No.

Date :

Nama : Muh Akbar As'ad

NIM : E1E120035

Mata kuliah : kriptografi

1. Key Scheduling Algorithm (KSA)

Kunci : "Saputra"

len(k) = 8

Array S = [0, 1, 2, 3, 4, 5, 6, 7, ..., 100, 101, 102, 103, ..., 253, 254, 255]

iterasi pertama → i = 0

j = 0

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

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

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

$= ("S") \bmod 256$

$= 115 \bmod 256$

$= 115$

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

swap (S[0], S[115])

Array S = [115, 1, 2, 3, 4, 5, 6, 7, ..., 110, 111, 112, 113, 114, 0, 116, 117, ...,
119, 200, 201, 202, 203, 204, 205, ..., 250, 251, 252, 253, 254, 255]

iterasi kedua → i = 1

j = 115

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

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

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

$= (116 + "a") \bmod 256$

$= (116 + 97) \bmod 256$

$= 213 \bmod 256$

$= 213$

swap (S[1], S[j])

swap (S[1], S[213])

Array S = [115, 213, 2, 3, 4, 5, 6, 7, ..., 112, 113, 114, 0, 116, ..., 210, 211, 212,
1, 214, ..., 250, 251, 252, 253, 254, 255]

No

Date :

iterasi ketiga → i = 2

j = 213

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

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

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

= (215 + "p") mod 256

= (215 + 112) mod 256

= 327 mod 256

= 71

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

swap (S[2], S[71])

Array S = [115, 213, 71, 3, 4, 5, 6, 7, ..., 69, 70, 2, 72, ..., 112, 113, 114, 0,
116, ..., 210, 211, 212, 1, 214, ..., 250, 251, 252, 253, 254, 255]

iterasi keempat → i = 3

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 + "u") mod 256

= (74 + 117) mod 256

= 191 mod 256

= 191

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

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

Array S = [115, 213, 71, 191, 4, 5, 6, 7, ..., 69, 70, 2, 72, ..., 112, 113, 114, 0,
116, ..., 189, 190, 3, 192, ..., 210, 211, 212, 1, 214, ..., 250,
251, 252, 253, 254, 255]

iterasi kelima → i = 4

j = 191

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

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

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

= (195 + "t") mod 256

= (195 + 116) mod 256

= 311 mod 256

= 55

PAPERLINE

swap (s[i], s[j])
swap (s[4], s[55])
Array s = [115, 213, 71, 191, 55, 5, 6, 7, ..., ..., 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]

iterasi ke enam i -> 5
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 + "5") mod 256
= (60 + 114) mod 256
= 174 mod 256
= 174
swap (s[i], s[j])
swap (s[5], s[174])
Array s = [115, 213, 71, 191, 55, 174, 6, 7, 8, ..., 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, ..., 250, 251, 252, 253, 254, 255]

iterasi ke tujuh i -> 6
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
= (180 + 97) mod 256
= 277 mod 256
= 21
swap (s[i], s[j])
swap (s[6], s[21])
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, ..., 250, 251,
252, 253, 254, 255]

iterasi kedelapan i → 7

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, ...,
250, 251, 252, 253, 254, 255]

Pseudo - random generation Algorithm (PRGA)

Array S = [115, 213, 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, ..., 211, 212, 1, 214, 215, ..., 250, 251,
252, 253, 254, 255]

Plainteks = "2035"

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[1]) mod 256
= (0 + 213) mod 256
= 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, ..., 250, 251, 252, 253, 254,
255]

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

u = S[t]
= S[214]
= 214
=> biner 214 => ~~101010~~ 11010110

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

```
  11010110
⊕ 00110010
----------
  11100100
```

c = "ä", didesimalkan menjadi 228

iterasi kedua idx = 1
i = 1
i = 213
i = (i+1) mod 256
= (1+1) mod 256
= 2 mod 256
= 2

j = (i + 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,
..., 26, 27, 71, 29, 30, ..., 53, 54, 4, 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, 214, 215, ..., 250, 251,
252, 253, 254, 255]

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

u = S[t]
= S[99]
= 99 => Biner 99 = 1100011

C = u ⊕ P[idx]
= u ⊕ P[1]
= u ⊕ "0" Biner "0" = 110000

1100011
0110000 ⊕ C = "S", desimal 83
1010011

iterasi ketiga → idx = 2
i = 2, j = 28
i = (i+1) mod 256
= (2+1) mod 256
= 3 mod 256
= 3

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

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, 73,
74, 75, 76, 7, 78, 79, ..., 113, 114, 0, 116, 117, ..., 172, 173, 5,
175, 176, ..., 185, 190, 3, 192, 193, ..., 212, 213, 214, 215,
216, 217, 218, 191, 220, ..., 253, 254, 255]

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

u = S[t]
= S[154]
= 154 Biner → 10011010

C = U ⊕ P[idx]
= U ⊕ P[3]
= U ⊕ "3" => Biner "3" = 110011

10011010
00110011 ⊕
10101001

C = "©" = 169

iterasi kedua 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, 28, 219, 18, 134, 21, 77, 8, ..., 16, 17, 55, 19, 20, 6,
72, 23, 24, 25, 26, 27, 71, 29, 30, ..., 53, 54, 4, 56, 57, 69, 8
2, 73, 74, 75, 76, 7, 78, 79, ..., 113, 114, 0, 116, 117, ...,
172, 173, 5, 175, 176, ..., 185, 190, 3, 192, 193, ...,
212, 213, 214, 215, 216, 217, 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 => Biner 73 = 1001001

C = U ⊕ P[idx]
= U ⊕ P[3]
= U ⊕ "5" Biner "5" = 110101

~~Ciphertext~~ 01001001
~~text~~ 00110101 ⊕
01111100

C = 124 = |