Nama : La Ode Muhamad Ilham
Nim : E1E12030
Kelas : Genap
Mata kuliah : Kriptografi

KSA (key Scheduling Algorithem)

Inisialisasi : $S_0 = S_1 \cdots S_{255} = 255$

Key = Saputra1 → length key = 8

Iterasi ke-0

i = 0 j = 0 s = 115
j = (j + s [i] + k (i mod len (k)]) mod 256
= (0 + 0 + k [0 mod 8]) mod 206
= (0 + k [0] mod 256
= (0 + 115) mod 256
= 115 mod 256
J = 115
swap = S[i], S[j] = S[0], S[115]
S = 115, 2, 3, 4, 5, 6, 7 ..., 114, 0, 116 .. 255

Iterasi ke-1

i = ~~0~~ 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, 214, .. 225

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
1, 214 ... 255.

Iterasi ke-3
i = 3 J = 71 u = 117
~~Iterasi~~
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
swap = S[i], S[J] = S [3], S[191]
S = 115, 213, 71, 191, 4, 5 ... 70, 2, 73, ...
114, 0, 116, ... 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 + k [4])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, ... 144 ..
0, 116, ..., 190, 3, 192 .. 212, 1, 214 ... 255

Algoritma : Pseudo -random Generation Algoritham (PRGA)

Array s : [115, 213, 71, 191, 55, 124, 21, 77, 8 ··, 19, 20, 6, 22, 23
53, 54, 4, 56, 56, ··· 69, 70, 2, 72, 73, 74, 75, 76, 7, 78 ·· 113
114, 0, 116, 117, ·· 172, 173, 5, 125, 176. ·· 189, 190, 3, 192
193, 8 ·· 211, 212, 1, 214, 215 ... 250, 251, 252, 253, 254, 255]

Plaintexs = "2090"

- Iterasi pertama - idx = 0

i = 0
j = 0

=> i = (i+1) % 256
= (0+1) % 256
= 1 % 256
= 1

=> j = (j + s (i]) % 256
= (0 + s(1]) % 256
= (0 + 213) % 256
= 213

Swap (s[i], s(j])
Swap (s[1], s[213])

Array s = [115, 1, 71, 191, 55, 174, 21, 77, 8, ··· , 19, 20, 6, 22, 23 ···
53, 54, 4, 56, 57 ·· 69, 70, 2, 72, 73, 74, 75, 76, 7, 78 ···
113, 114, 0, 116, 111, ·· 122, 173, 5, 175 176, 189, 190, 3, 192,
193, ·· 212, 213, 214, ·· 250 : 251, 253, 254, 255]

=> t = (s [i] + s [j]) % 256
= (s [1] + s{213]) % 256
= (1 + 213] % 256
= 214

=> = s(t)
= s (214] = 214 => biner 214 = 11010110

=> = u ⊕ p [idx]
= u ⊕ p [0]
= u ⊕ "2" => biner "2" = 110010

= 11010110
00110010 ⊕

11100100

c = "q" didesimalkan menjadi 223

Iterasi kedua → idx = 1

i = 1
j = 213

=> i = (i + 1) % 256
= (1 + 1) % 256
= 2

=> j = (j + S[i] % 256
= (213 + S[2] % 256
= (213 + 71) % 256
= 284 % 256
= 28

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

Array S = [115, 1, 28, 191, 55, 174, 21, 77, 8, .. 19, 20, 6, 22, 23, .. 26
27, 71, 29, 30 ... 53, 54, 4, 56, 57, ... 69, 70, 7, 72, 73
74, 75, 76, 7, 78 ... 113, 114, 0, 116, 117, ... 172, 173, 5, 175
176, ... 189, 190, 3, 192, 193, .. 212, 213, 219, 215, ...
250, 251, 252, 253, 254, 255]

=> t = (S[i] + S[j] % 256)
= (S[2] + S[28] % 256)
= (28 + 71) % 256
= 99 % 256
= 99

=> u = S[t]
= S[99]
= 99 => biner 99 : 1100011

=> c = u ⊕ P[idx
= u ⊕ P[1]
= u ⊕ "0" => biner "0" = 110000
= 1100011
110000
―――――
1110011

c = "S" desimal = 83

Iterasi ketiga = idx = 2

i = 2, j = 28
i = (i+1) % 256
= (2 + 1) % 256
= 3

Swap (S[i]), S[j])
Swap (S[3]). S[219])

Array S = [115, 1, 28, 219, 55, 174, 21, 77, 8, ... 19, 20, 6 22, 23, 26
27, 71, 29, 30, 53, 54, 4, 56, 57, ..69, 70, 2, 72, 73, 74,
75, 76, 7, 78, 79, 113, 114, 0, 116, 117, ..., 172, 173, 5, 175,
176, .., 189, 190, 3, 192, 193 .. 212, 213, 214, 215, 216, 217,
218, 191, 220, .. 253, 254, 255]

=> t = (S[i]] + (S[j]) % 256
= (S[3]] + S[219]) % 256
= (219 + 191) % 256
= 410 % 256
= 154

=> u = S[t]
= S[154]
= 154 biner 154 =

=> c = u ⊕ P[idx]
~~c~~ = u ⊕ P[2]
= u ⊕ "3" => biner "3" = 110011
= 10011010
110011
――――――
10101001

c = "C" desimal 169

- Iterasi keempat => idx = 3

i = 3, j = 219

=> i = (i + 1) % 256
= (3 + 1) % 250
= 4

=> j = (j + S[i]) % 256
= (219 + S[4]) % 256
= (219 + 55) % 526
= 274 % 256
= 18

Swap (S[i], S[j])
Swap (S(4], S(18))

Array S = [115, 1, 28, 219, 18, 174, 21, 77, 8, ..., 16
17, 55, 19, 20, 6, 22, 23, 24, 25, 26, 27
71, 29, 30, ... 53, 54, 4, 56, 57, 69, 70, 71,
72, 73, 74, 75, 76, 7, 78, 79 .. 113, 114, 0,
116, 117 .., 172, 173, 5, 175, 176, ... 189, 190
3, 192, 193 .. 212, 213, 214, 215, 216, 217, 218
191, 220 .. 253, 254, 255]

=> t = (S[i] + j [J] % 256
= (S [4] + S [18] % 256
= 18 + 55 % 256
= 73

=> u = S [t]
= S [73]
= 73 => Biner 73 = 1001001

=> c = 4 ⊕ p [idx]
= 4 ⊕ p [3]
= 4 ⊕ "0" => biner "0" = 110000
= 1001001
  110000 ⊕
  ―――――
  1111001

C = "y" desimal = 121