



**KELOMPOK 5**

# CAESAR CIPHER





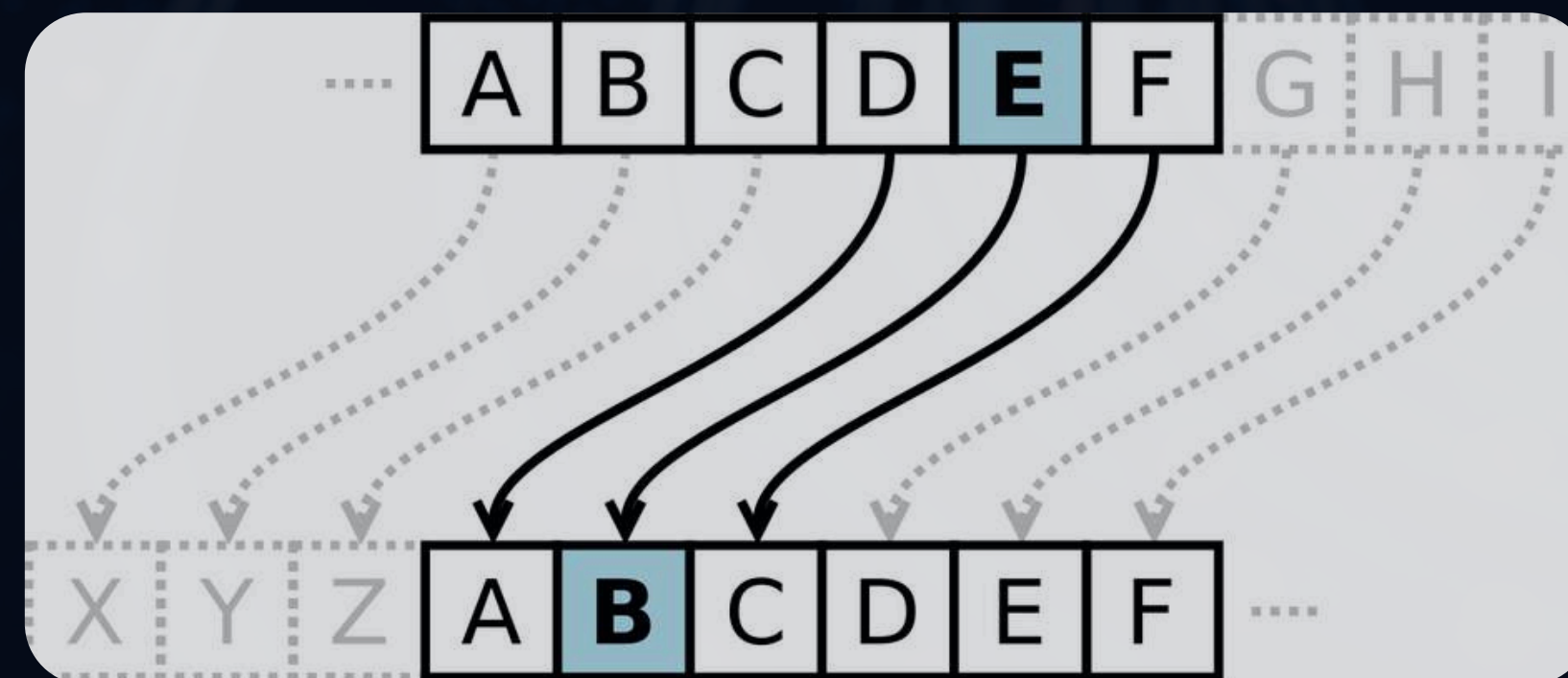
# ANGGOTA :

- Muhamad Fahreza
- Muhammad Fahmi P
- Muhammad Yalqa
- Wibi Nugraha
- Yoga Triansyah



# CAESAR CIPHER

Caesar cipher adalah salah satu metode enkripsi teks yang paling sederhana dan kuno. Metode ini ditemukan oleh Julius Caesar untuk mengirimkan pesan rahasia kepada tentaranya. Caesar cipher bekerja dengan menggeser setiap huruf dalam teks asli (plaintext) sejauh jumlah tertentu dalam alfabet untuk menghasilkan teks terenkripsi (ciphertext).







### Table Alphabet

Hanya bekerja pada huruf alfabet (A-Z atau a-z), biasanya dengan indeks 0–25.

Rumus Encrypt & Decrypt:

- $C = (P + k) \bmod 26$
- $P = (C - k) \bmod 26$



### Table Ascii

Menggunakan kode ASCII untuk setiap karakter. Pergeseran dilakukan dengan menambahkan nilai shift pada kode ASCII.

Rumus Encrypt & decrypt :

- $C = (P + k) \bmod 256$
- $P = (C - k) \bmod 256$

# 2 TIPE FUNCTION HASH TABLE



# STUDY CASE

Kami membuat dan menerima soal yang berkaitan dengan caesar cipher dan membuat penyelesaiannya



# SOAL KELOMPOK 7

## Diberikan soal berikut

Ciphertext :

key clue : segitiga sama sisi





# PENYELESAIAN

## Analisi clue

Diberikan gambar segitiga sama sisi, asumsi kami key nya adalah 3 bisa ke kanan atau ke kiri.

## Decrypt Cipher

Kami coba geser setiap cipher nya ke kanan dan juga ke kiri mengacu ke table ascii, karena cipher terdapat angka sudah pasti ini mengacu ke table ascii.

## Hasil Akhir

Plaintext dari cipher yang diberikan adalah :



# SOAL KELOMPOK 5

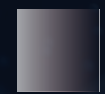
## Diberikan soal berikut

key4key = our group  
key = -/f\i\\I\\_`^^dd  
cipher = \h^dnX\_bWb





# PENYELESAIAN



## Mendecrypt key pertama

Dari clue 'key = group' maka, key 4 key adalah caesar cipher yang digeser sebanyak 5 kali. Ketika dicoba geser ke kiri, hasilnya 22kananascii



## Mendecrypt cipher ke 2

Cipher ke 2 adalah cipher yang asli, dimana dari hasil key yang sebelumnya diketahui bahwa cipher ini digeser sebanyak 22 kali ke kanan di table ascii,



## Hasil Akhir

Dari kedua langkah sebelumnya diketahui plain text nya yaitu :  
**FRHNBILAL**



**KELOMPOK 5**



# TERIMA KASIH