Nama : Dwi Hikmah Ramadhani
NIM : E1E120006
Kelas : Genap
Matkul : Kriptografi

Soal

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

Penyelesaian :

Array s : [0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, ..., 20, 23, 24, ..., 245, 246, 247, 248, 249, 250, 251, 252, 253, 254, 255, 256]

Dik :

K = Saputra 1
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/i pertama
j = (j + s[i] + k[i% mod length (k)]) mod 256
j(0) = (0 + s[0] k[0 mod length (8)]) mod 256
= (0+0 + k[5]) mod 256
= (0+k[115]) mod 256
= 115 mod 256 = 115
Swap = (s[i] . s[j])
Swap = (s[0] . s[115])

j(1) = (115 + s[1] + k[1 mod length (8)]) mod 256
= (115+1 + k[1]) mod 256
= (116 + k[a]) mod 256
= (116 + 97) mod 256
= 213 mod 256
= 213
Swap = (s[1], s[213])

J(2) = (213 + S[2] + k[2 mod length (8)]) mod 256
= (213 + 2 + k[2]) mod 256
= (215 + k[2]) mod 256
= (215 + 112) mod 256
= 327 mod 256
= 71
Swap = [S(2), S(71)]

J(3) = (71 + S[3] + k[3 mod length (8)]) mod 256
= (71 + 3 + k[3]) mod 256
= (74 + k[3]) mod 256
= (74 + 117) mod 256
= 191 mod 256
= 191
Swap = [S(3), S(191)]

J(4) = (191 + S[4] + k[4 mod length (8)]) mod 256
= (191 + 4 + k[4]) mod 256
= (195 + k[4]) mod 256
= (195 + 116) mod 256
= 311 mod 256
= 55
Swap = [S(4), S(55)]

J(5) = (55 + S(5) + k[5 mod length (8)]) mod 256
= (55 + 5 + k[5]) mod 256
= (60 + k[5]) mod 256
= (60 + 114) mod 256
= 174 mod 256
= 174
Swap = (S[5], S[174])

J(6) = (174 + S(6) + k[6 mod length (8)]) mod 256
= (174 + 6 + k[6]) mod 256
= (180 + k[6]) mod 256
= (180 + 97) mod 256
= 297 mod 256
= 21
Swap = (S[6], S[21])

$j(7) = (21 + s(7) + k[7 \bmod \text{length}(8)]) \bmod 256$

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

$= (28 + k[1]) \bmod 256$

$= (28 + 49) \bmod 256$

$= 77 \bmod 256$

$= 77$

swap : $(s[7], s[77])$

sehingga $s = [115, 213, 71, 191, 55, 174, 21, 77, 8, 9, 10, \ldots, 245, 246, 247, 248, 249, 250, 251, 252, 253, 254, 255]$

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, 194, 79, 119, 35, 34, 39, 13, 156, 2, 14, 99, 165, 187, 186, 118, 6,
113, 169, 171, 15, 97, 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, 209, 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, 218, 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, 197, 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, 29, 109, 10, 4, 168, 141, 130, 112, 84, 11, 202, 240, 90, 80, 5, 73,
50, 208, 200, 25]

PGRA

Plaintext : 2006

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

Dik : untuk

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, ..., 238, 75, 213, 81, ..., 25]

t = S[i] + S[j] = [201 + 213] mod 256 = 158

u = S[t] = 148 → nilai dari 158

C = u ⊕ p (index) = 148 ⊕ p[0] = 148 ⊕ 50

148 = 1001 0100

50 = 0011 0010 ⊕

1010 0110

C = 166 = ì

Untuk i = 1

J = 213

i ← (i+1) mod 256 = (1+1) mod 256 = 2

j ← (j+S[i]) mod 256

← (213+S[2]) mod 256

← (213+71) mod 256

J ← 284 mod 258 = 28

swap (S[i], S[j]) = swap (S[2], S[28])

S = (115, 201, 13, 156, 2, 14, ..., 13, 17, ..., 25)

t = S[i] + S[j] mod 256

= S[2] + S[28] mod 256

= 13 + 28 mod 256

= 41 mod 256

= 41

u = S[t] = 15

C = u ⊕ p[index]

= 15 ⊕ p[1]

15 = 1111 0000

48 = 0011 0000 ⊕

1100 0000

C = 192 = Á

Untuk i = 2

J = 28

i ← (i+1) mod 256 = (2+1) mod 256 = 3

J ← (J+S[i]) mod 256

← (28+S[3]) mod 256

J ← (28+191) mod 256

← 219 mod 256

← 219

swap (S[i], S[J]) = swap (S[3], S[219])

S = (115, 201, 13, 224, 2, 14, ..., 13, 17, ..., 25)

t = S[i] + S[J] mod 256

= S[3] + S[219] mod 256

= 224 + 219 mod 256

= 187

u = S[t] = 222

C = u ⊕ p (index)

222 = 1101 1110

48 = 0011 0000 ⊕

1110 1110

C = 238 = î

No.: Date.:

Untuk i = 3

J = 219

P = (i + 1) mod 256 (3 + 1) mod 256 = 4

= (J + S[i]) mod 256

= (219 + S[4] mod 256

= (219 + 55) mod 256

= 274 mod 256

= 18

swap (S[i], S[j]) = swap (S[4], S[18])

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

t = S[i] + S[j] mod 256

= S[4] + S[18] mod 256

= 7 + 18 mod 256

= 25 mod 256

= 25

U = S[t] = 35

C = U ⊕ p [index]

= 35 ⊕ p[3]

35 = 0010 0011

54 = 0011 0110 ⊕

0001 0101

C = 21 = NAK

KIKY