Tugas Kriptografi

Date

Nama : Endah Sekar Lembayung

NIM : E1E120065

Metode KSA (Key Scheduling Algoritma)

Kunci : Saputra1 , len(K) = 8

K_0 : s = 115 , K_1 : a = 97 , K_2 : p = 112 , K_3 : u = 117 , K_4 : t = 116

K_5 : r = 114 , K_6 : a = 97 , K_7 : 1 = 49.

Array s : [0,1,2,3,4,5, ..., 100,101,102,103,104,105, ..., 253, 254, 255]

* Iterasi Pertama

i = 0 , j = 0

j = (j + S[i] + K [i mod lenght (K)]) mod 256

= (0 + 0 + K [0 mod 8]) mod 256

= (0 + K[0]) mod 256

= 115 mod 256

j = 115//

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

swap (S[0] , S[115])

Array s = [115, 0, 2, 3, 4, 5, ..., 113, 114, 0, 116, 117, ..., 250, 251, 252, 253, 254, 255]

* Iterasi Kedua

i = 1 , j = 115

j = (j + S[i] + K [i mod lenght (K)] mod 256

= (115 + S[1] + K [1 mod 8]) mod 256

= (115 + 1 + K[1]) mod 256

= (116 + 97) mod 256

= 213 mod 256

j = 213//

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

swap (S[1], S [213])

Array s = [115, 213, 2, 3, 4, 5, 6, 7, ..., 113, 114, 0, 116, 117, ..., 211, 212, 1, 214, ...,
252, 253, 254, 255]

* Iterasi Ketiga

i = 2, j = 213

j = (j + S[i] + K[i mod lenght (K)]) mod 256

= (213 + S[2] + K[2 mod 8]) mod 256

= (213 + 2 + K[2]) mod 256

= (215 + 112) mod 256

= 327 mod 256

j = 71//

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

Swap (S[2], S[71])

Array s = [115, 213, 71, 3, 4, 5, 6, 7, ..., 69, 70, 2, 72, 73, ..., 113, 114, 0, 116, 117, ...,
211, 212, 1, 214, 215, ..., 253, 254, 255]

* Iterasi Keempat

i = 3, j = 71

j = (j + S[i] + K[i mod lenght (K)]) mod 256

= (71 + S[3] + K[3 mod 8]) mod 256

= (71 + 3 + K[3]) mod 256

= (74 + 117) mod 256

= 191 mod 256

j = 191//

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

swap (S[3], S[191])

Array s = [115, 213, 71, 191, 4, 5, 6, 7, ..., 69, 70, 2, 72, 73, ..., 113, 114, 0, 116, 117, ...,
190, 3, 192, 193, ..., 211, 212, 1, 214, ..., 253, 254, 255]

* Iterasi Kelima

i = 4, j = 191

j = (j + S[i] + K[i mod lenght (K)]) mod 256

= (191 + S[4] + K[4 mod 8]) mod 256

= (191 + 4 + K[4]) mod 256

= (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, 6, 7, ..., 53, 54, 4, 56, 57, ..., 70, 2, 72, 73, ...,
190, 3, 192, 193, ..., 211, 212, 1, 214, ..., 253, 254, 255]

Date

* Iterasi Keenam

i = 5 , j = 55

j : (j + S[i] + K[i mod lenght (K)]) mod 256
= (55 + S[5] + K[5 mod 8]) mod 256
= (55 + 5 + K[5]) mod 256
= (60 + 114) mod 256
= 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, ..., 53, 54, 4, 56, 57, ..., 70, 2, 72, 73,
..., 172, 173, 5, 175, ..., 190, 3, 192, 193, ..., 211, 212, 1, 214, ...,
253, 254, 255]

* Iterasi Ketujuh

i = 6 , j = 174

j : (j + S[i] + K[i mod lenght (K)]) mod 256
= (174 + S[6] + K[6 mod 8]) mod 256
= (174 + 6 + K[6]) mod 256
= (180 + 97) mod 256
= (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, ..., 20, 6, 22, 23, ..., 53, 54, 4, 56, ...,
70, 2, 72, 73, ..., 113, 114, 0, 116, ..., 173, 5, 175, 176, ..., 190, 3, 192,
..., 211, 212, 1, 214, ... 253, 254, 255]

* Iterasi Kedelapan

i = 7 , j = 21

j : (j + S[i] + K[i mod lenght (K)]) mod 256
= (21 + 7 + K[7 mod 8]) mod 256)
= (28 + K[7]) mod 256
= (28 + 49) mod 256
j = 77//

Swap (S[i], S[j])
Swap (S[7], S[77])

Array S = [115, 213, 71, 191, 55, 174, 21, 77, ..., 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]

Metode PRGA (Pseudo-Random Generation Algorithm)

Diketahui :

Array s = [115, 213, 71, 191, 55, 174, 21, 77, 8, ..., 20, 6, 22, 23, ..., 54, 4, 56, ..., 70, 2, 72, 73, 74, 75, 76, 7, 78, ..., 114, 0, 116, ..., 173, 5, 175, ..., 190, 3, 192, 193, ..., 211, 212, 1, 214, ..., 253, 254, 255]

Plaintext = [2 0 6 5]

$P_0 \rightarrow 2 = 00110010$

$P_1 \rightarrow 0 = 00110000$

$P_2 \rightarrow 6 = 00110110$

$P_3 \rightarrow 5 = 00110101$

* Iterasi Pertama

i = 0 , j = 0

for index = 0 to lengnt (P) - 1

= 0 to (4) - 1

= 0 to (3)

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

$= (0 + 1) \bmod 256$

$i = 1$

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

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

$= (0 + 213) \bmod 256$

$= 213 \bmod 256$

$j = 213$ //

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

(S[1], S[213])

$t = (S[1] + S[213]) \bmod 256$

$= (1 + 213) \bmod 256$

$t = 214$

$u = S[214]$

$c = u \oplus P[0]$

$= 214 \oplus 2$

$= 11010110$

$ 00110010 \oplus$

$11100100 \longrightarrow 228 = \ddot{a}$

* Iterasi Kedua

i = 1 , j = 213

for index = 0 to (3)

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

$= 2$

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

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

$= (213 + 71) \bmod 256$

$= 284 \bmod 256$

$j = 28$ //

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

$(S[2], S[28])$

$t = (S[2] + S[28]) \bmod 256$

$= (28 + 71) \bmod 256$

$= 99 \bmod 256$

$t = 99$

$u = S[99]$

$c = u \oplus P[1]$

$= 99 \oplus 0$

$= 01100011$

$\underline{00110000 \oplus}$

$01010011 \rightarrow 83 = S$ (capital S)

* Iterasi ketiga

$i = 2, \; j = 28$

for index = 0 to 3

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

$= 3$

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

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

$= (28 + 191) \bmod 256$

$= 219 \bmod 256$

$j = 219$

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

$(S[3], S[219])$

$t = (S[3] + S[219]) \bmod 256$

$= (219 + 191) \bmod 256$

$= 410 \bmod 256$

$t = 154$

$u = S[154]$

$c = u \oplus P[2]$

$= 154 \oplus 6$

$= 10011010$

$\underline{00110110 \oplus}$

$10101100 \rightarrow 172 = \neg$

* Iterasi Keempat

$i = 3, \; j = 219$

for index = 0 to 3

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

$= 4$

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

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

$= (219 + 55) \bmod 256$

$= 274 \bmod 256$

$j = 18$

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

$(S[4], S[18])$

$t = (S[4] + S[18]) \bmod 256$

$= (18 + 55) \bmod 256$

$= 73 \bmod 256$

$t = 73$

$u = S[73]$

$c = u \oplus P[3]$

$= 73 \oplus 5$

$= 01001001$

$\underline{00110101 \oplus}$

$01111100 \rightarrow 124 = |$ (Vertical bar)