

Nama : Abby Indika Risdiani Batubara

NIM : ELEJ 20 002

Mata kuliah : Kriptografi

1. Kerjakan soal dengan metode KSA dan PGRA, plaintext nim (4 angka) dan kunci (Saputra 1)

peny: Array $S = [0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, \dots, 20, 23, 24, \dots, 245, 246, 247, 248, 249, 250, 251, 252, 253, 254, 255, 256]$

Dik: $k = \text{Saputra 1}$ Length = 8

$$k_0 = S = 115$$

$$k_1 = a = 97$$

$$k_2 = p$$

$$k_3 = u$$

$$k_4 = t$$

$$k_5 = r$$

$$k_6 = a$$

$$k_7 = j$$

$$j = 0 \quad j = 0 \text{ pertama}$$

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

$$j_{(0)} = (0 + s[0] + k[0 \bmod \text{length}(8)]) \bmod 256$$

$$= (0 + 0 + k[5]) \bmod 256$$

$$= (0 + k[115]) \bmod 256$$

$$= 115 \bmod 256 = 115$$

$$\text{swap} = (s[i], s[j])$$

$$\text{swap} = (s[0], s[115])$$

$$j_{(1)} = (115 + s[1] + k[1 \bmod \text{length}(8)]) \bmod 256$$

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

$$= (116 + k[a]) \bmod 256$$

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

$$= 213 \bmod 256$$

$$= 213$$

$$\text{swap} = (s[1], s[213])$$

$$j_{(2)} = (213 + s[2] + k[2 \bmod \text{length}(8)]) \bmod 256$$

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

$$= (215 + k[p]) \bmod 256$$

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

$$= 71$$

$$\text{Swap} = [s(2), s(71)]$$

$$\begin{aligned} J(3) &= (71 + s[3] + k[3 \bmod \text{length}(0)]) \bmod 256 \\ &= (71 + 3 + k[3]) \bmod 256 \\ &= (74 + k[u]) \bmod 256 \\ &= (74 + 117) \bmod 256 \\ &= 191 \bmod 256 \\ &= 191 \end{aligned}$$

$$\text{Swap} = [s(3), s(191)]$$

$$\begin{aligned} J(4) &= (191 + s[4] + k[4 \bmod \text{length}(8)]) \bmod 256 \\ &= (191 + 4 + k[4]) \bmod 256 \\ &= (195 + k[t]) \bmod 256 \\ &= 311 \bmod 256 \\ &= 55 \end{aligned}$$

$$\text{Swap} = [s(4), s(55)]$$

$$\begin{aligned} J(5) &= (55 + s[5] + k[5 \bmod \text{length}(8)]) \bmod 256 \\ &= (55 + 5 + k[5]) \bmod 256 \\ &= (60 + k[r]) \bmod 256 \\ &= (60 + 114) \bmod 256 \\ &= 174 \bmod 256 \\ &= 174 \end{aligned}$$

$$\text{Swap} = [s[5], s[174]]$$

$$\begin{aligned} J(6) &= (174 + s[6] + k[6 \bmod \text{length}(8)]) \bmod 256 \\ &= (174 + 6 + k[6]) \bmod 256 \\ &= (180 + k[a]) \bmod 256 \\ &= (180 + 97) \bmod 256 \\ &= 297 \bmod 256 \\ &= 21 \end{aligned}$$

$$\text{Swap} = [s[6], s[21]]$$

$$\begin{aligned} J(7) &= (21 + s[7] + k[7 \bmod (8)]) \bmod 256 \\ &= (21 + 7 + k[7]) \bmod 256 \\ &= (28 + k[i]) \bmod 256 \\ &= (28 + 49) \bmod 256 \\ &= 77 \bmod 256 \\ &= 77 \end{aligned}$$

$$\text{Swap} = [s[7], s[77]]$$

PGRA

plaintext = ~~20002~~ 2002

index	value	decimal
0	2	50
1	0	48
2	0	48
3	2	50

Dik: $i = 0$

$j = 0$

index: 0

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

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

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

$j \leftarrow (0 + S[1]) \bmod 256$

$\leftarrow (0 + S[213]) \bmod 256$

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

$j \leftarrow 213$

swap ($S[i], S[j]$) = swap ($S[1], S[213]$)

$S = [115, 201, 71, \dots, 238, 175, 213, 81, \dots, 25]$

$l = S[i] + S[j] = [201 + 213] \bmod 256 = 158$

$u = S[l] = 148 \rightarrow$ nilai dari 158

$c = u \oplus P[\text{index}] = 148 \oplus P[0] = 148 \oplus 50 = 1001 \ 0100$

$0011 \ 0010 \oplus$

$1010 \ 0110$

$c = 166 = 1$



Lakukan iterasi hingga iterasi ke-255, sehingga:

$S = [115, 213, 71, 191, 55, 174, 21, 77, 255, 105, 71, 44, 211, 101, 150, 244, 93, 207,$
 $121, 129, 59, 144, 79, 119, 35, 34, 39, 13, 156, 2, 14, 99, 165, 187, 186, 118, 6,$
 $113, 169, 171, 15, 47, 255, 134, 250, 32, 57, 8, 117, 106, 104, 29, 3, 143, 64,$
 $100, 42, 18, 30, 54, 9, 7, 196, 0, 173, 242, 205, 78, 137, 133, 249, 176,$
 $87, 83, 194, 204, 22, 40, 132, 146, 233, 193, 195, 189, 89, 96, 212, 159,$
 $103, 28, 23, 124, 230, 236, 188, 72, 85, 82, 164, 46, 225, 114, 56, 247,$
 $192, 86, 142, 123, 1, 181, 149, 116, 215, 227, 198, 131, 231, 184, 177,$
 $36, 76, 180, 107, 136, 140, 251, 127, 95, 7, 51, 66, 259, 158, 102, 237,$
 $98, 69, 226, 26, 191, 38, 138, 139, 122, 16, 62, 19, 77, 220, 153, 33, 152,$
 $154, 9, 161, 21, 216, 232, 248, 88, 148, 209, 228, 210, 175, 199, 53, 155,$
 $178, 243, 234, 91, 166, 52, 239, 197, 183, 175, 199, 53, 155, 178, 243,$
 $234, 91, 166, 52, 239, 197, 183, 254, 65, 157, 12, 120, 170, 224, 147, 60,$
 $222, 108, 61, 160, 48, 14, 41, 126, 190, 68, 125, 145, 27, 151, 163, 128,$
 $233, 203, 185, 45, 252, 92, 170, 172, 246, 63, 210, 238, 75, 201, 81, 182,$
 $219, 162, 221, 110, 167, 111, 253, 179, 206, 245, 43, 241, 58, 20, 219, 55, 67,$
 $135, 37, 24, 109, 10, 4, 168, 141, 130, 112, 84, 11, 202, 240, 90, 80, 5, 73,$
 $50, 200, 200, 25]$

untuk $i = 1$

$$j = 213$$

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

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

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

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

$$j \leftarrow 284 \bmod 256 = 28$$

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

$$S = (118, 201, 13, 156, 2, 19, \dots, 13, 17, \dots, 75)$$

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

$$= S[2] + S[28] \bmod 256$$

$$= 13 + 20 \bmod 256$$

$$= 41 \bmod 256$$

$$= 41$$

$$u = S[t] = 15$$

$$c = u \oplus P[\text{index}]$$

$$= 15 \oplus P[1]$$

$$15 = 1111 \ 0000$$

$$48 = 0011 \ 0000 \oplus$$
$$\hline 1100 \ 0000$$

$$c = 192 = \hat{A}$$

untuk $i = 2$

$$j = 20$$

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

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

$$(20 + s[3]) \bmod 256$$

$$j \leftarrow 219 \bmod 256$$

$$j \leftarrow 219$$

$$\text{swap}(s[i], s[j]) = \text{swap}(s[3], s[219])$$

$$s = (115, 201, 13, 224, 2, 14, \dots, 13, 17, \dots, 25)$$

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

$$= s[3] + s[219] \bmod 256$$

$$= 224 + 219 \bmod 256$$

$$= 443 \bmod 256$$

$$= 187$$

$$u = s[t] = 222$$

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

$$222 = 1101\ 1110$$

$$40 = 0011\ 0000 \oplus$$

$$1110\ 1110$$

$$c = 238 = \uparrow \uparrow$$

untuk $i = 3$

$$j = 219$$

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

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

$$= 274 \bmod 256$$

$$= 18$$

$$\text{swap}(s[i], s[j]) = \text{swap}(s[4], s[18])$$

$$s = (115, 201, 13, 224, 7, \dots)$$

$$t = s[i] + s[j]$$

$$= s[4] + s[18]$$

$$= 7 + 10 \bmod 256$$

$$= 25 \bmod 256 = 25$$

$$u = s[t] = 35$$

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

$$c = 35 \oplus p[3]$$

$$35 \quad 0010\ 0011$$

$$50 \quad 0011\ 0010 \oplus$$

$$\underline{0001}$$

$$0001\ 0001$$

$$c = 17 = DC1$$