# Tugas Kriptografi

Nama : Tasya Berlianiswah B
NIM : E1E120095
Kelas : Ganjil.

1. Kerjakan 4 iterasi menggunakan Algoritma KSA (key-Scheduling Algorithm) dan PRGA (Pseudo-random Generation Algorithm) menggunakan kunci /k = Saputra1.

= Array S = [0, 1, 2, 3, 4, 5, . . . . , 253, 254, 255]

I iterasi pertama

i = 0, j = 0
j = (j + S[i] + k[i mod length(k)]) mod 256
j = (0 + 0 + k[0 mod (8)]) mod 256
j = ($k_0$) mod 256
j = 115 mod 256
j = 115

Swap (S[i], S[j])
= swap (S[0], S[115])

Array S = [115, 1, 2, 3, 4, . . . . , 114, 0, 116, . . . . , 254, 255]

II. iterasi kedua

i = 1, j = 115
j = (j + S[i] + k[i mod length (k)]) mod 256
j = (115 + 1 + k[1 mod (8)]) mod 256
j = (116 + $k_1$) mod 256
j = (116 + 97) mod 256
j = 213 mod 256
j = 213

Swap (S[i], S[j])
= Swap (S[1], S[213])

Array S = [115, 213, 2, 3, 4, 5, . . . , 114, 0, 116, . . . , 212, 1, 214, . . . 254, 255]

III. iterasi ketiga

i = 2, j = 213
j = (j + S[i] + k[i mod length (k)]) mod 256
j = (213 + 2 + k[2 mod (8)]) mod 256
j = (215 + $k_2$) mod 256
j = (215 + 112) mod 256
j = 327 mod 256
j = 71 $\Longrightarrow$ Swap (S[i], S[j])
= Swap (S[2], S[71])

$\longrightarrow$ Array S = [115, 213, 71, 3, 4, 5, . . . , 70, 2, 72, . . . 114, 0, 116, . . . , 212, 1, 214, . . . . , 254, 255]

IV. Iterasi keempat

i = 3 , j = 71

j = (j + S[i] + k[i mod length (k)]) mod 256

j = (71 + 3 + k[3 mod (8)]) mod 256

j = (74 + $k_3$) mod 256

j = (74 + 117) mod 256

j = 191 mod 256

j = 191

Swap ( S[i], S[j])

= Swap ( S[3], S[191])

Array S = [115, 213, 71, 191, 4, 5, ... ,70, 2, 72, ... ,114, 0, 116, ... ,190, 3, 192, ... ... ,212, 1, 214, ... , 253, 254, 255 ]

V. Iterasi kelima

i = 4, j = 191

j = (j + S[i] + k[i mod length (k)]) mod 256

j = (191 + 4 + k[4 mod (8)]) mod 256

j = ( 195 + $k_4$) mod 256

j = ( 195 + 116 ) mod 256 = 311 mod 256

j = 55

Swap ( S[i], S[j])

= Swap ( S[4], S[55])

Array S = [115, 213, 71, 191, 55, 5, ... , 53, 54, 4, 56, ... , 70, 2, 72, ... ,114, 0, 116, ... , 190, 3, 192, ... , 212, 1, 214, ... ... , 253, 254, 255]

VI. iterasi keenam

i = 5 , j = 55

j = (j + S[i] + k[i mod length (k)]) mod 256

j = (55 + 5 + k[5 mod (8)]) mod 256

j = ( 60 + $k_5$) mod 256

j = (60 + 114) mod 256

j = 174 mod 256

j = 174

Swap (S[i], S[j])

= Swap ( S[5] S[174])

Array S = [115, 213, 71, 191, 55, 174, 6, 7, 8, ... , 53, 54, 4, 56, ... , 70, 2, 72, ... ,114, 0, 116, ... , 173, 5, 175, ... , 190, 3, 192, ... , 212, 1, 214, ... 254, 255]

VII. Iterasi ketujuh

i = 6, j = 174

j = (j + S[i] + k [i mod length (k)]) mod 256

j = (174 + 6 + k [6 mod (8)]) mod 256

j = (180 + k6) mod 256

j = (180 + 97) mod 256

j = 277 mod 256

j = 21

Swap (S[i], S[j])

= Swap (S[6], S[21])

Array S = [115, 213, 71, 191, 55, 174, 21, 7, 8, 9, ...., 20, 6, 22, ...., 54, 4, 56, ...., 70, 2, 72, ..., 114, 0, 116, ..., 173, 5, 175, ..., 190, 3, 192, ...., 212, 1, 214, ...., 254, 255]

VIII. Iterasi kedelapan

i = 7, j = 21

j = (j + S[i] + k [i mod length (k)]) mod 256

j = (21 + 7 + k [7 mod (8)]) mod 256

j = (28 + k7) mod 256

j = (28 + 49) mod 256

j = 77 mod 256

j = 77

Swap (S[i], S[j])

= swap (S[7], S[77])

Array S = [115, 213, 71, 191, 55, 174, 21, 77, 8, 9, ...., 20, 6, 22, ..., 54, 4, 56, ..., 70, 2, 72, 73, 74, 75, 76, 7, 78, ...., 114, 0, 116, ..., 173, 5, 175, ...., 190, 3, 192, ...., 212, 1, 214, ..., 253, 254, 255]

PRGA (Pseudo-random Generation Algorithm).

Array S = [115, 213, 71, 191, 55, 174, 21, 77, 8, 9, 10, ..., 20, 6, 22, ..., 54, 4, 56, ...
, 70, 2, 72, ..., 76, 7, 78, ..., 114, 0, 116, ..., 173, 5, 175, ..., 190, 3, 192,
..., 212, 1, 214, ..., 259, 255]
Plainteks / p = 2095

I. iterasi pertama
i = 0, j = 0
for index = 0 to length (p) - 1
= 0 to (4) - 1 = 0 to (3).
i = (i+1) mod 256
i = (0+1) mod 256
i = 1
j = (j + S[i]) mod 256
j = (0 + S[1]) mod 256
j = (0 + 213) mod 256 = 213 mod 256
j = 213
Swap (S[i], S[j]) = (S[1], S[213])

t = (S[1] + S[213]) mod 256
t = 1 + 213 mod 256 = 214 mod 256
t = 214
u = S[214]
C = u ⊕ P[0]
= 214 ⊕ 2
= 11010110
00110010 ⊕
11 100100 = 228 = ä

II. iterasi kedua
i = 1, j = 213
for index = 0 to (3)
i = (i+1) mod 256
i = (1+1) mod 256
i = 2
j = (j + S[i]) mod 256
j = (213 + S[2]) mod 256
j = (213 + 71) mod 256 = 284 mod 256
j = 28

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

t = (S[2] + S[28]) mod 256
t = (28 + 71) mod 256 = 99 mod 256
t = 99
u = S[99]
C = u $\oplus$ P[1]
= 99 $\oplus$ 0
= 01100011
$\underline{00110000 \oplus}$
01010011 = 83 = S (capital S).

III itorasi ketiga
i = 2, j = 28
for index = 0 to (3)
i = (i+1) mod 256
i = (2+1) mod 256
i = 3
j = (j + S[i]) mod 256
j = (28 + S[3]) mod 256
j = (28 + 191) mod 256 = 219 mod 256
j = 219
Swap (S[i], S[j]) = (S[3], S[219])

t = (S[3] + S[219]) mod 256
t = (219 + 191) mod 256 = 410 mod 256
t = 154
u = S[154]
C = u $\oplus$ P[2]
= 154 $\oplus$ 9
= 10011010
$\underline{00111001 \oplus}$
10100011 = 163 = £ (karakter).

IV. Itorasi keempat
i = 3, j = 219
for index = 0 to (3)
i = (i+1) mod 256
i = (3+1) mod 256

i = 4
j = (j + S[i]) mod 256
j = (219 + S[4]) mod 256
j = (219 + 55) mod 256 = 274 mod 256
j = 18
Swap (S[i], S[j]) = (S[4], S[18])

t = (S[4], S[18]) mod 256
t = (18 + 55) mod 256 = 73 mod 256
t = 73
u = S[73]
C = 73 ⊕ P[3]
= 73 ⊕ 5
= 0100 1001
0011 0101 ⊕
0111 1100 = 124 = | (vertical bar)

Hasilnya = äS£|

Kemudian hasil arraynya :
Array S = [115, 1, 28, 219, 18, 174, 21, 77, 8, 9, 10, ...., 17, 55, 19, .., 20, 6, 22, .., 27, 71,
29, ...., 70, 2, 72, ...., 76, 7, 78, ..., 114, 0, 116, ..., 173, 5, 175, .., 212,
213, 214, 215, ...., 218, 291, 220, ...., 253, 254, 255]