Kryptografi

Nama : La Ode Yamin Arsy Fadillah Mbota

NIM : E1E1 20 077

Kelas : Ganjil

KSA (Key Scheduling Algorithm)

Inisilisasi : $S_0 = S_1 \ldots S_{255} = 255$

Key = Sopulcas → length key = 8

Iterasi Ke-0

$i = 0 \quad j = 0 \quad s = 115$

$j = (j + S[i] + k[i \bmod \text{len}(k)]) \bmod 256$

$= (0 + 0 + k[0 \bmod 8]) \bmod 256$

$= (0 + k[0]) \bmod 256$

$= (0 + 115) \bmod 256$

$= 115 \bmod 256$

$j = 115$

No.

Date

swap : s[i], s[j] = s[0], s[115]

S : 115, 2, 11, 5, 6, 7, ..., 114, 0, 116, ..., 255

Iterasi Ke-1

i = 1   j = 115   a = 97

j = (j + s[i] + k[i mod len[k]) mod 256

= (115 + 1 + k[i mod 8]) mod 256

= (116 + k[1]) mod 256

= (116 + 97) mod 256

= 213 mod 256

j = 213

swap : s[i], s[j], = s[1], s[213]

S : 115, 213, 3, 4, 5 ...., 114, 0, 116 212, 1, 2

..., 255

Iterasi Ke-2

i = 2   j = 213   p = 112

j : (j + S [i] + k [i mod len (k)] mod 256

= (213 + 2 + k (2 mod 8]) mod 256

= (215 + k [2]) mod 256

= (215 + 112) mod 256

= 327 mod 256

J = 71

Swap : S [i] , s [j] : s [2] , s [71]

S = 115, 213, 71, 3, 4, 5, ..., 70, 2, 72, ..., 114, 0, 116

, ..., 212

Iterasi Ke - 3

i = 3   J = 71   u = 117

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

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

: 74 + k (3]) mod 256

= (74 + 117) mod 256

= 191 mod 256   J = 191

Suap : S[i], S[j] : S[3], S[191]

S = 115, 213, 71, 191, 4, 5, ..., 70, 2, 73, ..., 114, 0, 116,

...., 190, 3, 192, ..., 212, 1, 214, ..., 255

iterasi ke-4

i = 4 j = 191 t = 116

j = (j + S[i] + K[i mod len[K] mod 256

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

= (195 + 116) mod 256

= 311 mod 256

j = 55

Swap : S[i], S[j] = S[4], S[55]

S = 115, 213, 71, 191, 55, 5, ..., 54, 4, 56, ..., 70, 2, 72, ...

114, 0, 116, ..., 190, 3, 192, ... 212, 1, 214, ..., 255

Date

Iterasi Ke-5

i = 5   j = 55   r = 114

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

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

= (60 + 114) mod 256

= 174 mod 256

j = 174

Swap = S[i], S[j] = S(5), S [174]

S = 115, 213, 71, 191, 55, 174, 6, ..., 54, 4, 56, ..., 70,

2, 72, ..., 114, 0, 116, ..., 190, 3, 192, ..., 212, 1, 214,

.... 255

Iterasi Ke-6

i = 6   j = 174   a = 97

j = (j + i + k[i mod len [k]) mod 256

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

= (180 + 97) mod 256

= 277 mod 256

j = 21

Swap = S[i], S[j] = S[6], S(21]

S = 115, 213, 71, 191, 55, 74, 21, 7, ..., 20, 6, 22, ... , 54, 4, 56

..., 70, 2, 72, ..., 114, 0, 116, ..., 173, 5, 175, ..., 190, 3, 192

..., 212, 1, 214, ..., 255

Iterasi ke-7

i = 7 j = 21 k = 49

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

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

= (28 + 49) mod 256

j = 77 mod 256

j = 77

Swap = S[i], S[j] = S[7], S[77]

S = 115, 213, 71, 191 55, 74, 21, 77, 8, ..., 20, 6, 22, ...

54, 4, 56, ..., 70, 2, 72, ..., 76, 7, 78, ..., 114, 0, 116,

..., 173, 5, 175, ..., 190, 3, 192, ... 212, 1, 214, ..., 255

Nama : Laode Yamin Arsy Fadillah Mbota

NIM = E1E1 20077

Pseudo Random Generation Algorithm (PRGA)

Plainteks : [redacted] 20077

Iterasi ke - 1

```
i = 0     j = 0
For Idx = 0 to length (p) - 1 do
        = 0 to len (s) - 1 do
        = 0 to 4 do
  i = (i + 1) mod 256
  i = (0 + 1) mod 256
  i = 1
j = (j + S[i]) mod 256
J = (0 + 213) mod 256 // nilai i diambil dari Array
J = 213                 sebelumnya di KSA
```

Swap : S[i], S[j] = S[1], S[213]

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

u = S[t]

= (1 + 213) mod 256

= 214 mod 256

t = 214

= S[214]

C = u $\oplus$ p[0]

= 214 $\oplus$ 2

⇒ Binary ⇒ 214 ⇒ 11010110

$$\begin{array}{r} 11010110 \\ 00110010 \\ \hline 11100100 \end{array} \quad \oplus \text{ XOR}$$

11100100 → 228 ⇒ ä

Iterasi ke-2

i = 1 , j = 213

For Index = 0 to 4

i = (i+1) mod 256

i = (1 + 1) mod 256

= 2 mod 256

= 2

No.

Date

$j : (s[i], s[j]) \bmod 256$

$= 213 + s[2]) \bmod 256$

$= 213 + 71) \bmod 256$

$= 284 \bmod 256$

$j = 28$

$t = (s[i], s[j]) = (s[2], s[28])$

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

$= (99) \bmod 256$

$= 99$

$C = u \oplus P[i]$

$= 99 \oplus 0$

$\Rightarrow$ 01100011

00110000 $\oplus$

01010011 $\Rightarrow$ Chr $\Rightarrow$ S (kapital)

Iterasi ke-3

i = 2   J = 28

for ldx = 0 to 4 do

i = (2+1) mod 256

i = 3 mod 256

i = 3

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

= 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

= (219 + 191) mod 256

= 410 mod 256

= 154

U = S [154]   → 10011010

C = U $\oplus$ 0   00110000 . Dec = 170

=   10101010 afzil : a

Iterasi ke-4

i = 3   J = 219

For idx = 0 to 4 do

i = (3+1) mod 256

= 4

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

= (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

= (18 + 55) mod 256

= 73

u = S (73

C = u ⊕ P [3]

= 73 ⊕ 7

Binarry = 10011010   Desimal : 173

00110111 ⊕   ascii : i

10101101

Iterasi ke-5

i = 4 J = 18

for Idx = 0 to 4 do

i = (4+1) mod 256

= 5

j = (18 + 174) mod 256

= 192 mod 256 ⇒ J = 192

swap = S [i J, S [j] = S [5], S [192]

t = (192 + 174) mod 256

= (366) mod 256

t = 110

U = S [110]

C = U ⊕ P [7] ⇒ 110 ⊕ 7

0110 1110

00110111 ⊕ Desimal = 84

01011001 Ascii : Y (kapital)