No.

Date :

Nama : Esy Anugerah Rahayu Kasim

Nim : E1E120007

* Algoritma : Key- Scheduling Algoritma (KSA)

Kunci : " Saputra1" , len (K) = 8

Array S : [0.1.2.3.4, 5, 6. 7, 8. ...., 100, 101, 102. 103, ..., 253, 254, 255]

* Iterasi pertama → i : 0

J : 0

⇒ J : (J + S [i] + K [i mod len (K)]) mod 256

= (0 + 0 + K [0 % 8]) % 256

= (K [0]) % 256

: ("S") % 256 ⇒ nilai desimal dari "S" = 115

: 115 % 256

J = 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, ...

199, 200, 201, 202, 203, 204, 205, ..., 250, 251, 252, 253, 254, 255]

* Iterasi Kedua → i : 1

J : 115

⇒ J : (J + S [i] + K [i % len (K)]) % 256

: (115 + S [i] + K [i % 8]) % 256

: (115 + 1 + K [1]) % 256

: (116 + "a") % 256 ⇒ desimal dari "a" = 97

: (116 + 97) % 256

J : 213

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

Swap (S [i], 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]

* Iterasi ketiga → i : 2

j : 213

→ j : (j + s [i] + k [i % len (k)]) % 256

: (213 + s [2] + k [2 % 8] % 256

: (213 + 2 + k [2]) % 256

: (215 + "p") % 256 ⇒ desimal dari "p" : 112

: (215 + 112) % 256

: 327 % 256

j : 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, 119, 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 % len (k)] % 256

: (71 + s [3] + k [3 % 8]) % 256

: (71 + 3 + k [3]) % 256

: (74 + "u" % 256 ⇒ desimal dari "u" = 117

: (74 + 117) % 256

: 191 % 256

j : 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, 219, ... 250, 251, 252, 253, 254, 255]

No.

Date :

* Iterasi Kelima → i = 4

J = 191

⇒ J = (J + S(i) + K[i % len (K)]) % 256

= (191 + S [4] + K [4 % 8]) % 256

= (191 + 4 + K [4]) % 256

= (195 + 116) % 256

= 311 % 256

J = 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]

* Iterasi Keenam → i = 5

J = 55

⇒ J : (J + S (i) + K [i % len (K)]) % 256

= (55 + S [5] + K [5 % 8]) % 256

= (55 + 5 + K [5]) % 256

= (60 + "r") % 256 ⇒ desimal "r" = 119

= (60 + 119) % 256

= 174 % 256

= 179

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

Swap (S [5]), S [179])

Array S = [115, 213, 71, 191, 55, 179, 6. 7, 8. . . . , 53, 54, 4, 56, 57, . . .
69, 70, 2, 72, 73, ... , 113, 114, 0, 116, 117, ..., 172, 173, 5, 175,
250, 251, 252, 253, 254, 255]

PAPERLINE

No.

Date :

* Iterasi ketujuh → i = 6

J : 174

→ J = (J + S [i] + K [i % len (K)]) % 256

: (174 + S [6] + K [6 % 8]) % 256

: (174 + 6 + K [6]) % 256

: (180 + "a") % 256 ⇒ desimal "a" = 97

: (180 + 97) % 256

= 277 % 256

= 21

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

Swap (6, 21)

Array S : [115, 213, 71, 191, 55, 174, 21, 7, 8, ..., 19, 20, 6, 22, 23, 116, 117, ...,
53, 54, 9, 56, 57, ..., 69, 70, 2, 72, 73, ..., 113, 114, 0, 211, 212
1, 214, 215, ..., 250, 251, 252, 253, 254, 255].

* Iterasi kedelapan → i = 7.

J = 21

⇒ J = (J + S [i] + K [i % len (K)] % 256

: (21 + S [7] + K [7 % 8]) % 256

: (21 + 7 + K [7]) % 256

: (28 + 49) % 256

: 77 % 256

J = 77

Swap (S(i)), S (J))

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

Array S = (115, 213, 71, 191, 55, 174, 21, 77, 8, ..., 19, 20, 6, 22, 23, ... 53, 54, 9, ...
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).

PAPERLINE

No.

Date :

* Algoritma : 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 = "2007"

* 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, 117, ..., 172, 173, 5, 175, 176, ..., 189, 190, 3, 192, 193, ..., 212, 213, 214, ..., 250, 251, 252, 253, ..., 255]

⇒ t = (S[i] + S[j]) % 256

= (S[i] + S[213]) % 256

= (1 + 213) % 256

= 214

⇒ U = S(t)

= S[214] = 214 ⇒ biner 214 = 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
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, 179, 21, 77, 8. ...., 19. 20, 6, 22, 23, ..., 26, 27, 71, 29, 30, ...,
53, 59, 9, 56, 57, ..., 69, 70, 2, 73, 79, 75, 76, 7. 78, ..., 113, 119, 0, 116, 117, ...,
172, 173, 5, 250, 251, 252, 253, ..., 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" → binernya = 110000
= 1100011
110000 ⊕
1010011
c = "S", desimalnya = 83 //

* Iterasi ketiga → idx = 2

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

j = (j + s[i]) % 256
= (28 + s[3]) % 256
= (28 + 191) % 256
= 219 //

swap (s[i], s[j])
swap (s[3], s[219])
Array s. ⇒ [115, 1, 28, 219, 55, 179, 21, 77, 8, ..., 19, 20, 6, 22, 23, ..., 26, 27, 71,
29, 30 ..., 53, 59, 9, 56, 57, ..., 69, 70, 2, 73, 79, 75, 76, 77, 78, 79, ...,
113, 119, 0, 116, 117, ..., 212, 213, 219, 215, 216, 217, ..., 255]

→ t : (s[i] + (s[j]) % 256
= s[3] + s[219] % 256
= (219 + 191) % 256
= 910 % 256
= 159

→ U = s[t]
= s[159]
= 159 ⇒ biner 159 = 10011010

→ C = U $\oplus$ P [idx]
= U $\oplus$ P [2]
= U $\oplus$ "0" ⇒ biner "0" = 110000

= 10011010
00110000 $\oplus$
10101010

C = "ª" desimalnya : 170
//

* Iterasi ke empat ⇒ idx = 3

i = 3, j = 219

⇒ i = (i + 1) % 256
= (3+1) % 256
= 4 //

→ j = (j + s [i] % 256
= (219 + s[4] % 256
= (219 + 55) % 256
= 274 % 256
= 18 //

swap (s[i] . s[j])
swap (s[4], s[18])
Array s : [115, 1, 28, 219, 18, 179, 21, 77, 8, ..., 16, 17, 55, 19, 20, 6, 22, ... 27, 71, 29, 30, ...
53, 54, 4, 56, 57, 69, 70, 2, ... 79, ... 113, 114, 0, 116, 117, ... , 172, 173, 5,
175, 176, ... 189, 190, 3, 192, 193, ..., 212, 213, ... 220, ..., 253, 254,
255]

⇒ t : (s[i] + s [j] % 256
= (s[4] + s [18] % 256
= (18 + 55) % 256
= 73 //

⇒ U : s[t]
= s [73]
= 73 ⇒ biner 73
= 1001001

→ C : U $\oplus$ P[idx]
= U $\oplus$ P[3]
= U $\oplus$ "7" → biner "7" = 110111
= 1001001
0110111 $\oplus$
1111110

→ C = "~" = 126
//