No.

Date :

Nama : Ilmi Faizan
NIM : E1E120011
Mata Kuliah : Kriptografi

* Algoritma Key Scheduling Algorithm (KSA)

Array S = [0, 1, 2, 3, 4, 5, 6, ..., 253, 254, 255]

Kunci = saputra1 → panjang = 8 karakter.

1) i = 0, j = 0 — swap(S[i], S[j])

j = (j + S[i] + k[i mod length(kunci)]) mod 256 — swap(0, 115)

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

j = 115 mod 256

j = 115

Array S = [115, 1, 2, 3, 4, ..., 114, 0, 116, ..., 253, 254, 255]

2) i = 1, j = 115

j = (115 + 1 + k[1 mod 8]) mod 256 — swap(S[i], S[j])

j = (116 + 97) mod 256 — swap(1, 213)

j = 213 mod 256

j = 213

Array S = [115, 213, 2, 3, 4, ..., 114, 0, 116, ..., 212, 1, 214, ..., 253, 254, 255]

3) i = 2, j = 213

j = (213 + 2 + k[2]) mod 256 — swap(S[i], S[j])

j = (215 + 112) mod 256 — swap(2, 71)

j = 327 mod 256

j = 71

Array S = [115, 213, 71, 3, 4, ..., 70, 2, 72, ..., 114, 0, 116, ..., 212, 1, 214, ..., 253, 254, 255]

4) i = 3, j = 71

j = (71 + 3 + k[3]) mod 256 — swap(S[i], S[j])

j = (74 + 117) mod 256 — swap(3, 191)

j = 191 mod 256

j = 191

Array S = [115, 213, 71, 191, 4, 5, ..., 70, 2, 72, ..., 114, 0, 116, ..., 190, 3, 192, ..., 212, 1, 214, ... 253, 254, 255].

No.

Date :

5) $i = 4,\ j = 191$

$j = (191 + 4 + k[4]) \bmod 256$ swap (S[i], S[j])

$j = (195 + 116) \bmod 256$ swap (4, 55)

$j = 311 \bmod 256$

$j = 55$

Array S = [115, 213, 71, 191, 55, 5, 6, ..., 59, 4, 56, ..., 70, 2, 72, ..., 119, 0, 116, ..., 190, 3, 192, ... 212, 1, 214, ..., 253, 254, 255].

6) $i = 5,\ j = 55$

$j = (55 + 5 + k[5]) \bmod 256$ swap (S[i], S[j])

$j = (60 + 114) \bmod 256$ swap (5, 174)

$j = 174 \bmod 256$

$j = 174$

Array S = [115, 213, 71, 191, 55, 174, 6, 7, ..., 59, 4, 56, ..., 70, 2, 72, ..., 119, 0, 116, ..., 173, 5, 175, ... 190, 3, 192, ..., 212, 1, 214, ..., 253, 254, 255].

7) $i = 6,\ j = 174$

$j = (174 + 6 + k[6]) \bmod 256$ swap (S[i], S[j])

$j = (180 + 97) \bmod 256$ swap (6, 21)

$j = 277 \bmod 256$

$j = 21$

Array S = [115, 231, 71, 191, 55, 179, 21, 7, 8, ..., 20, 6, 22, ..., 54, 4, 56, ..., 70, 2, 72..., 119, 0, 116, ... 173, 5, 175..., 190, 3, 192. ... 212, 1, 214, ..., 253, 254, 255].

8) $i = 7,\ j = 21$

$j = (21 + 7 + k[7]) \bmod 256$

$j = (28 + 49) \bmod 256$

$j = 77 \bmod 256$

$j = 77$

Array S = [115, 231, 71, 191, 55, 174, 21, 77, 8, 9, ..., 20, 6, 22, ... 54, 4, 56, ... 70, 2, 72. ..., 76, 7, 78, ..., 119, 0, 116, ..., 173, 5, 175, ..., 190, 3, 192, ..., 212, 1, 214, ..., 253, 254, 255].

No.

Date :

* Algoritma Pseudo-random generation algorithm (PRGA)

Array S = [115, 213, 71, 191, 55, 174, 21, 77, 8, 9, ..., 20, 6, 22, ..., 54, 9, 56, ..., 70, 2, 72, ..., 76, 7, 78, ..., 114, 0, 116, ..., 173, 5, 175, ..., 190, 3, 192, ..., 212, 1, 214, ..., 253, 254, 255].

Plaintext = "2011"

1) idx = 0, i = 0, j = 0

⇒ i = (i + 1) mod 256
= (0 + 1) mod 256
= 1

⇒ j = (j + S[i]) mod 256
= (0 + S[1]) mod 256
= 213

swap (S[i], S[j]) → swap (213, 1)
swap (S[1], S[213])

Array S = [115, 1, 71, 191, 55, 174, 21, 77, 8, ..., 20, 6, 22, ..., 54, 9, 56, ..., 70, 2, 72, ..., 76, 7, 78, ..., 114, 0, 116, ..., 173, 5, 175, ..., 190, 3, 192, ..., 212, 213, 214, ..., 253, 254, 255]

⇒ t = (S[i] + S[j]) mod 256
= (S[1] + S[213]) mod 256
= (1 + 213) mod 256
= 214

⇒ u = S[t]
= S[214]
= 214 = 11010110

⇒ c = u ⊕ P[idx]
= u ⊕ P[0]
= u ⊕ "2"
= 11010110
00110010
11100100 → konversi ke desimal
c = 228 → ä

2) idx = 1, i = 1, j = 213

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

⇒ j = (j + S[i]) mod 256
= (213 + 71) mod 256
= 28

swap (S[i], S[j]) → swap (71, 28)
swap (S[2], S[28])

Array S = [115, 1, 28, 191, 55, 174, 21, 77, 8, ..., 20, 6, 22, ..., 27, 71, 29, ..., 54, 9, 56, ..., 70, 2, 72, ..., 76, 7, 78, ..., 114, 0, 116, ..., 173, 5, 175, ..., 190, 3, 192, ..., 212, 213, 214, ..., 253, 254, 255].

⇒ t = (S[i] + S[j]) mod 256
= (S[2] + S[28]) mod 256
= (28 + 71) mod 256
= 99

⇒ u = S[t]
= S[99]
= 99 = 01100011

⇒ c = u ⊕ P[idx]
= u ⊕ P[1]
= u ⊕ "0"
= 01100011
00110000
01010011 → konvert ke desimal
c = 83 → S

No.

Date :

3) idx = 2, i = 2, j = 28

⇒ i = (i+1) mod 256
= (2+1) mod 256
= 3

⇒ j = (j + S[i]) mod 256
= (28 + 191) mod 256
= 219

Swap(S[i], S[j]) → swap(191, 219)
swap(S[3], S[219])

Array S = [115, 1, 28, 219, 55, 174, 21, 77, 8, ..., 20, 6, 22, ..., 27, 71, 29, ..., 59, 9, 56, ..., 70, 2, 72, ... 76, 7, 78, ..., 114, 0, 116, ..., 173, 5, 175, ..., 190, 3, 192, ..., 212, 213, 214, ..., 218, 191, 220, ... 253, 254, 255].

⇒ t = (S[i] + S[j]) mod 256
= (S[3] + S[219]) mod 256
= (219 + 191) mod 256
= 154

⇒ u = S[t]
= S[154]
= 154 = 10011010

⇒ c = u ⊕ P[idx]
= u ⊕ P[2]
= u ⊕ "1"
= 10011010
00110001
10101011 → konvert ke desimal
c = 171 → «

4) idx = 3, i = 3, j = 219

⇒ i = (i+1) mod 256
= (3+1) mod 256
= 4

⇒ j = (j + S[i]) mod 256
= (219 + S[4]) mod 256
= (219 + 55) mod 256 = 18

Swap(S[i], S[j]) → Swap(55, 18)
swap(S[4], S[18])

Array S = [115, 1, 28, 219, 18, 174, 21, 77, 8, ..., 17, 55, 19, 20, 6, 22, ..., 27, 71, 29, ..., 59, 9, 56, ..., 70, 2, 72, ..., 76, 7, 78, ..., 114, 0, 116, ..., 173, 5, 175, ..., 190, 3, 192, ..., 212, 213, 214, ..., 218, 191, 220, ..., 253, 254, 255].

⇒ t = (S[i] + S[j]) mod 256
= (S[4] + S[18]) mod 256
= (18 + 55) mod 256
= 73

⇒ u = S[t]
= S[73]
= 73 = 01001001

⇒ c = u ⊕ P[idx]
= u ⊕ p[3]
= u ⊕ "1"
= 01001001
00110001
01111000 → konversi ke desimal
c = 120 → x

Plaintext = 2011
Enkripsi = äSxx