

Nama : Muhammad Ishak Jaelani

NIM : E1E120042

Mata Kuliah : Kriptografi

Soal

1. Kerja KSA dan PRGA dengan plaintext NIM (2042) dan kunci (saputra1). Tulis di kertas!
2. Buat program RC4 menggunakan python

Jawaban

1. KSA dan PRGA

1) KSA

Index	value	decimal
0	s	115
1	a	97
2	p	112
3	u	119
4	t	116
5	r	114
6	a	97
7	1	49

$S = [0, 1, 2, 3, 4, 5, 6, \dots, 254, 255]$

untuk $i=0, j=0$

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

$j = (0 + 0 + k[0 \bmod 8]) \bmod 256$

$= (0 + k[0]) \bmod 256$

$= (0 + 115) \bmod 256$

$= 115 \bmod 256 = 115$

Swap $(S[i], S[j]) = \text{Swap}(S[0], S[115])$

$S = [115, 1, 2, 3, \dots, 114, 0, 116, \dots, 255]$

untuk $i=1, j=115$

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

$= (115 + 1 + k[1 \bmod 8]) \bmod 256$

No.:

Date:

$$= (116 + k(1)) \bmod 256$$

$$= (116 + 97) \bmod 256$$

$$= 213 \bmod 256 = 213$$

$$\text{swap}(S[i], S[j]) = \text{swap}(S[1], S[213])$$

$$S = [115, 213, 2, 3, \dots, 212, 1, 214, \dots, 255]$$

untuk $i = 2, j = 213$

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

$$j = (213 + 2 + k(2 \bmod 8)) \bmod 256$$

$$= (215 + k(2)) \bmod 256$$

$$= (215 + 112) \bmod 256$$

$$= 327 \bmod 256 = 71$$

$$\text{swap}(S[i], S[j]) = \text{swap}(S[2], S[71])$$

$$S = [115, 213, 71, 3, \dots, 70, 2, 72, \dots, 255]$$

untuk $i = 3, j = 71$

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

$$= (71 + 3 + k(3 \bmod 8)) \bmod 256$$

$$= (74 + k(3)) \bmod 256$$

$$= (74 + 117) \bmod 256$$

$$= 191 \bmod 256 = 191$$

$$\text{swap}(S[i], S[j]) = \text{swap}(S[3], S[191])$$

$$S = [115, 213, 71, 191, 4, \dots, 190, 3, 192, \dots, 255]$$

KIKY

Never give up, winner never stop trying

No.:

<input type="checkbox"/>	untuk $i = 4, j = 191$
<input type="checkbox"/>	$j = (j + S[i] + k(i \bmod \text{length}(k))) \bmod 256$
<input type="checkbox"/>	$= (191 + 4 + k(4 \bmod 256)) \bmod 256$
<input type="checkbox"/>	$= (195 + k(4)) \bmod 256$
<input type="checkbox"/>	$= (195 + 116) \bmod 256$
<input type="checkbox"/>	$= 311 \bmod 256 = 55$
<input type="checkbox"/>	$\text{swap}(S[i], S[j]) = \text{swap}(S[4], S[55])$
<input type="checkbox"/>	$S = [115, 213, 71, 191, 55, \dots, 54, 4, 56, \dots, 255]$
<input type="checkbox"/>	untuk $i = 5, j = 55$
<input type="checkbox"/>	$j = (j + S[i] + k(i \bmod \text{length}(k))) \bmod 256$
<input type="checkbox"/>	$= (55 + 5 + k(5 \bmod 256)) \bmod 256$
<input type="checkbox"/>	$= (60 + 114) \bmod 256$
<input type="checkbox"/>	$= 174 \bmod 256 = 174$
<input type="checkbox"/>	$\text{swap}(S[i], S[j]) = \text{swap}(S[5], S[174])$
<input type="checkbox"/>	$S = [115, 213, 71, 191, 55, 174, 6, \dots, 173, 5, 175, \dots, 255]$
<input type="checkbox"/>	untuk $i = 6, j = 174$
<input type="checkbox"/>	$j = (j + S[i] + k(i \bmod \text{length}(k))) \bmod 256$
<input type="checkbox"/>	$= (174 + 6 + k(6 \bmod 256)) \bmod 256$
<input type="checkbox"/>	$= (180 + 97) \bmod 256$
<input type="checkbox"/>	$= 277 \bmod 256 = 21$
<input type="checkbox"/>	$\text{swap}(S[i], S[j]) = \text{swap}(S[6], S[21])$
<input type="checkbox"/>	$S = [115, 213, 71, 191, 55, 174, 21, \dots, 20, 6, 22, \dots, 255]$
<input type="checkbox"/>	

No.:

Date:

☐ untuk $i = 7, j = 21$

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

☐ $= (21 + 7 + k[7 \bmod 8]) \bmod 256$

☐ $= (28 + 49) \bmod 256$

☐ $= 77 \bmod 256 = 77$

☐ $\text{swap}(S[i], S[j]) = \text{swap}(S[7], S[77])$

☐ $S = [115, 213, 71, 191, 55, 174, 21, 77, 8, \dots, 76, 7, 78, \dots, 255]$

☐ Lakukan iterasi hingga iterasi ke-255, sehingga:

☐ $S = [115, 213, 71, 49, 31, 174, 20, 74, 235, 105, 17, 44, 211, 101, 150, 244, 93, 207, 121, 129, 59, 144, 79, 119, 35, 34, 39, 13, 156, 2, 14, 93, 165, 197, 186, 118, 6, 113, 169, 171, 15, 47, 255, 134, 258, 32, 57, 8, 117, 106, 104, 29, 3, 143, 64, 100, 42, 18, 30, 54, 9, 7, 196, 0, 173, 242, 205, 78, 137, 133, 249, 176, 87, 83, 194, 204, 22, 40, 132, 146, 233, 193, 195, 189, 89, 96, 212, 159, 103, 28, 23, 124, 230, 236, 188, 72, 85, 82, 164, 46, 225, 114, 56, 247, 192, 86, 142, 123, 1, 181, 149, 116, 215, 227, 198, 131, 231, 184, 177, 36, 76, 180, 107, 136, 140, 251, 127, 95, 7, 51, 66, 259, 158, 102, 237, 98, 69, 226, 26, 191, 38, 138, 130, 122, 16, 62, 19, 77, 220, 153, 33, 152, 154, 9, 161, 21, 216, 232, 148, 88, 148, 209, 228, 218, 175, 199, 53, 155, 178, 243, 234, 91, 166, 52, 239, 197, 183, 254, 65, 157, 12, 120, 170, 224, 147, 60, 222, 108, 61, 160, 48, 14, 41, 126, 100, 68, 125, 145, 27, 151, 163, 128, 223, 203, 85, 45, 252, 92, 170, 172, 246, 63, 210, 238, 75,$

KKY

One thousand problems, million solution

☐ $201, 81, 182, 219, 162, 221, 110, 167, 111, 253, 179, 206,$

☐ $245, 43, 241, 58, 28, 219, 4, 55, 67, 135, 37, 24, 109,$

☐ $10, 4, 168, 141, 130, 112, 84, 11, 202, 240, 90, 80, 5,$

☐ $73, 50, 208, 200, 25]$

2) PRGA

<input type="checkbox"/>	plaintext = 2042		
<input type="checkbox"/>	Index	value	decimal
<input type="checkbox"/>	0	50	
<input type="checkbox"/>	1	40	
<input type="checkbox"/>	2	52	
<input type="checkbox"/>	3	50	
<input type="checkbox"/>			
<input type="checkbox"/>	untuk $i=0, j=0, index=0$		
<input type="checkbox"/>	$i = (i+1) \bmod 256 = (0+1) \bmod 256 = 1$		
<input type="checkbox"/>	$j = (j + S[i]) \bmod 256 = (0 + S[1]) \bmod 256$		
<input type="checkbox"/>	$= (0 + 40) \bmod 256$		
<input type="checkbox"/>	$= 40$		
<input type="checkbox"/>	$swap(S[i], S[j]) = swap(S[1], S[40])$		
<input type="checkbox"/>	$S = [15, 20, 71, \dots, 75, 213, 81, \dots, 25]$		
<input type="checkbox"/>	$t = S[i] + S[j] = 15 + 40 = 55$		
<input type="checkbox"/>	$u = S[t] = 140$		
<input type="checkbox"/>	$c = u \oplus p[index] = 140 \oplus 141 = 1$		

No.:

Date:

☐untuk $i=1, j=213$ ☐

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

☐

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

☐

$$= (213 + S[2]) \bmod 256$$

☐

$$= (213 + 71) \bmod 256$$

☐

$$(284) \bmod 256 = 28$$

☐

$$\text{swap}(S[i], S[j]) = \text{swap}(S[2], S[28])$$

☐

$$S = [115, 201, 156, 49, \dots, 13, 71, \dots, 25]$$

☐

$$t = S[i] + S[j] = 227$$

☐

$$u = S[t] = 241$$

☐

$$c = u \oplus p[\text{index}] = 193 = A$$

☐☐untuk $i=2, j=28$ ☐

$$i = (i+1) \bmod 256 = (2+1) \bmod 256 = 3$$

☐

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

☐

$$= (28 + 49) \bmod 256$$

☐

$$= (77) \bmod 256 = 77$$

☐

$$\text{swap}(S[i], S[j]) = \text{swap}(S[3], S[77])$$

☐

$$S = [115, 201, 156, 146, 31, \dots, 132, 49, 233, \dots, 25]$$

☐

$$t = S[i] + S[j] = 195$$

☐

$$u = S[t] = 145$$

☐

$$c = u \oplus p[\text{index}] = 165 = \neq$$

☐☐untuk $i=3, j=77$ ☐

$$i = (i+1) \bmod 256 = (3+1) \bmod 256 = 4$$

KKY

Never give up, winner never stop trying

$$\begin{aligned}
 j &= (j + S(i)) \bmod 256 \\
 &= (77 + S(4)) \bmod 256 \\
 &= (77 + 31) \bmod 256 \\
 &= 108 \bmod 256 \\
 &= 108 \\
 \text{swap}(S[i], S[j]) &= \text{swap}(S[4], S[108]) \\
 S &= (115, 201, 156, 146, 149, \dots, 181, 31, 116, \dots, 25) \\
 t &= S[i] + S[j] = 180 \\
 u &= S[t] = 70 \\
 c &= u \oplus p(\text{index}) = 116 = t \\
 A &= 87 = (108 \bmod 17) \oplus 0 = 3
 \end{aligned}$$

2. Program RC4 Enkripsi dan Dekripsi

1) Input Output String

```

Masukkan PlainText : 2042
Masukkan Kunci Enkripsi : saputra1
ChiperText : !Á¥t
  
```

Gambar 2. 1 Terminal Program Enkripsi Menggunakan File EncryptionString.py

```

Masukkan ChiperText : !Á¥t
Masukkan Kunci Dekripsi : saputra1
PlainText : 2042
  
```

Gambar 2. 2 Terminal Program Dekripsi Menggunakan File DecryptionString.py

2) Input Output File

```

≡ input.txt
1 2042
  
```

Gambar 2. 3 File input.txt

```

≡ output.txt
1 !Á¥t
  
```

Gambar 2. 4 File output.txt

```
Masukkan Nama File PlainText : input.txt  
Masukkan Nama File ChiperText : output.txt  
Masukkan Kunci Enkripsi : saputra1
```

Gambar 2. 5 Terminal Program Enkripsi Menggunakan File EncryptionFile.py

```
Masukkan Nama File ChiperText : output.txt  
Masukkan Nama File PlainText : input.txt  
Masukkan Kunci Dekripsi : saputra1
```

Gambar 2. 6 Terminal Program Dekripsi Menggunakan File DecryptionFile.py