Date 30 - 12 - 2022

Nama : Aldriani Adhyaksa

NIM : E1E1 20 003

Kelas : Ganjil

Tugas Kriptografi <=> Metode KSA (Key Algorithm Scheduling)

K = saputra1 <=> K_0 = s, K_1 = a, K_2 = p, K_3 = u, K_4 = t, K_5 = r, K_6 = a, K_7 = 1

s = 115, a = 97, p = 112, u = 117, t = 116, r = 114, a = 97, 1 = 49

Array S = [0, 1, 2, 3, ... 252, 253, 254, 255]

(j = 0 i = 0 / iterasi pertama dan seterusnya)

K_0 <=> j = (j + S[i] + K[i mod length (K)]) mod 256

j = (0 + S[0] + K[0 mod length (8)]) mod 256

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

j = (0 + 115) mod 256

j = 115 //

swap (S[i], S[j])
swap (S[0], S[115]) } Array S = [115, 1, 2, 3, ..., 111, 112, 113, 114, 0, 116, ... 253, 254, 255]

K_1 <=> j = [j + S[i] + K[i mod length (K)]] mod 256

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

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

j = (116 + 97) mod 256

j = 213 //

swap (S[i], S[j])
swap (S[1], S[213]) } Array S = [115, 213, 2, 3, ..., 112, 113, 114, 0, 116, ... 212, 1, 214, ..., 252, 253, 254, 255]

K_2 <=> j = [j + S[i] + K[i mod length (K)]] mod 256

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

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

j = (215 + 112) mod 256

j = 327 mod 256

j = 71 //

KIKY

Date

Swap (S[i], S[j])
Swap (S[2], S[71])
} Array S = [115, 213, 71, 3, 4, ..., 69, 70, 2, 72, 73, ... 112, 113, 114, 0, 116, ..., 212, 1, 214, ..., 250, 251, 252, 253, 254, 255]

K3 (=) j = (j + S[i] + K[i mod length (K)]) mod 256
j = (71 + S[3] + K[3 mod length (8)]) mod 256
j = (71 + 3 + K[3]) mod 256
j = (74 + 117) mod 256
j = (191) mod 256
j = 191 ✓

Swap (S[i], S[j])
(S[3], S[191])
} Array S = [115, 213, 71, 191, 4, ..., 70, 2, 72, 73, ..., 113, 114, 0, 116, ..., 189, 190, 3, 192, ..., 210, 211, 212, 1, 214, ... 253, 254, 255]

K4 (=) j = (j + S[i] + K[i mod length (K)]) mod 256
j = (191 + S[4] + K[4 mod length (8)]) mod 256
j = (191 + 4 + K[4]) mod 256
j = (195 + 116) mod 256
j = 311 mod 256
j = 55 ✓

Swap (S[i], S[j])
(S[4], S[55])
} Array S = [115, 213, 71, 191, 55, 5, ..., 50, 51, 52, 53, 54, 4, ... 70, 2, 72, 73, ..., 113, 114, 0, 116, ... 189, 190, 3, 192, ..., 210, 211, 212, 1, 214, ..., 253, 254, 255]

K5 (=) j = (j + S[i] + K[i mod length (K)]) mod 256
j = (55 + S[5] + K[5 mod length (8)]) mod 256
j = (55 + 5 + K[5]) mod 256
j = (60 + 114) mod 256
j = 174 ✓

Swap (S[i], S[j])
(S[5], S[174])
} Array S = [115, 213, 71, 191, 55, 174, ..., 50, 51, 52, 53, 54, 4, ... 70, 2, 72, 73, ... 113, 114, 0, 116, ... 172, 173, 5, 175, ..., 189, 190, 3, 192, ..., 210, 211, 212, 1, 214, ..., 253, 254, 255]

KIKY

Date

K6 => j = (j + S[i] + K[i mod length(K)]) mod 256
j = (174 + S[6] + K[6 mod length(8)]) mod 256
j = (174 + 6 + K[6]) mod 256
j = (180 + 97) mod 256
j = (277) mod 256
j = 21 ,,

Swap (S[i], S[j])
(S[6], S[21])
} Array S = [115, 213, 71, 191, 55, 174, 21, ..., 20, 6, 22, ... 53, 54, 4, ... 70, 2, 72, 73, ..., 113, 114, 0, 116, ..., 172, 173, 5, 175, ..., 189, 190, 3, 192, ..., 211, 212, 1, 214, ... 253, 254, 255]

K7 => j = (j + S[i] + K[i mod length(K)]) mod 256
j = (21 + S[7] + K[7 mod length(8)]) mod 256
j = (21 + 7 + K[7]) mod 256
j = (28 + 99) 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, ..., 20, 6, 22, ..., 53, 54, 4, ..., 70, 2, 72, 73, 74, 75, 76, 7, ... 113, 114, 0, 116, ..., 172, 173, 5, 175, ..., 189, 190, 3, 192, ..., 211, 212, 1, 214, ..., 253, 254, 255]

Metode PRGA

•> P = 2003

i = 0

j = 0

for index = 0 to length (P) - 1

for index = 0 to (4) - 1

i = (0+1) mod 256

i = 1 "

j = (j + S[1]) mod 256

j = (0 + 213) mod 256

j = 213

=> S[i], S[j] } t = S[213] + S[1] = ke index

S[1], S[213] } t = 214 "

u = S[214]

c = 214 ⊕ P[idx]

= 214 ⊕ P[0]

= 214 ⊕ 2 = 11010110

00110010 ⊕

11100000

= 228 = ä

• i = 1

j = 213

for index = 0 to length (P) • - 1

= 0 to (4) - 1

i = (i + 1) mod 256

i = (1+1) mod 256 = 2 mod 256

i = 2 "

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

= (213 + S[2]) mod 256

= (213 + 71) mod 256

KIKY = 284 mod 256

j = 28 "

Date

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

t = (S[2] + S[28]) mod 256
t = (28 + 71) mod 256
= 99 //

u = S[99]
c = u ⊕ P[1]
= 99 ⊕ 0
= 01100011
00110000 ⊕
01010011 = 83 S (capital S) //

•> 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
j = (219) mod 256

swap (S[3] + S[219])
t = (S[3] + S[219])
t = 219 + 191 mod 256
t = 154

u = S[154]
c = u ⊕ P[2]
= 154 ⊕ 0
= 10011010
00110000 ⊕
00101010 => 42 * (Asterisk)

KIKY

Date

$i = 3$, $j = 219$

for index = 0 to (3)

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

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

$i = 4$ //

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

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

$= (219 + 55) \bmod 256$

$= (274) \bmod 256$

$j = 18$ //

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

$t = 18 + 55 \bmod 256 = 73$

$u = S[73]$

$C = u \oplus P[3]$

$= 73 \oplus 3$

$= 01001001$

$\quad\; 00110011$

$01111010 \oplus$ z (small z)

$= 122$ //