

**KEAMANAN INFORMASI**  
**ULANGAN TENGAH SEMESTER**



Dosen Pengampu Kelas C  
I Putu Sugi Almantara, S.TI., M.T.

Oleh:  
Resandy Prisdana  
(2205551050)

**PROGRAM STUDI TEKNOLOGI INFORMASI**  
**FAKULTAS TEKNIK**  
**UNIVERSITAS UDAYANA**  
**BALI**  
**2024**

## Soal

1. Apa yang dimaksud dengan keamanan informasi?
2. Apa yang dimaksud dengan Kriptografi dan Kriptanalisis? Jelaskan perbedaannya!
3. Menurut anda, mengapa keamanan informasi dibutuhkan?
4. Sebuah pesan rahasia (Bahasa Indonesia) sepanjang 35 karakter dienkripsi dengan super enkripsi. Pertama pesan dienkripsi dengan cipher transposisi berbasis kolom dengan ukuran kunci kolom 7, selanjutnya dienkripsi kembali dengan cipher substitusi homofonik (tabel homofon terlampir) yang menghasilkan cipherteks akhir adalah:

FYBUFY MLJOJO HEUAFA XPXPSI HEBUHE VTJOVT  
TWBUVS XPBUBU PNBUMML HEXPUA MLJOAF FYML

Dekripsilah cipherteks tersebut untuk mendapatkan kembali plainteksnya!

5. Sebuah pesan dienkripsi dengan *One Time Pad* (OTP). Chiperteks yang dihasilkan adalah:

NKNWWDOKQFBLZALAOCLHBJKT

Temukan dua buah kunci OTP yang berbeda sehingga dekripsi dengan OTP menghasilkan dua buah plainteks berbeda yang bermakna sebagai berikut:

- Kunci OTP ke-1 menghasilkan plainteks: PERGI KE PASAR MEMBELI BERAS
- Kunci OTP ke-2 menghasilkan plainteks: LANGIT BIRU TERBENTANG LUAS
- Gunakan kunci berikut untuk mendapatkan plainteks dari chiperteks diatas:  
UQHWELKZMNBDYWUIOPSHTYKM

## Jawaban

1. Keamanan informasi adalah upaya perlindungan dari berbagai macam ancaman baik secara fisik maupun secara nonfisik terhadap sarana teknologi informasi maupun sistem yang ada di dalamnya, untuk memastikan keberlanjutan bisnis, meminimalisir resiko bisnis dan meningkatkan investasi dan peluang bisnis. Dalam keamanan

informasi juga terdapat 3 komponen penting yang disebut juga dengan CIA Triangle, yaitu:

- ***Confidentiality (Rahasia)***

Berarti menjaga kerahasiaan informasi dengan melakukan pembatasan hak akses seseorang, dan contoh yang paling umum sering digunakan adalah dengan menggunakan enkripsi.

- ***Integrity (Keaslian)***

Berarti menjamin bahwa data atau informasi yang dimiliki terjaga keasliannya, tidak berubah tanpa adanya persetujuan atau pemberitahuan dari pemilik informasi. Komponen ini merujuk pada tingkat kepercayaan terhadap suatu informasi.

- ***Availability (Ketersediaan)***

Hal ini berhubungan dengan ketersediaan informasi ketika dibutuhkan. Artinya, informasi harus selalu tersedia saat dibutuhkan oleh pengguna dan dapat dengan cepat diakses untuk keperluan dari masing-masing *user*.

2. **Kriptografi** adalah ilmu dan teknik untuk mengamankan informasi dengan menyandikan umumnya dengan mengenkripsi data menjadi bentuk tersandi atau disebut dengan *ciphertext* sehingga hanya pihak yang berwenang dapat membaca dan memahami isinya. Proses ini melibatkan penggunaan kunci rahasia atau algoritma tertentu untuk mengubah data asli (*plaintext*) menjadi data tersandi (*chipertext*). Dengan kata lain, kriptografi mengacu pada ilmu dan seni untuk mendesain penyandian.

**Kriptanalisis** adalah ilmu dan praktik untuk memecahkan atau memecah kode terenkripsi tanpa memiliki kunci rahasia atau pengetahuan tentang algoritma enkripsi yang digunakan. Kriptanalisis mengubah *chipertext* menjadi *plaintext*. Dengan kata lain, kriptanalisis mengacu pada ilmu dan seni untuk memecahkan penyandian.

Perbedaan utama antara kriptografi dan kriptanalisis terletak pada tujuannya. Kriptografi bertujuan untuk melindungi data dengan menyandikannya, sementara kriptanalisis bertujuan untuk memecahkan data tersandi tersebut tanpa kunci yang valid.

**Perbedaan utama antara kriptografi dan kriptanalisis** terletak pada tujuannya. Kriptografi bertujuan untuk melindungi data dengan menyandikannya, dengan

mengubah *plaintext* menjadi *chipertext*, sedangkan kriptanalisis bertujuan untuk memecahkan data tersandi tersebut tanpa kunci yang valid, dengan mengubah *chipertext* menjadi *plaintext*.

3. Menurut saya keamanan informasi dibutuhkan, karena tidak semua informasi itu dapat disebarluaskan. Informasi yang tidak dapat disebarluaskan itu contohnya seperti, informasi perusahaan yang memiliki tingkat kepentingan yang tinggi, yang mana bila disebar secara umum maka informasi tersebut dapat mempengaruhi keseimbangan perusahaan tersebut. Misalnya seperti informasi atau data pada perusahaan yang akan digunakan untuk menentukan strategi bisnis kedepannya. Jika data itu bocor ke luar perusahaan dan ada kompetitor yang mengetahui hal tersebut, maka kompetitor tersebut bisa saja mengambil langkah ataupun strategi yang akhirnya berdampak pada perusahaan tersebut.

Keamanan informasi juga diperlukan untuk menjaga informasi pribadi yang dirasa sensitif atau merupakan privasi pribadi. Jika terdapat informasi penting mengenai diri kita, maka bisa saja terdapat oknum yang memanfaatkan hal tersebut. Misalnya saja jika kita mengunggah informasi pribadi seperti foto KTP pada media sosial, maka bisa saja terdapat oknum yang akan memanfaatkan hal tersebut untuk keperluan pribadinya yang merugikan kita. Bisa saja KTP tersebut dijadikan jaminan atau syarat salah satu pinjaman *online* tanpa kita ketahui.

Jadi, dengan mengetahui pentingnya menjaga informasi kita bisa lebih waspada terhadap sesuatu yang berkaitan dengan informasi yang ada.

4. Diberikan *chipertext*:

FYBUFY MLJOJO HEUAFA XPXPSI HEBUHE VTJOVT  
TWBUVS XPBUBU PNBUMML HEXPUA MLJOAF FYML

FY = B

BU = A

FY = B

ML = L

JO = L/E

JO = L/E

HE = H

UA = I  
FA = U  
XP = R  
XP = R  
SI = T  
HE = H  
BU = A  
HE = H  
VT = D  
JO = L/E  
VT = D  
TW = G  
BU = A  
VS = O  
XP = R  
BU = A  
BU = A  
PN = S  
BU = A  
ML = L  
HE = H  
XP = R  
UA = I  
ML = L  
JO = L/E  
FA = U  
FY = B  
ML = L

Lalu disusun menjadi 7 baris

BABLE  
EHIUR  
RTHAH  
DEDGA

ORAAS

ALHRI

LEUBL

Dikarenakan JO yang paling memungkinkan berdasarkan tabel pada lampiran adalah E, maka yang digunakan adalah E. Maka didapat *plaintext* jika disusun secara vertikal, yaitu:

**BERDOALAH TERLEBIH DAHULU AGAR BERHASIL**

## 5. One-Time Pad (OTP)

Diberikan chipertext:

NKNWWDOKQFBLZALAOCLHBJKT

- Temukan kunci yang menghasilkan *plaintext*

PERGI KE PASAR MEMBELI BERAS

Dengan menggunakan cara OTP digunakan rumus untuk mendeskripsikan:

$$p = (c + k) \bmod 26$$

Dengan menggunakan acuan:

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

$$P1 = (N - P) \bmod 26 = (13 - 15) \bmod 26 = -2 \bmod 26 = 24, 24 = 'Y'$$

$$P2 = (K - E) \bmod 26 = (10 - 4) \bmod 26 = 6 \bmod 26 = 6, 6 = 'G'$$

$$P3 = (N - R) \bmod 26 = (13 - 17) \bmod 26 = -4 \bmod 26 = 22, 22 = 'W'$$

$$P4 = (W - G) \bmod 26 = (22 - 6) \bmod 26 = 16 \bmod 26 = 16, 16 = 'Q'$$

$$P5 = (W - I) \bmod 26 = (22 - 8) \bmod 26 = 14 \bmod 26 = 14, 14 = 'O'$$

$$P6 = (D - K) \bmod 26 = (3 - 10) \bmod 26 = -7 \bmod 26 = 19, 19 = 'T'$$

$$P7 = (O - E) \bmod 26 = (14 - 4) \bmod 26 = 10 \bmod 26 = 10, 10 = 'K'$$

$$P8 = (K - P) \bmod 26 = (10 - 15) \bmod 26 = -5 \bmod 26 = 21, 21 = 'V'$$

$$P9 = (Q - A) \bmod 26 = (16 - 0) \bmod 26 = 16 \bmod 26 = 16, 16 = 'Q'$$

$$P10 = (F - S) \bmod 26 = (5 - 18) \bmod 26 = -13 \bmod 26 = 13, 13 = 'N'$$

$P11 = (B - A) \bmod 26 = (1 - 0) \bmod 26 = 1 \bmod 26 = 1, 1 = \text{'B'}$   
 $P12 = (L - R) \bmod 26 = (11 - 17) \bmod 26 = -6 \bmod 26 = 20, 20 = \text{'U'}$   
 $P13 = (Z - M) \bmod 26 = (25 - 12) \bmod 26 = 13 \bmod 26 = 13, 13 = \text{'N'}$   
 $P14 = (A - E) \bmod 26 = (0 - 4) \bmod 26 = -4 \bmod 26 = 22, 22 = \text{'W'}$   
 $P15 = (L - M) \bmod 26 = (11 - 12) \bmod 26 = -1 \bmod 26 = 25, 25 = \text{'Z'}$   
 $P16 = (A - B) \bmod 26 = (0 - 1) \bmod 26 = -1 \bmod 26 = 25, 25 = \text{'Z'}$   
 $P17 = (O - E) \bmod 26 = (14 - 4) \bmod 26 = 10 \bmod 26 = 10, 10 = \text{'K'}$   
 $P18 = (C - L) \bmod 26 = (2 - 11) \bmod 26 = -9 \bmod 26 = 17, 17 = \text{'R'}$   
 $P19 = (L - I) \bmod 26 = (11 - 8) \bmod 26 = 3 \bmod 26 = 3, 3 = \text{'D'}$   
 $P20 = (H - B) \bmod 26 = (7 - 1) \bmod 26 = 8 \bmod 26 = 8, 8 = \text{'I'}$   
 $P21 = (B - E) \bmod 26 = (1 - 4) \bmod 26 = -3 \bmod 26 = 23, 23 = \text{'X'}$   
 $P22 = (J - R) \bmod 26 = (9 - 17) \bmod 26 = -8 \bmod 26 = 18, 18 = \text{'S'}$   
 $P23 = (K - A) \bmod 26 = (10 - 0) \bmod 26 = 10 \bmod 26 = 10, 10 = \text{'K'}$   
 $P24 = (T - S) \bmod 26 = (19 - 18) \bmod 26 = 1 \bmod 26 = 1, 1 = \text{'B'}$

Jadi kata kunci yang didapatkan adalah:

**YGWQOTKVQNBUNWZZKRDIXSKB**

- Temukan kunci yang menghasilkan *plaintext*

LANGIT BIRU TERBENTANG LUAS

Dengan menggunakan cara OTP digunakan rumus untu mendeskripsikan:

**$p = (c - k) \bmod 26$**

Dengan menggunakan acuan:

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

$P1 = (N - L) \bmod 26 = (13 - 11) \bmod 26 = 2 \bmod 26 = 2, 2 = \text{'C'}$   
 $P2 = (K - A) \bmod 26 = (10 - 0) \bmod 26 = 10 \bmod 26 = 10, 10 = \text{'K'}$   
 $P3 = (N - N) \bmod 26 = (13 - 13) \bmod 26 = 0 \bmod 26 = 0, 0 = \text{'A'}$   
 $P4 = (W - G) \bmod 26 = (22 - 6) \bmod 26 = 16 \bmod 26 = 16, 16 = \text{'Q'}$   
 $P5 = (W - I) \bmod 26 = (22 - 8) \bmod 26 = 14 \bmod 26 = 14, 14 = \text{'O'}$

$P6 = (D - T) \bmod 26 = (3 - 19) \bmod 26 = -16 \bmod 26 = 10, 10 = \text{'K'}$   
 $P7 = (O - B) \bmod 26 = (14 - 1) \bmod 26 = 13 \bmod 26 = 13, 13 = \text{'N'}$   
 $P8 = (K - I) \bmod 26 = (10 - 8) \bmod 26 = 2 \bmod 26 = 2, 2 = \text{'C'}$   
 $P9 = (Q - R) \bmod 26 = (16 - 17) \bmod 26 = -1 \bmod 26 = 25, 25 = \text{'Z'}$   
 $P10 = (F - U) \bmod 26 = (5 - 20) \bmod 26 = -15 \bmod 26 = 11, 11 = \text{'L'}$   
 $P11 = (B - T) \bmod 26 = (1 - 19) \bmod 26 = -18 \bmod 26 = 8, 8 = \text{'I'}$   
 $P12 = (L - E) \bmod 26 = (11 - 4) \bmod 26 = 7 \bmod 26 = 7, 7 = \text{'H'}$   
 $P13 = (Z - R) \bmod 26 = (25 - 17) \bmod 26 = 8 \bmod 26 = 8, 8 = \text{'I'}$   
 $P14 = (A - B) \bmod 26 = (0 - 1) \bmod 26 = -1 \bmod 26 = 25, 25 = \text{'Z'}$   
 $P15 = (L - E) \bmod 26 = (11 - 4) \bmod 26 = 7 \bmod 26 = 7, 7 = \text{'H'}$   
 $P16 = (A - N) \bmod 26 = (0 - 13) \bmod 26 = -13 \bmod 26 = 13, 13 = \text{'N'}$   
 $P17 = (O - T) \bmod 26 = (14 - 19) \bmod 26 = -5 \bmod 26 = 21, 21 = \text{'V'}$   
 $P18 = (C - A) \bmod 26 = (2 - 0) \bmod 26 = 2 \bmod 26 = 2, 2 = \text{'B'}$   
 $P19 = (L - N) \bmod 26 = (11 - 13) \bmod 26 = -2 \bmod 26 = 24, 24 = \text{'Y'}$   
 $P20 = (H - G) \bmod 26 = (7 - 6) \bmod 26 = 1 \bmod 26 = 1, 1 = \text{'B'}$   
 $P21 = (B - L) \bmod 26 = (1 - 11) \bmod 26 = -10 \bmod 26 = 16, 16 = \text{'Q'}$   
 $P22 = (J - U) \bmod 26 = (9 - 20) \bmod 26 = -11 \bmod 26 = 15, 15 = \text{'P'}$   
 $P23 = (K - A) \bmod 26 = (10 - 0) \bmod 26 = 10 \bmod 26 = 10, 10 = \text{'K'}$   
 $P24 = (T - S) \bmod 26 = (19 - 18) \bmod 26 = 1 \bmod 26 = 1, 1 = \text{'B'}$

Jadi kata kunci yang didapatkan adalah:

**CKAQOKNCZLIHIZHNVBYBQPKB**

- Temukan plaintext dengan menggunakan kunci:

UQHWELKZMNB DYWUIOPSH TYKM

Dengan menggunakan cara OTP digunakan rumus untuk mendeskripsikan:

$$p = (c + k) \bmod 26$$

Dengan menggunakan acuan:

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



$P1 = (N - U) \bmod 26 = (13 - 20) \bmod 26 = -7 \bmod 26 = 19, 19 = 'T'$   
 $P2 = (K - Q) \bmod 26 = (10 - 16) \bmod 26 = -6 \bmod 26 = 20, 20 = 'U'$   
 $P3 = (N - H) \bmod 26 = (13 - 7) \bmod 26 = 6 \bmod 26 = 6, 6 = 'G'$   
 $P4 = (W - W) \bmod 26 = (22 - 22) \bmod 26 = 0 \bmod 26 = 0, 0 = 'A'$   
 $P5 = (W - E) \bmod 26 = (22 - 4) \bmod 26 = 18 \bmod 26 = 18, 18 = 'S'$   
 $P6 = (D - L) \bmod 26 = (3 - 11) \bmod 26 = -8 \bmod 26 = 18, 18 = 'S'$   
 $P7 = (O - K) \bmod 26 = (14 - 10) \bmod 26 = 4 \bmod 26 = 4, 4 = 'E'$   
 $P8 = (K - Z) \bmod 26 = (10 - 25) \bmod 26 = -15 \bmod 26 = 11, 11 = 'L'$   
 $P9 = (Q - M) \bmod 26 = (16 - 12) \bmod 26 = 4 \bmod 26 = 4, 4 = 'E'$   
 $P10 = (F - N) \bmod 26 = (5 - 13) \bmod 26 = -8 \bmod 26 = 18, 18 = 'S'$   
 $P11 = (B - B) \bmod 26 = (1 - 1) \bmod 26 = 0 \bmod 26 = 0, 0 = 'A'$   
 $P12 = (L - D) \bmod 26 = (11 - 3) \bmod 26 = 8 \bmod 26 = 8, 8 = 'I'$   
 $P13 = (Z - Y) \bmod 26 = (25 - 24) \bmod 26 = 1 \bmod 26 = 1, 1 = 'B'$   
 $P14 = (A - W) \bmod 26 = (0 - 22) \bmod 26 = -22 \bmod 26 = 4, 4 = 'E'$   
 $P15 = (L - U) \bmod 26 = (11 - 20) \bmod 26 = -9 \bmod 26 = 17, 17 = 'R'$   
 $P16 = (A - I) \bmod 26 = (0 - 8) \bmod 26 = -8 \bmod 26 = 18, 18 = 'S'$   
 $P17 = (O - O) \bmod 26 = (14 - 14) \bmod 26 = 0 \bmod 26 = 0, 0 = 'A'$   
 $P18 = (C - P) \bmod 26 = (2 - 15) \bmod 26 = -13 \bmod 26 = 13, 13 = 'N'$   
 $P19 = (L - S) \bmod 26 = (11 - 18) \bmod 26 = -7 \bmod 26 = 19, 19 = 'T'$   
 $P20 = (H - H) \bmod 26 = (7 - 7) \bmod 26 = 0 \bmod 26 = 0, 0 = 'A'$   
 $P21 = (B - T) \bmod 26 = (1 - 19) \bmod 26 = -18 \bmod 26 = 8, 8 = 'I'$   
 $P22 = (J - Y) \bmod 26 = (9 - 24) \bmod 26 = -15 \bmod 26 = 11, 11 = 'L'$   
 $P23 = (K - K) \bmod 26 = (10 - 10) \bmod 26 = 0 \bmod 26 = 0, 0 = 'A'$   
 $P24 = (T - M) \bmod 26 = (19 - 12) \bmod 26 = 7 \bmod 26 = 7, 7 = 'H'$

Jadi kata kunci yang didapatkan adalah:

**TUGASSELESAIBERSANTAILAH** disempurnakan menajdi,  
**TUGAS SELESAI BERSANTAILAH**