No.

Date :

Nama : Muh. Bayu Aidil Adhalik T.
NIM : E1E120078
Kelas : Genap
Tugas II Kriptografi

1. Algoritma : Key-Scheduling Algorithm (KSA)
Kunci : saputra1 (8) => leng(k)
Array s : [0,1,2,3,4,5,6,7,8,9,10, ... , 100,101,102, ... ,253,254,255]

a) Iterasi pertama : i = 0 , K[0] = s => 115
j = 0
j = (j + s[i] + k[i mod len(k)]) mod 256
= (0 + 0 + k[0 mod 8]) mod 256
= (k[0]) mod 256
= ("s") mod 256
= 115 mod 256
= 115
Swap (S[i], S[j])
swap (S[0], S[115])
Array s : [115, 1,2,3,4,5,6,7,8,9,10, ... , 110, 111, 112, 113, 114, 0, 116, 117, 118, ... , 253, 254, 255]

No.

Date :

(b.) Iterasi kedua : $i = 1$, $K_1 = a \Rightarrow 97$

$j = 115$

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

$= (115 + S(1) + K[1 \bmod 8]) \bmod 256$

$= (115 + 1 + K[1]) \bmod 256$

$= (116 + K[1]) \bmod 256$

$= (116 + \text{"a"}) \bmod 256$

$= (116 + 97) \bmod 256$

$= 213 \bmod 256$

$= 213$

Swap (S[i] = S[j])

Swap (S[1] = S[213])

Array S : [115, 213, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, ... , 113, 114, 0, 116, ... , 212, 1, 214, 215, ... , 254, 255]

(c.) Iterasi ketiga : $i = 2$, $K_2 = p \Rightarrow 112$

$j = 213$

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

$= (213 + S(2) + K[2 \bmod 8]) \bmod 256$

$= (213 + 2 + K[2]) \bmod 256$

$= (215 + K[2]) \bmod 256$

$= (215 + \text{"p"}) \bmod 256$

$= (215 + 112) \bmod 256$

$= 327 \bmod 256$

2.

No.

Date :

j = 71

swap = (S[i], S[j])

Swap = (S[2], S[71])

Array S = [115, 213, 71, 3, 4, 5, 6, 7, 8, 9, 10, ... , 69, 70,
2, 72, 73, ... , 113, 114, 0, 116, ... , 211, 212,
1, 214, ... , 253, 254, 255]

(d.) Iterasi keempat : $i = 3$, $K_3 = u$ => 117

j = 71

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

= (71 + S(3) + K[3 mod 8]) mod 256

= (71 + 3 + K[3]) mod 256

= (74 + K[3]) mod 256

= (74 + "u") mod 256

= (74 + 117) mod 256

= 191 mod 256

= 191

swap = (S[i], S[j])

= (S[3], S[191])

Array S = [115, 213, 71, 191, 4, 5, 6, 7, 8, ... 70, 2, 72, 73,
..... , 113, 114, 0, 116, ... , 190, 3, 192, ... , 211,
213, 214, ... 0, 216, ... , 189, 190, 3, 192, ... ,
210, 211, 212, 1, 214, ... 253, 254, 255].

No.

Date :

(e) Iterasi kelima → i = 4 k_4 = t = 116

j = 191

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

= (191 + S[4] + k[4 mod 8]) mod 256

= (191 + 9 + k[4]) mod 256

= (195 + "t") mod 256

= (195 + 116) mod 256

= 311 mod 255

= 55

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

Swap (S[4], S[55])

Array S = [115, 213, 71, 191, 55, 5, 6, 7, 8, ..., 53, 54, 4, 56, 57, ..., 69, 70, 2, 72, 73, ..., 113, 114, 0, 116, 117, ..., 189, 190, 3, 192, ..., 211, 212, 1, 214, ..., 250, 251, 252, 253, 254, 255]

(f) Iterasi keenam → i = 5 k_5 = r = 114

j = 55

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

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

= (55 + 5 + k[5] mod 256

= (60 + "r") mod 256

= (60 + 114) mod 256

= 174 mod 255

= 174

4.

No.

Date :

Array S = [115, 213, 71, 191, 55, 174, 6, 7, 8, ..., 53, 54, 4, 55, 57, ..., 69, 70, 2, 72, 73, ..., 113, 114, 0, 116, 117, ..., 173, 5, 175, 176, ..., 190, 3, 192, 193, ..., 212, 1, 214, 215, ..., 253, 254, 255]

(9.) Iterasi ketujuh karena → i = 6, k_5 = "a" → 97

j = 174

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

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

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

= (180 + "a") mod 256

= 277 mod 256

= 21

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

Swap (s[6], s[174])

Array S = [115, 213, 71, 191, 55, 174, 21, 7, 8, ..., 19, 20, 6, 22, 23, ..., 53, 54, 4, 56, 57, ..., 69, 70, 2, 72, 73, ..., 113, 114, 0, 116, 117, ..., 172, 173, 5, 175, 176, ..., 189, 190, 3, 192, 193, ..., 211, 212, 1, 214, 215, ..., 253, 254, 255]

5.

(h.) Iterasi kedelapan → i = 7, k_7 = 1 ⇒ 49

j = 21

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

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

= (21 + 7 + K[7]) mod 256

= (28 + "1") mod 256

= (28 + 49) mod 256

= 77 mod 256

= 77

swap (S[i], S[j])

swap (S[7], S[77])

Array S = [115, 213, 71, 191, 55, 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, 117, ..., 172, 173, 5, 175, 176,
..., 189, 190, 3, 192, 193, ..., 211, 212, 1, 214, 215,
..., 253, 254, 255].

6.

No.

Date :

2. Algoritma : Pseudo-random Generation Algoritm (PGRA)

Array S : [115, 213, 71, 191, 55, 174, 21, 77, 8, ..., 19, 20, 6, 22, ...
53, 54, 4, 56, 57, ... , 69, 70, 2, 72, 73, 74, 75, 76, 7, 78, ...
113, 114, 0, 116, 117, ..., 172, 173, 5, 175, 176, ..., 189, 190,
3, 192, 193, ..., 211, 212, 1, 214, 215, ..., 250, 251,
252, 253, 254, 255]

Plainteks : "2078"

- Iterasi pertama : idx = 0

  i = 0

  j = 0

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

  * j = (j + s[i]) mod 256
    = (0 + s[i]) mod 256
    = (0 + 213) mod 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, 117, ..., 172, 173, 5, 175, 176,
  ...., 189, 190, 3, 192, 193, ..., 212, 213, 214, ...,
  253, 254, 255]

  * t = (s[i] + s[j] mod 256
    = (s(1) + s(213)] mod 256
    = (1 + 213) mod 256

  t = 214

7.

No.

Date :

* u = S[t]
  = S[214] = 214 => binernya = 11010110
* C = u ⊕ P[idx]
  = u ⊕ P[0]
  = u ⊕ "2" => biner "2" = 110010
  = 11010110
    00110010 ⊕
    11100100
  = "ä", didecimalkan menjadi 228

- Iterasi kedua → idx = 1
  i = 1
  j = 213

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

* j = (j + S[i]) mod 256
  = (213 + S[2]) mod 256
  = (213 + 71) mod 256
  = 284 mod 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, ..., 27, 71, 29, 30, ..., 53, 54, 9, 56, 57,
..., 69, 70, 2, 73, 74, 75, 76, 7, 78, ..., 113, 114,
0, 116, 117, ..., 172, 173, 5, 175, 176, ..., 189, 190, 3,
192, 193, ..., 212, 213, 215, ..., 253, 254, 255]

8.

No.

Date :

* t = (S[i] + S[j]) mod 256
  = (S[2] + S[28]) mod 256
  = (28 + 71) mod 255
  = 99 mod 256
  = 99

* u = S[t]
  = S[99]
  = 99 ⇒ binernya 1100011

* C = u ⊕ P[idx]
  = u ⊕ P[i]
  = u ⊕ "0" ⇒ binernya 110000
  = 1100011 1100011
    1100011 0110000 ⊕
    1010011
  = "S", desimal = 83

▶ Iterasi ketiga → idx = 2
  j = 28 , i = 2

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

* j = (j + S[i]) mod 256
  = (28 + S[3]) mod 256
  = (28 + 191) mod 256
  = 219 mod 256
  = 219

9.

No.

Date :

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, ..., 27, 71, 29, 30, ..., 53, 54, 4, 56, 57, ..., 69, 70, 2,
73, 74, 75, 76, 7, 78, ..., 113, 114, 0, 116, 117, 118, 3, 120,
120, 122, ..., 172, 173, 5, 175, 176, ..., 189, 190, 3, 192,
193, ..., 212, 213, 219, ..., 253, 254, 255]

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

* u = S[t]
= S[154]
= 154 => binernya = 10011010

* c = u ⊕ p[idx]
= u ⊕ p[2]
= u ⊕ "7" => binernya = ~~00000111~~ 110111
= 10011010 10011010
~~00000111~~ ⊕ 00110111
10011111 10101101
= "_", desimal = 173

No.

Date :

- Iterasi keempat → 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
    = (274) mod 256
    = 18

  swap(S[i], S[j])

  swap(S[4], S[18])

  Array S = [115, 1, 20, 219, 18, 174, 21, 77, 0, ..., 17, 55, 19, 20, 6, 22, 23, ... 27, 71, 29, 30, ..., 53, 54, 54, 56, 57, ..., 69, 70, 2, 73, 74, 75, 7, 78, ..., 113, 114, 0, 116, 117, 118, 3, 120, 121, 122, ..., 172, 173, 5, 175, 176, ..., 189, 190, 3, 192, 193, ..., 212, 213, 214, ..., 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 ⇒ binernya 1001001

No.

Date :

* C = U ⊕ P [CP[idx]]

= U ⊕ P [3]

= U ⊕ "8" => binernya => ~~00~~ 111000

= 01001001
  00001111

  01001110

= 1001001
  0111000
  -------- ⊕
  1110001

= "q", desimal = 161