Date

Nama : Alfriyanti Ahmad sipa
Nim : E1E120058
Matkul : kriptografi

Soal

1. Kerjakan soal dengan metode KSA dan PGRA, plainteks nim (Gangra) dan kunci (saputra1)

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]

Diketahui :

K = 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 / 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[8]) 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(0)]) 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])

Date

J(2) = (213 + S[2] + k[2 mod length(0)]) 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(0)]) 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(0)]) 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(0)]) 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(0)]) mod 256
= (174 + 6 + k[6]) mod 256
= (100 + k[a]) mod 256
= (100 + 97) mod 256
= 297 mod 256
= 21
Swap = (s[6], s[71])

KKY

Date

$j(7) = (21 + S(7) + k[7 \bmod (0)]) \bmod 256$

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

$= (28 + k[7]) \bmod 256$

$= (28 + 49) \bmod 256$

$= 77 \bmod 256$

$= 77$

swap $= [S[7], S[77]]$

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, 154, 250, 32, 57, 0, 117, 106, 109, 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, 196, 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, 32, 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, 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, 29, 109, 10, 4, 168, 191, 130, 112, 84, 11, 202, 240, 90, 80, 5, 73,
50, 200, 200, 25]

PGRA

Plaintext : 2058

| Index | value | decimal |
|---|---|---|
| 0 | 2 | 50 |
| 1 | 0 | 48 |
| 2 | 5 | 53 |
| 3 | 8 | 56 |

Dik : untuk
i = 0
j = 0
index : 0

i ← (i + 1) mod 256
j ← (j + S[i]) mod 256

i ← (0 + 1) mod 256 = 1 mod 256 = 1
j ← (0 + S[1]) mod 256
← (0 + S[213]) mod 256
← (0 + 213) mod 256
j ← 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

1001 0100
0011 0010 ⊕
10100 110

c = 166 = ¦

KEY k =

Date

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 256 = 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] = ~~227~~ mod 256

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

= 13 + 28 ~~256~~ mod 256

= 41 mod 256

= 41

u = S[t] = 15

C = u ⊕ P [index]

= 15 ⊕ P[1]

15 = 1111 0000

40 = 0011 0000 ⊕

11000000

C = 192 = ë À

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

= 443 mod 256

= 187

u = s[t] = 222

c = u ⊕ p[index]

222 = 1101 1110

53 = 0011 0101 ⊕

1110 1011

c = 235 = ë

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] = S[4] + S[18] = 7 + 18 mod 256

= 25 mod 256

= 25

u = S[t] = 35

C = u ⊕ P [index]

C = 35 ⊕ P[3]

35 0010 0011

56 0011 1000 ⊕

0001 1011

C = 27 = ESC