# SYMMETRIC CIPHERS PART 1
# PENGAYAAN

--Dr. Mike Yuliana--

Mata Kuliah : Keamanan Jaringan

*Politeknik Elektronika Negeri Surabaya (PENS)*

# Outline

- Multiplicative Invers Matrik
- Pengayaan Caesar Cipher

# Multiplicative Invers Matrik

Mekanisme Pencarian invers matrik

- Menentukan determinan matrik
- Menentukan invers modulo

$$\det^{-1} \bmod 26$$

**det. x=1 mod 26**

**det. x= 1+ 26 k**
**x=(1+26.k)/det, k=0,1,...**

x harus bilangan bulat

- Menentukan invers modulo determinan

$$misal\ k = \begin{bmatrix} a & b \\ c & d \end{bmatrix}\ maka\ k^{-1} = (\ x.\ \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}\ ) \bmod 26$$

# Caesar Cipher (1)

Substitusi kode yang pertama dalam dunia penyandian terjadi pada pemerintah Julius Caesar yang dikenal dengan kode Kaisar, dengan mengganti posisi huruf awal dari alfabet atau disebut juga dengan algoritma ROT3.

**Caesar Cipher (ROT3)**

| Plain Text | Encoded Text |
|---|---|
| ABC | DEF |
| Hello | Khoor |
| Attack | Dwwdfn |

# Caesar Cipher (2)

Kemudian pada perkembangannya algoritma kode caesar memberikan suatu gagasan baru untuk menggunakan kunci lain yang disebut *polyalphabetic*. Kunci bisa jadi nama, alamat atau apa saja yang diinginkan oleh pengirim pesan.

Satu Kunci

K1

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

Plainteks : KENAIKAN HARGA BBM MEMBUAT RAKYAT KECIL MENDERITA

Kunci : DONY ARIYUS

Proses :

| Plainteks | K | E |
|---|---|---|
| Kunci | C | A |

Dan seterusnya

Cipherteks : CAGDSCDGUDLIDOOFFAFOQDPLDCXDPCANSEFAGYAL SPD

# Caesar Cipher (3)

K1

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

K2

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

Plainteks : KENAIKAN HARGA BBM MEMBUAT RAKYAT KECIL

MENDERITA

Kunci 1 : DONY ARIYUS

Kunci 2 : CHILDVANIA

Proses :

| Plainteks | K | E |
|---|---|---|
| Kunci 1 | C | A |
| Kunci 2 | I | C |

Dan seterusnya

Dua Kunci

Ciphertext?

# Caesar Cipher (4)

Tiga Kunci

Plainteks : KENAIKAN HARGA BBM MEMBUAT RAKYAT KECIL MENDERITA

Kunci 1 : DONY ARIYUS

Kunci 2 : CHILDVANIA

Kunci 3 : MUTHIA CITRA

Proses :

| Plainteks | K | E |
|---|---|---|
| Kunci 1 | C | A |
| Kunci 2 | I | C |
| Kunci 3 | B | T |

Dan seterusnya

Ciphertext?

# Caesar Cipher (5)

a. Blok

Metode untuk mengenkripsi dengan menggunakan blok adalah dengan membagi jumlah teks asli menjadi blok-blok yang ditentukan, tergantung dari keinginan pengirim pesan.

Teks asli: BANJIR MERENDAM JAKARTA HARGA BAHAN POKOK NAIK.

Teks asli di atas dibagi menjadi 7 blok. Setiap blok berisi 6 karakter. Karena blok yang ketujuh tidak mencukupi maka ditambah dengan karakter "X" atau karakter lain yang diinginkan.

| BANJIR | MEREND | AMJAKA | RTAHAR | GAHABA | NPOKOK |
|---|---|---|---|---|---|
| Blok 1 | Blok 2 | Blok 3 | Blok 4 | Blok 5 | Blok 6 |

| NAIKXX |
|---|
| Blok 7 |

Kunci 1: DONY ARIYUS

Kunci 2: YOGYAKARTA

Kunci 3: KRIPTOGRAFI

# Caesar Cipher (6)

K1

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

K2

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

K3

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

Dengan aturan K1 digunakan pada blok pertama, K2 blok kedua, K3 blok ketiga, dan seterusnya. Atau juga bisa dipakai untuk mengenkripsi dua blok sekaligus.

Ciphertext?

# Caesar Cipher (7)

b. Karakter

Metode ini menggunakan pendistribusian perkarakter, hampir sama dengan metode blok. Metode ini enkripsi dan dekripsi sama.

Contoh:

Teks asli: BANJIR MERENDAM JAKARTA HARGA BAHAN POKOK NAIK.

Kunci 1: DONY ARIYUS

Kunci 2: YOGYAKARTA

Kunci 3: KRIPTOGRAFI

K1

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

K2

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

K3

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

Ciphertext?