

Kelompok 9:

- Edrick Saputra Lionard (0806022310013)
- Excel Marcello (0806022310029)
- Tiffany Tjandinegara (080602231027)

## Soal

Create a Cryptography system in Python with rule encryption as :

$$((((A \wedge B1) \wedge B2) \wedge B3) \wedge B4) \rightarrow C$$

A is the plaintext, C is the ciphertext, and B1, B2, B3, B4 are binary keys generated from a single secret\_key.

1. You must create the appropriate Decryption according to the encryption rule
2. You are free to define your function to get the values B1, B2, B3, B4
3. Give the name of your Cryptography system
4. Give an explanation of your Cryptography system and an example of how your Cryptography system works from encryption to decryption process in single pdf file.

## Jawaban

Berikut adalah langkah-langkah enkripsi dan dekripsi yang sudah diringkas dan diperjelas, termasuk representasi biner untuk setiap nilai:

### 1. Inisialisasi dan Persiapan

- **Plaintext (A):** Data asli yang ingin kita lindungi adalah huruf "Y".
- **Secret Key:** "Makassar".

### 2. Konversi Plaintext ke Biner

- **Plaintext:** "Y"
- **Nilai ASCII:** 89
- **Biner:** 01011001

### 3. Menghasilkan Kunci

Dari secret key "Makassar", kita menghasilkan empat kunci (B1, B2, B3, B4):

- **B1:** Karakter pertama 'M' (ASCII 77) → **Biner:** 01001101
- **B2:** Karakter kedua 'a' (ASCII 97) → **Biner:** 01100001
- **B3:** Karakter ketiga 'k' (ASCII 107) → **Biner:** 01101011
- **B4:** Karakter keempat 'a' (ASCII 97) → **Biner:** 01100001

#### 4. Proses Enkripsi

Proses enkripsi dilakukan dengan langkah-langkah berikut:

##### Langkah 1: XOR dengan B1

$$C_1 = A \oplus B_1$$

- **Hitung:**
  - A = 89 (biner: 01011001)
  - B1 = 77 (biner: 01001101)
- **Operasi XOR:**
  - $C_1 = 01011001 \oplus 01001101 = 00010100$
- **Hasil:**  $C_1 = 20$

##### Langkah 2: XOR dengan B2

$$C_2 = C_1 \oplus B_2$$

- **Hitung:**
  - $C_1 = 20$  (biner: 00010100)
  - $B_2 = 97$  (biner: 01100001)
- **Operasi XOR:**
  - $C_2 = 00010100 \oplus 01100001 = 01110101$
- **Hasil:**  $C_2 = 117$

##### Langkah 3: XOR dengan B3

$$C_3 = C_2 \oplus B_3$$

- **Hitung:**
  - $C_2 = 117$  (biner: 01110101)
  - $B_3 = 107$  (biner: 01101011)
- **Operasi XOR:**
  - $C_3 = 01110101 \oplus 01101011 = 00011110$
- **Hasil:**  $C_3 = 30$

##### Langkah 4: XOR dengan B4

$$C = C_3 \oplus B_4$$

- **Hitung:**
  - $C_3 = 30$  (biner: 00011110)

- $B_4=97$  (biner: 01100001)
- **Operasi XOR:**
  - $C=00011110 \oplus 01100001 = 01111111$  \
- **Hasil akhir dari enkripsi:  $C=127$**

## 5. Proses Dekripsi

Dekripsi adalah kebalikan dari proses enkripsi. Kita menggunakan ciphertext untuk mendapatkan kembali plaintext.

### Langkah 1: XOR dengan $B_4$

$$A_1 = C \oplus B_4$$

- **Hitung:**
  - $C=127$  (biner: 01111111)
  - $B_4=97$  (biner: 01100001)
- **Operasi XOR:**
  - $A_1 = 01111111 \oplus 01100001 = 00011110$
- **Hasil:  $A_1=30$**

### Langkah 2: XOR dengan $B_3$

$$A_2 = A_1 \oplus B_3$$

- **Hitung:**
  - $A_1=30$  (biner: 00011110)
  - $B_3=107$  (biner: 01101011)
- **Operasi XOR:**
  - $A_2 = 00011110 \oplus 01101011 = 01110101$
- **Hasil:  $A_2=117$**

### Langkah 3: XOR dengan $B_2$

$$A_3 = A_2 \oplus B_2$$

- **Hitung:**
  - $A_2=117$  (biner: 01110101)
  - $B_2=97$  (biner: 01100001)
- **Operasi XOR:**
  - $A_3 = 01110101 \oplus 01100001 = 00010100$
- **Hasil:  $A_3=20$**

### Langkah 4: XOR dengan $B_1$

$$A = A_3 \oplus B_1$$

- **Hitung:**
  - $A_3=20$  (biner: 00010100)
  - $B_1=77$  (biner: 01001101)

- **Operasi XOR:**
  - $A = 00010100 \oplus 01001101 = 01011001$
- **Hasil akhir dari dekripsi:** A = 89 (nilai ASCII untuk huruf "Y").

## Kesimpulan

- **Ciphertext:** 127 (biner: 01111111)
- **Plaintext:** "Y" (ASCII: 89, biner: 01011001)

Proses enkripsi dan dekripsi ini menunjukkan bagaimana kunci dihasilkan dari secret key dan digunakan untuk melindungi data. Jika ada yang perlu diperjelas atau ditambahkan, silakan beri tahu!