D(c) = (c - 3) \bmod 256$

k = kunci rahasia

Caesar Cipher



- Kelemahan:
- Caesar cipher mudah dipecahkan dengan *exhaustive key search* karena jumlah kuncinya sangat sedikit (hanya ada 26 kunci)

Caesar Cipher

Contoh: kriptogram XMZVH

Tabel 1. Contoh *exhaustive key search* terhadap cipherteks XMZVH

Kunci (k) <i>ciphering</i>	'Pesan' hasil dekripsi	Kunci (k) <i>ciphering</i>	'Pesan' hasil dekripsi	Kunci (k) <i>ciphering</i>	'Pesan' hasil dekripsi
0	XMZVH	17	GVIEQ	8	PERNZ
25	YNAWI	16	HWJFR	7	QFSOA
24	ZOBXJ	15	IXKGS	6	RGTPB
23	APCYK	14	JYLHT	5	SHUQC
22	BQDZL	13	KZMIU	4	TIVRD
21	CREAM	12	LANJV	3	UJWSE
20	DSFBN	11	MBOKW	2	VKXTF
19	ETGCO	10	NCPLX	1	WLYUG
18	FUHDP	9	ODQMY		

Plainteks yang potensial adalah CREAM dengan $k = 21$.
Kunci ini digunakan untuk mendekripsikan cipherteks lainnya.

Cipher Transposisi



- Cipherteks diperoleh dengan mengubah posisi huruf di dalam plainteks
- Nama lain untuk metode ini adalah **permutasi**, karena transpose setiap karakter di dalam teks sama dnegan mempermutasikan karakter-karakter tersebut.

- Contoh:

Plainteks: hari kamis keamanan data

Enkripsi: harik
 amisk
 eaman
 andat
 aXXXX

Cipher Transposisi



- Contoh:

Plainteks: i n f o r m a s i

Enkripsi: i n f o

 R m a s

 I x x x

Cipherteks: i r i n m x f a x o s x

Cipher Transposisi



Cipherteks: `irinmxfaxosx`

Dekripsi: Bagi panjang dengan kunci (kolom)

(Contoh di atas, $12/4 = 3$ baris)

`I n f o`

`r m a s`

`i x x x`

Plainteks: `informasi`

Cipher Transposisi



Plainteks: `sains data ikopin`

Bagi menjadi blok-blok 8 huruf, jika < 8 tambah huruf palsu

1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
s	a	i	n	s	d	a	t	a	i	k	o	p	i	n	X

1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
n	s	d	a	t	s	a	i	o	p	i	n	x	a	i	K

Cipherteks: `nsdatσαιopinxaik`

Cipher Transposisi



Plainteks: `sains data ikopin`

Bagi menjadi blok-blok 8 huruf, jika < 8 tambah huruf palsu

1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
s	a	i	n	s	d	a	t	a	i	k	o	p	i	n	X

1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
n	s	d	a	t	s	a	i	o	p	i	n	x	a	i	K

Cipherteks: `nsdatsaiopinxaik`

Super-enkripsi

- Menggabungkan *cipher* substitusi dengan *cipher* transposisi.

Contoh: plainteks `hello world`

- Dienkripsi dengan caesar cipher menjadi `KHOOR ZRUOG`
- Kemudian hasil ini dienkripsi lagi dengan cipher transposisi (k-4)

`KHOO`

`RZRU`

`OGZZ`

- Cipherteks akhir adalah `KROHZGORZOUZ`

Beberapa Cipher Klasik



- Vigenere Cipher
- Playfair Cipher
- Affine Cipher
- Hill Cipher
- Enigma Cipher

Vigenere Cipher



- Termasuk ke dalam cipher abjad-majemuk
- Berhasil dipecahkan oleh Babbage dan Kasiski pada pertengahan abad 19
- Vigenere Cipher digunakan oleh Tentara Konfederasi pada Perang Sipil Amerika
- Perang Sipil terjadi setelah Vigenere Cipher berhasil dipecahkan.

Vigenere Cipher



- Menggunakan matriks Vigenere untuk melakukan enkripsi
- Setiap baris menyatakan huruf-huruf cipherteks yang diperoleh dengan Caesar Cipher
- Artinya, setiap baris i menggunakan pergeseran huruf alfabet sejauh i ke kanan

Vigenere Cipher

Plainteks

Kunci

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

Vigenere Cipher



- Kunci adalah string: $k = k_1 k_2 \dots k_m$
- k_i untuk $1 \leq i \leq m$ menyatakan huruf-huruf alfabet
- Jika panjang kunci lebih pendek daripada panjang plainteks, maka kunci diulang secara periodik
- Misal, panjang kunci $m=10$, maka 10 huruf pertama plainteks dienkripsi dengan kunci K , setiap huruf ke- i menggunakan kunci k_i

Contoh: kunci = univ

Plainteks: sainsdataikopin

Kunci: univunivunivuni

Vigenere Cipher

- Enkripsi dilakukan dengan mencari titik potong huruf plainteks dengan huruf kunci:
- Plainteks. : **sainsdataikopin**
Kunci : **univunivunivuni**
Cipherteks: **M**

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

Vigenere Cipher



- Hasil enkripsi seluruhnya:

Plainteks : `sainsdataikopin`

Kunci. : `univunivunivuni`

Chiperteks: `MNQIMQIOUVSJJVV`

- Pada dasarnya, setiap enkripsi huruf plainteks p_j adalah Caesar Cipher dengan kunci k_i yang berbeda-beda:

Enkripsi: $c_j = E(p_j) = (p_j + k_i) \bmod 26$

Dekripsi: $p_j = D(c_j) = (c_j - k_i) \bmod 26$

$(s + u) \bmod 26 = (18+20) \bmod 26 = 12 = M$

$(a + n) \bmod 26 = (0+13) \bmod 26 = 13 = N$

Vigenere Cipher



- Huruf plainteks yang sama tidak selalu dienkripsi menjadi cipher yang sama pula, bergantung huruf kunci yang digunakan.

Contoh: huruf plainteks T dapat dienkripsi menjadi L atau H

Huruf cipher V dapat merepresentasikan huruf plainteks H, I, dan X

- Hal ini merupakan karakteristik dari cipher abjad-majemuk: setiap huruf di cipherteks dapat memiliki kemungkinan banyak huruf plainteks
- Jika periode kunci diketahui dan tidak terlalu panjang, maka kunci dapat ditentukan dengan menulis program komputer untuk melakukan *exhaustive key search*

Affine Cipher



- Perluasan dari Caesar cipher
- Enkripsi: $C \equiv mP + b \pmod{n}$
- Dekripsi: $P \equiv m^{-1}(C - b) \pmod{n}$
- Kunci : m dan b

Keterangan:

- n ukuran alfabet
- m bulat yang relatif prima dengan n
- b jumlah pergeseran
- Caesar cipher adalah khusus dari affine cipher dengan $m = 1$
- m^{-1} adalah inversi $m \pmod{n}$, yaitu $m \cdot m^{-1} \equiv 1 \pmod{n}$

Affine Cipher

- Contoh:

Plainteks: krypto (10 17 8 15 19 14)

$n = 26$, $b = 10$, $m = 7$ (7 relatif prima dengan 26)

Enkripsi: $C \equiv 7P + 10 \pmod{26}$

$$p_1 = 10 \rightarrow c_1 \equiv 7 \cdot 10 + 10 \equiv 80 \equiv 2 \pmod{26} \quad (\text{huruf 'C'})$$

$$p_2 = 17 \rightarrow c_2 \equiv 7 \cdot 17 + 10 \equiv 129 \equiv 25 \pmod{26} \quad (\text{huruf 'Z'})$$

$$p_3 = 8 \rightarrow c_3 \equiv 7 \cdot 8 + 10 \equiv 66 \equiv 14 \pmod{26} \quad (\text{huruf 'O'})$$

$$p_4 = 15 \rightarrow c_4 \equiv 7 \cdot 15 + 10 \equiv 115 \equiv 11 \pmod{26} \quad (\text{huruf 'L'})$$

$$p_5 = 19 \rightarrow c_1 \equiv 7 \cdot 19 + 10 \equiv 143 \equiv 13 \pmod{26} \quad (\text{huruf 'N'})$$

$$p_6 = 14 \rightarrow c_1 \equiv 7 \cdot 14 + 10 \equiv 108 \equiv 4 \pmod{26} \quad (\text{huruf 'E'})$$

Cipherteks: CZOLNE

Affine Cipher

- Dekripsi:
 - Mula-mula hitung m^{-1} yaitu $7^{-1} \pmod{26}$ dengan memecahkan $7x \equiv 1 \pmod{26}$
 - Solusi: $x \equiv 15 \pmod{26}$ sebab $7.15 = 105 \equiv 1 \pmod{26}$
 - Jadi, $P \equiv 15(C - 10) \pmod{26}$
 - $c_1 = 2 \rightarrow p_1 \equiv 15 \cdot (2 - 10) = -120 \equiv 10 \pmod{26}$ (huruf 'k')
 - $c_2 = 25 \rightarrow p_2 \equiv 15 \cdot (25 - 10) = 225 \equiv 17 \pmod{26}$ (huruf 'r')
 - $c_3 = 14 \rightarrow p_3 \equiv 15 \cdot (14 - 10) = 60 \equiv 8 \pmod{26}$ (huruf 'i')
 - $c_4 = 11 \rightarrow p_4 \equiv 15 \cdot (11 - 10) = 15 \equiv 15 \pmod{26}$ (huruf 'p')
 - $c_5 = 13 \rightarrow p_5 \equiv 15 \cdot (13 - 10) = 45 \equiv 19 \pmod{26}$ (huruf 't')
 - $c_6 = 4 \rightarrow p_6 \equiv 15 \cdot (4 - 10) = -90 \equiv 14 \pmod{26}$ (huruf 'o')

Plainteks yang diungkap kembali: `kripto`

Affine Cipher



- Affine cipher. Tidak aman, karena kunci mudah ditemukan dengan *exhaustive search*,
- Sebab ada 25 pilihan b dan 12 nilai m yang relatif prima dengan 26 (yaitu 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, dan 25)
- Salah satu cara memperbesar faktor kerja untuk exhaustive key search: enkripsi tidak dilakukan terhadap individual, tetapi dalam blok huruf.
- Misal, pesan kriptografi dipecah menjadi kelompok 4-huruf:

krip togr afi

Ekuivalen dengan 10170815 19140617 000508

Affine Cipher



- Nilai terbesar yang dapat muncul untuk merepresentasikan blok: 25252525 (ZZZZ), maka 25252525 dapat digunakan sebagai modulus n .
- Nilai m yang relative prima dengan 25252525?, misal 21035433,
- B dipilih antara 1 sampai 25252525, misalnya 23210025

- Fungsi enkripsi menjadi:

$$C \equiv 21035433P + 23210025 \pmod{25252525}$$

- Fungsi dekripsi, setelah dihitung menjadi

$$P \equiv 5174971(C - 23210025) \pmod{25252525}$$

Affine Cipher

- Affine Cipher mudah diserang dengan *known-plaintext attack*.
- Misalkan kriptanalisis mempunyai dua buah plainteks, P_1 dan P_2 yang berkoresponden dengan cipherteks C_1 dan C_2
- Maka m dan b mudah dihitung dari kekongruenan simultan berikut ini:

$$C_1 \equiv mP_1 + b \pmod{n}$$

$$C_2 \equiv mP_2 + b \pmod{n}$$

Affine Cipher

- Contoh: Misalkan kriptanalisis menemukan
cipherteks C dan plainteks berkoresponden K
cipherteks E dan plainteks berkoresponden O .

- Kriptanalisis m dan n dari kekongruenan berikut:

$$2 \equiv 10m + b \pmod{26} \quad (i)$$

$$4 \equiv 14m + b \pmod{26} \quad (ii)$$

- Kurangkan (ii) dengan (i), menghasilkan

$$2 \equiv 4m \pmod{26} \quad (iii)$$

Solusi: $m = 7$

Substitusi $m = 7$ ke dalam (i),

$$2 \equiv 70 + b \pmod{26} \quad (iv)$$

Solusi: $b = 10$.

**SELAMAT
BELAJAR**