

Nama : Raya Srikandi

NIM : E1E120096

Mata kuliah : Kriptografi

Soal

1. Kerjakan soal dengan metode KSA dan PGRA, plaintext NIM (4 angka) dan kunci (Saputra1)

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 : $K = \text{Saputra1}$ length = 8

$$k_0 = S = 115$$

$$k_1 = a = 97$$

$$k_2 = p$$

$$k_3 = u$$

$$k_4 = t$$

$$k_5 = r$$

$$k_6 = a$$

$$k_7 = 1$$

$J = 0$ $J = 0/1$ pertama

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

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

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

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

$$= 115 \bmod 256 = 115$$

$$\text{Swap} = (S[i], S[J])$$

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

$$J_{(1)} = (115 + S[i] + k[1 \bmod \text{length}(8)]) \bmod 256$$

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

$$= (116 + k[9]) \bmod 256$$

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

$$= 213 \bmod 256$$

$$= 213$$

$$\text{Swap} = (S[i], S[213])$$

$$\begin{aligned}
 J(2) &= (213 + s[2] + k[2 \bmod \text{length}[87]]) \bmod 256 \\
 &= (213 + 2 + k[2]) \bmod 256 \\
 &= (215 + k[p]) \bmod 256 \\
 &= (215 + 112) \bmod 256 \\
 &= 327 \bmod 256 \\
 &= 71
 \end{aligned}$$

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

$$\begin{aligned}
 J(3) &= (71 + s[3] + k[3 \bmod \text{length}[87]]) \bmod 256 \\
 &= (71 + 3 + k[3]) \bmod 256 \\
 &= (74 + k[4]) \bmod 256 \\
 &= (74 + 117) \bmod 256 \\
 &= 191 \bmod 256 \\
 &= 191
 \end{aligned}$$

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

$$\begin{aligned}
 J(4) &= (191 + s[4] + k[4 \bmod \text{length}[87]]) \bmod 256 \\
 &= (191 + 4 + k[4]) \bmod 256 \\
 &= (195 + k[+]) \bmod 256 \\
 &= (195 + 116) \bmod 256 \\
 &= 311 \bmod 256 \\
 &= 55
 \end{aligned}$$

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

$$\begin{aligned}
 J(5) &= (55 + s[5] + k[5 \bmod \text{length}[87]]) \bmod 256 \\
 &= (55 + 5 + k[5]) \bmod 256 \\
 &= (60 + k[r]) \bmod 256 \\
 &= (60 + 114) \bmod 256 \\
 &= 174 \bmod 256 \\
 &= 174
 \end{aligned}$$

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

$$\begin{aligned}
 J(6) &= (174 + s[6] + k[6 \bmod \text{length}[87]]) \bmod 256 \\
 &= (174 + 6 + k[6]) \bmod 256 \\
 &= (180 + k[a]) \bmod 256 \\
 &= (180 + 97) \bmod 256 \\
 &= 297 \bmod 256 \\
 &= 21
 \end{aligned}$$

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



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

$$\text{Swap} = [S(7), S(77)]$$

Sehingga $S = [115, 213, 71, 191, 55, 179, 21, 77, 8, 9, 10, \dots, 245, 246, 247, 248, 249, 250, 251, 252, 253, 254, 255]$

PGRA

Plaintext = 2006

Index	Value	decimal
0	2	50
1	0	48
2	4	34
3	6	54

Dik : untuk

$$i = 0$$

$$j = 0$$

$$\text{index} = 0$$

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

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

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

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

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

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

$$j \leftarrow 213$$

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

$$S = [115, 201, 71, \dots, 238, 75, 213, 81, \dots, 25]$$

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

$$u = S[t] = 148 \rightarrow \text{nilai dari } 158$$

$$C = u \oplus P(\text{index}) = 148 \oplus P[0] = 148 \oplus 50 \rightarrow 148 = 10010100$$

$$50 = 00110010$$

$$10100110$$

$$C = 166 = i$$

6(00)

Lakukan iterasi hingga iterasi ke-255, sehingga:

$S = [115, 213, 71, 191, 55, 174, 21, 77, 255, 105, 71, 44, 211, 101, 150, 244, 93, 207, 121, 129, 59, 144, 79, 119, 35, 34, 39, 13, 156, 2, 14, 99, 165, 187, 186, 118, 6, 113, 169, 171, 15, 97, 255, 154, 250, 32, 57, 0, 117, 106, 104, 29, 3, 143, 64, 100, 42, 18, 30, 54, 9, 7, 196, 0, 173, 242, 205, 78, 137, 133, 249, 176, 87, 83, 194, 204, 22, 40, 132, 146, 233, 193, 195, 189, 89, 46, 212, 159, 103, 28, 23, 124, 230, 236, 188, 72, 85, 82, 164, 46, 225, 114, 56, 247, 192, 86, 142, 123, 1, 181, 149, 116, 215, 227, 198, 131, 231, 184, 177, 36, 76, 180, 107, 136, 140, 251, 127, 95, 7, 51, 66, 259, 158, 102, 237, 98, 69, 226, 26, 191, 38, 138, 139, 122, 16, 62, 19, 77, 220, 153, 33, 152, 154, 9, 161, 21, 216, 232, 248, 88, 148, 209, 228, 218, 175, 199, 53, 155, 178, 243, 234, 91, 166, 52, 239, 197, 183, 175, 199, 53, 155, 178, 243, 222, 108, 61, 160, 48, 14, 41, 126, 190, 68, 125, 145, 27, 151, 163, 128, 233, 203, 185, 45, 252, 92, 170, 172, 246, 63, 210, 238, 75, 201, 81, 182, 219, 162, 221, 110, 167, 111, 253, 179, 206, 245, 43, 241, 58, 20, 219, 55, 67, 135, 37, 29, 109, 10, 4, 168, 141, 130, 112, 84, 11, 202, 240, 90, 80, 5, 73, 50, 200, 200, 25]$

Untuk $i = 1$

$$j = 213$$

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

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

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

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

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

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

$$S = (115, 201, 13, 156, 2, 14, \dots, 13, 17, \dots, 25)$$

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

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

$$= 13 + 28 \bmod 256$$

$$= 41 \bmod 256$$

$$= 41$$

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

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

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

$$15 = 1111\ 0000$$

$$48 = \underline{0011\ 0000} \oplus$$

$$1000\ 0000$$

$$c = 192$$

Untuk $i = 2$

$$j = 28$$

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

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

$$\leftarrow (28 + S[3]) \bmod 256$$

$$\leftarrow (28 + S[229]) \bmod 256$$

$$\leftarrow 219 \bmod 256$$

$$\leftarrow 219$$

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

$$S = (115, 201, 13, 229, 2, 14, \dots, 13, 17, \dots, 25)$$

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

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

$$= 229 + 219 \bmod 256$$

$$= 187$$

$$u = S[t] = 222$$

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

$$222 = 1101\ 1110$$

$$\rightarrow 39 = \underline{00100010} \oplus$$

$$11111100$$

$$c = 252 = u$$

No. : _____

Date : _____

untuk $i = 3$

$$J = 219$$

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

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

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

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

$$= 274 \bmod 256$$

$$= 18$$

$$\text{Swap}(S[i], S[J]) = \text{Swap}(S[4], S[18])$$

$$S = (115, 201, 13, 224, 7)$$

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

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

$$= 7 + 18 \bmod 256$$

$$= 25 \bmod 256$$

$$= 25$$

$$u = S[t] = 35$$

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

$$= 35 \oplus P[3]$$

$$35 = 00100101$$

$$00110110 \oplus$$

$$00010101$$

$$C = 21 = \text{NAK}$$