

NAMA : SITTI NUR HALIZA

NIM : E1E120051

KELAS : GANJIL

## MATA KULIAH KRIPTOGRAFI

### Tugas 2

1. Kerjakan KSA dan PRGA dengan kunci 'saputra1' dan plaintext '2(3 angka terakhir NIM)'.  
Tulis tangan!
2. Buat Program python dengan algoritma RC4 (untuk kelas ganjil) bagian sub-proses KSA!

### JAWAB

#### 1. Sub-proses Key-Scheduling Algorithm (KSA)

Nama : Sitti Nur Haliza      Kelas : Ganjil  
NIM : E1E120051

Kriptografi | Tugas 2

1.  $\Delta$  Key - Scheduling Algorithm (KSA)

Array  $S = [0, 1, 2, 3, 4, 5, 6, 7, \dots, 250, 251, 252, 253, 254, 255]$   
 $K = \text{saputra1} \rightarrow \text{length} = 8$

• Iterasi pertama  
 $j = 0 \quad i = 0$   
$$j = (j + S[i] + K[i \bmod \text{length}(K)]) \bmod 256$$
$$j = (0 + S[0] + K[0 \bmod 8]) \bmod 256$$
$$j = (0 + 0 + K[0] \bmod 256) \quad \boxed{K[0] = 9 = 115}$$
$$j = (0 + 115) \bmod 256$$
$$j = 115$$
$$\text{swap}(S[i], S[j]) \rightarrow S[0] \leftrightarrow S[115]$$
$$S = [115, 1, 2, 3, \dots, 113, 114, 0, 116, \dots, 254, 255]$$

• Iterasi Kedua  
 $j = 115 \quad i = 1$ 
$$j = (j + S[i] + K[i \bmod \text{length}(K)]) \bmod 256$$
$$j = (115 + 1 + 97) \bmod 256 \quad \boxed{K[1] = a = 97}$$
$$j = 213 \bmod 256$$
$$j = 213$$
$$\text{swap}(S[i], S[j]) \rightarrow S[1] \leftrightarrow S[213]$$
$$S = [115, 213, 2, 3, \dots, 113, 114, 0, 116, \dots, 212, 1, 214, \dots, 254, 255]$$

• Iterasi Ketiga  
 $j = 213 \quad i = 2$ 
$$j = (j + S[i] + K[i \bmod \text{length}(K)]) \bmod 256$$
$$j = (213 + 2 + 112) \bmod 256 \quad \boxed{K[2] = p = 112}$$
$$j = (327) \bmod 256$$
$$j = 71$$
$$\text{swap}(S[i], S[j]) \rightarrow S[2] \leftrightarrow S[71]$$
$$S = [115, 213, 71, 3, 4, 5, \dots, 70, 2, 72, 73, \dots, 113, 114, 0, 116, \dots, 212, 1, 214, 215, \dots, 254, 255]$$

• Iterasi keempat

$$j = 71 \quad i = 3$$

$$j = (j + s[i] + k[i \bmod \text{length}(k)]) \bmod 256$$

$$j = (71 + 3 + 117) \bmod 256 \quad [k[3] = u = 117]$$

$$j = 191 \bmod 256$$

$$j = 191$$

$$\text{swap}(s[i], s[j]) \rightarrow s[3] \leftrightarrow s[191]$$

$$s = [115, 213, 71, 191, 4, 5, \dots, 70, 2, 72, 73, \dots, 113, 114, 0, 116, 117, \dots, 190, 3, 192, \dots, 212, 1, 214, 215, \dots, 254, 255]$$

• Iterasi kelima

$$j = 191 \quad i = 4$$

$$j = (j + s[i] + k[i \bmod \text{length}(k)]) \bmod 256$$

$$j = (191 + 4 + 116) \bmod 256 \quad [k[4] = t = 116]$$

$$j = (311) \bmod 256$$

$$j = 55$$

$$\text{swap}(s[i], s[j]) \rightarrow s[4] \leftrightarrow s[55]$$

$$s = [115, 213, 71, 191, 55, 5, 6, \dots, 54, 4, 56, \dots, 70, 2, 72, 73, \dots, 113, 114, 0, 116, \dots, 190, 3, 192, \dots, 212, 1, 214, 215, \dots, 254, 255]$$

• Iterasi keenam

$$j = 55 \quad i = 5$$

$$j = (j + s[i] + k[i \bmod \text{length}(k)]) \bmod 256$$

$$j = (55 + 5 + 114) \bmod 256 \quad [k[5] = r = 114]$$

$$j = 174 \bmod 256$$

$$j = 174$$

$$\text{swap}(s[i], s[j]) \rightarrow s[5] \leftrightarrow s[174]$$

$$s = [115, 213, 71, 191, 55, 174, 6, 7, \dots, 54, 4, 56, \dots, 70, 2, 72, 73, \dots, 113, 114, 0, 116, \dots, 173, 5, 175, \dots, 190, 3, 192, \dots, 212, 1, 214, 215, \dots, 254, 255]$$

• Iterasi ketujuh

$$j = 174 \quad i = 6$$

$$j = (j + s[i] + k[i \bmod \text{length}(k)]) \bmod 256$$

$$j = (174 + 6 + 97) \bmod 256 \quad [k[6] = a = 97]$$

$$j = (277) \bmod 256$$

$$j = 21$$

$$\text{swap}(s[i], s[j]) \rightarrow s[6] \leftrightarrow s[21]$$

$$s = [115, 213, 71, 191, 55, 174, 21, 7, \dots, 19, 20, 6, 22, \dots, 54, 4, 56, \dots, 70, 2, 72, 73, \dots, 113, 114, 0, 116, \dots, 173, 5, 175, \dots, 190, 3, 192, \dots, 212, 1, 214, 215, \dots, 254, 255]$$

• Iterasi kedelapan

$$j = 21 \quad i = 7$$

$$j = (j + s[i] + k[i \bmod \text{length}(k)]) \bmod 256$$

$$j = (21 + 7 + 49) \bmod 256 \quad \boxed{k[7] = 1 = 49}$$

$$j = 77 \bmod 256$$

$$j = 77$$

$$\text{swap}(s[i], s[j]) \rightarrow s[7] \leftrightarrow s[77]$$

$$s = [115, 213, 71, 191, 55, 174, 21, 77, 8, 9, \dots, 19, 20, 6, 22, \dots, 54, 4, 56, \dots, 70, 2, 72, 73, \dots, 76, 7, 78, \dots, 113, 114, 0, 116, \dots, 173, 5, 175, \dots, 190, 3, 192, \dots, 212, 1, 214, \dots, 254, 255]$$

### Sub-proses Pseudo-Random Generation Algorithm (PRGA)

2 - Pseudo-random-generation algorithm (PRGA)

$$\text{NIM} = \text{E1E120051}$$

$$P = 2051 \quad (4 \text{ iterasi})$$

$$\text{Array } s = [115, 213, 71, 191, 55, 174, 21, 77, 8, 9, \dots, 19, 20, 6, 22, \dots, 54, 4, 56, \dots, 70, 2, 72, 73, \dots, 76, 7, 78, \dots, 113, 114, 0, 116, \dots, 173, 5, 175, \dots, 190, 3, 192, \dots, 212, 1, 214, \dots, 254, 255]$$

• Iterasi pertama

$$j = 0 \quad i = 0$$

$$i = (i + 1) \bmod 256$$

$$= (0 + 1) \bmod 256$$

$$= 1 \bmod 256$$

$$i = 1$$

$$j = (j + s[i]) \bmod 256$$

$$= (0 + s[1]) \bmod 256$$

$$= (0 + 213) \bmod 256$$

$$j = 213$$

$$\text{swap}(s[i], s[j]) \rightarrow s[1] \leftrightarrow s[213]$$

$$t = (s[i] + s[j]) \bmod 256$$

$$= (s[213] + s[1]) \bmod 256$$

$$= (213 + 1) \bmod 256$$

$$= 214 \bmod 256$$

$$t = 214$$

$$u = s[t] \rightarrow s[214]$$

$$c = u \oplus p[0]$$

$$= 214 \oplus 2$$

$$= 11010110$$

$$\underline{00000000}$$

$$11010100$$

// Ubah ke biner

↳ Ubah ke dec

$$\rightarrow 212 = \text{O}$$

↳ Ubah ke char



• Iterasi kedua

$$\underline{j = 213 \quad i = 01}$$

$$\begin{aligned} i &= (i+1) \bmod 256 \\ &= (1+1) \bmod 256 \\ &= 2 \bmod 256 \end{aligned}$$

$$i = 2$$

$$\begin{aligned} j &= (j + s[i]) \bmod 256 \\ &= (213 + s[2]) \bmod 256 \\ &= (213 + 71) \bmod 256 \\ j &= 284 \bmod 256 = 28 \end{aligned}$$

Swap ( $s[i], s[j] \rightarrow s[2] \leftrightarrow s[28]$ )

$$\begin{aligned} t &= (s[i] + s[j]) \bmod 256 \\ &= (s[28] + s[2]) \bmod 256 \\ &= (71 + 28) \bmod 256 \\ &= 99 \bmod 256 \end{aligned}$$

$$t = 99$$

$$u = s[t] \rightarrow s[99]$$

$$c = u \oplus p[1]$$

$$= 99 \oplus 0$$

$$= 01100011$$

// ubah ke biner

$$\begin{array}{r} 01100011 \\ 00000000 \\ \hline 01100011 \end{array}$$

↓ ubah ke dec

$$01100011$$

→ 99 = c // ubah ke char  
\* c kecil

• Iterasi keempat tiga

$$j = 20 \quad i = 2$$

$$i = (i + 1) \bmod 256$$

$$= (2 + 1) \bmod 256$$

$$= 3 \bmod 256$$

$$i = 3$$

$$j = (j + S[i]) \bmod 256$$

$$= (20 + S[3]) \bmod 256$$

$$= (20 + 191) \bmod 256$$

$$j = 219 \bmod 256 = 219$$

$$\text{Swap}(S[i], S[j]) \rightarrow S[3] \leftrightarrow S[219]$$

$$t = (S[i] + S[j]) \bmod 256$$

$$= (S[219] + S[3]) \bmod 256$$

$$= (219 + 191) \bmod 256$$

$$t = 154$$

$$u = S[t] \rightarrow S[154]$$

$$c = u \oplus P[2]$$

$$= 154 \oplus 5$$

$$= 10011010$$

// ubah ke biner

$$\begin{array}{r} 00000101 \\ \oplus \\ 10011111 \end{array}$$

// ubah ke dec

$$\rightarrow 159$$

// ubah ke char

• Iterasi keempat

$$j = 219 \quad i = 3$$

$$i = (i + 1) \bmod 256$$

$$= (3 + 1) \bmod 256$$

$$= 4 \bmod 256$$

$$i = 4$$

$j$

$$j = (j + S[i]) \bmod 256$$

$$= (219 + S[4]) \bmod 256$$

$$= (219 + 55) \bmod 256$$

$$j = 274 \bmod 256 = 18$$

$$\text{Swap}(S[i], S[j]) \rightarrow S[4] \leftrightarrow S[18]$$

$$t = (S[i] + S[j]) \bmod 256$$

$$= (S[18] + S[4]) \bmod 256$$

$$= (55 + 18) \bmod 256$$

$$t = 73$$

$$u = S[t] \rightarrow S[73]$$

$$c = \cancel{u} \oplus P[3]$$

$$= 73 \oplus 1$$

$$= 01001001$$

// ubah ke biner

$$\begin{array}{r} 00000001 \\ \oplus \\ 01001001 \end{array}$$

// ubah ke dec

$$\rightarrow 72$$

// ubah ke char.

## 2. Program python KSA

```
#E1E120051_SITTI NUR HALIZA_KSA
s = []
k = ['s','a','p','u','t','r','a','l']

panjangk = len(k)
for i in range(256):
    s.append(i)
print("s = ",s)

j = 0
for i in range(256):
    key_index = k[i % panjangk]
    j = (j + s[i] + ord(key_index)) % 256

    temp = s[i]
    s[i] = s[j]
    s[j] = temp
print()
print("s = ",s)
```

### HASIL OUTPUT KEY-SCHEDULING ALGORITHM (KSA)

Larik Awal : Array S dari index 0 - 255

Key : saputra1

Hasil Permutasi : Dapat dilihat pada foto

### Hasil Screenshot:

```
PS D:\SEMESTER 5\KRIPTOGRAFI\kripto2> & C:/Users/Acer/AppData/Local/Programs/Python/Python39/python.exe "d:/SEMESTER 5/KRIPTOGRAFI/kripto2/ksa1.py"
```

```
s = [0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96, 97, 98, 99, 100, 101, 102, 103, 104, 105, 106, 107, 108, 109, 110, 111, 112, 113, 114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126, 127, 128, 129, 130, 131, 132, 133, 134, 135, 136, 137, 138, 139, 140, 141, 142, 143, 144, 145, 146, 147, 148, 149, 150, 151, 152, 153, 154, 155, 156, 157, 158, 159, 160, 161, 162, 163, 164, 165, 166, 167, 168, 169, 170, 171, 172, 173, 174, 175, 176, 177, 178, 179, 180, 181, 182, 183, 184, 185, 186, 187, 188, 189, 190, 191, 192, 193, 194, 195, 196, 197, 198, 199, 200, 201, 202, 203, 204, 205, 206, 207, 208, 209, 210, 211, 212, 213, 214, 215, 216, 217, 218, 219, 220, 221, 222, 223, 224, 225, 226, 227, 228, 229, 230, 231, 232, 233, 234, 235, 236, 237, 238, 239, 240, 241, 242, 243, 244, 245, 246, 247, 248, 249, 250, 251, 252, 253, 254, 255]
```

```
s = [115, 213, 71, 49, 31, 174, 20, 74, 235, 105, 17, 44, 211, 101, 150, 244, 93, 207, 121, 129, 59, 144, 79, 119, 35, 34, 39, 13, 156, 214, 99, 165, 187, 186, 118, 6, 113, 169, 171, 15, 47, 255, 134, 250, 32, 57, 8, 117, 106, 104, 29, 3, 143, 64, 100, 42, 18, 30, 54, 97, 196, 0, 173, 242, 205, 78, 137, 133, 249, 176, 87, 83, 194, 204, 122, 40, 132, 146, 233, 193, 195, 189, 89, 96, 212, 159, 1, 03, 28, 23, 124, 230, 236, 188, 72, 85, 82, 164, 46, 225, 114, 56, 247, 192, 86, 142, 123, 1, 181, 149, 116, 215, 227, 198, 131, 231, 184, 177, 36, 76, 180, 107, 136, 140, 251, 127, 95, 7, 51, 66, 229, 158, 102, 237, 98, 69, 226, 26, 191, 38, 138, 139, 122, 16, 62, 19, 77, 220, 153, 33, 152, 154, 9, 161, 21, 216, 232, 248, 88, 148, 209, 228, 218, 175, 199, 53, 155, 178, 243, 234, 91, 166, 52, 239, 197, 183, 254, 65, 157, 12, 120, 70, 224, 147, 60, 222, 108, 61, 160, 48, 14, 41, 126, 190, 68, 125, 145, 27, 151, 163, 128, 22, 3, 203, 185, 45, 252, 92, 170, 172, 246, 63, 210, 238, 75, 201, 81, 182, 219, 162, 221, 110, 167, 111, 253, 179, 206, 245, 43, 241, 58, 217, 2, 94, 55, 67, 135, 37, 24, 109, 10, 4, 168, 141, 130, 112, 84, 11, 202, 240, 90, 80, 5, 73, 50, 208, 200, 25]
```

```
PS D:\SEMESTER 5\KRIPTOGRAFI\kripto2>
```