Nama : Muh. Rahmat Dhyan F.
Nim : E1E120084
Kelas : Genap
Mata kuliah : Kriptografi

KSA (key scheduling Algorithm)

inisilisasi : $S_0 = S_1 \dots S_{255} = 255$
Key = Saputra1 → length key = 8

Iterasi ke - 0
$i = 0 \quad j = 0 \quad S = 115$
$j = (j + S[i] + k[i \bmod len(k)]) \bmod 256$
$= (0 + 0 + k[0 \bmod 8]) \bmod 256$
$= (0 + k[0]) \bmod 256$
$= (0 + 115) \bmod 256$
$= 115 \bmod 256$
$j = 115$
swap = $S[i], S[j] = S[0], S[115]$
S = 115, 2, 3, 4, 5, 6, 7, ..., 114, 0, 116, ..., 255

Iterasi ke - 1
$i = 1 \quad j = 115 \quad a = 97$
$j = (j + S[i] + k[i \bmod len(k)]) \bmod 256$
$= (115 + 1 + k[i \bmod 8]) \bmod 256$
$= (116 + k[1]) \bmod 256$
$= (116 + 97) \bmod 256$
$= 213 \bmod 256$
$j = 213$
Swap = $S[i], S[j] = S[1], S[213]$
S = 115, 213, 3, 4, 5, ..., 114, 0, 116, ..., 212, 1, 214, ... 255

Iterasi ke - 2
$i = 2 \quad j = 213 \quad P = 112$
$j = (j + S[i] + k[i \bmod len(k)]) \bmod 256$
$= (213 + 2 + k[2 \bmod 8]) \bmod 256$
$= (215 + k[2]) \bmod 256$
$= (215 + 112) \bmod 256$
$= (327 \bmod 256) \Rightarrow j = 71$

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

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 + k[5]) 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 + S[i] + k[i mod len(k)]) mod 256

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

= (180 + k[6]) mod 256

~~(180 + 174) mod 256~~ (180 + 97) mod 256

= ~~277 mod~~ 277 mod 256

j = 21

swap . S[i], S[j] = S[6], S[21]

S = 115, 213, 71, 191, 55, 174, 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 1 = 49

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

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

= (28 + k[7]) mod 256

= (28 + 49) mod 256

= 77 mod 256

j = 77

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

S = 115, 213, 71, 191, 55, 174, 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 : Dauh - Rahmat Dhyan F.
Nim : E1E120084
Kelas : Genap
Mata kuliah : Kriptografi

Pseudo Random generation Algoritthm (PRGA)

Plainteks = 20084

- Iterasi Pertama
  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 sebelumnya di KSA
  j = 213 mod 256
  j = 213
  Swap = S[i], S[j] = S[1], S[213]
  t = (S[1] + S[j]) mod 256
  u = S[t]
  = (1 + 213) mod 256
  = 214 mod 256
  t = 214
  = S[214]
  c = u ⊕ P[0]
  = 214 ⊕ 2
  ⇒ Binary ⇒ 214 ⇒ 11010110
  2 ⇒ 00110010 ⊕ 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

j = (S[i], S[j]) mod 256
Swap = (213 + S[2]) mod 256
= (213 + 71) mod 256
= 284 mod 256
j = 28
t = (S[i], S[j]) = (S[2], S[28])
t = (S[2] + S[28]) mod 256
= (71 + 28) mod 256
= (99) mod 256
= 99
C = U ⊕ P[1]
= 99 ⊕ 0
⇒ 01100011
00110000 ⊕
01010011 → Chr => S (kapital)

- iterasi ke-3
i = 2 j = 28

for idx = 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]
C = U ⊕ P[2]
= 154 ⊕ 0
= 10011010
00110000 Dec = 170 asCii = ª
10101010

- 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 ⊕ 8

Binary = 01001001

00111000 ⊕

01110001

Dec = 113 ascii = 9

- 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], S[j] = S[5], S[192]

t = (192 + 174) mod 256

= (366) mod 256

t = 110

u = S[110]

C = u ⊕ P[4] ⇒ = 110 ⊕ 4

= 01101110

00110100 ⊕

01011010

Dec = 90

Ascii = Z (kapital)