Nama : Farid rahman laode

NIM : E1E120028

* Algoritma Key - Scheduling algorithm (KSA)

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

Array S = [0, 1, 2, 3, ..., 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]

No.

Date

* Iterasi kedua → i = 1

j = 115

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

= (115 + S[1] + K[1 % 8]) % 256

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

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

= (116 + 97) % 256 = 213 % 256

j = 213

swap (S[i], 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]

* Iterasi ke tiga → 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 → swap(S[i], S[j])

j = 71 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 ke empat → 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

= 191

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

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

Array = [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

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 + "t") % 256 ⇒ desimal "t" = 116

= (195 + 116) % 256

= 311 % 256

j = 55

Swap = (S[i], S[j]) ⇒ (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,
..., 189, 190, 3, 192, ..., 211, 212, 1, 214,
256, 251, 252, 253, 254, 255].

* Iterasi kepenam → 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" = 114

= (60 + 114) % 256

= 174 % 256

= 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, ..., 189, 190, 3, 192, ..., 211, 212, 1, 214, 256, 251, 252, 253, 254, 255]~~

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

No.

Date

* Iterasi ketujuh → i = 6

i = 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 (S[6], S[21])

array S = [115, 213, 71, 191, 55, 179, 21, 7, 8, ...
19, 20, 6, 22, 23, ..., 53, 54, 4, 5, 57, ...
69, 70, 2, 72, 73, ..., 113, 114, 0, 116, 117, ...
172, 173, 189, 5, 175, 176, ..., 189, 190, 3, 192
193, ..., 211, 212, 1, 214, 215, ...
250, 251, 252, 253, 254, 255

Iterasi ketujuh → 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 + "1") % 256 ⇒ desimal "1" = 49

= (28 + 49) % 256

= 77 % 256

j = 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]

* 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, ... , 212, 213,
214, 215, ... , 250, 251, 252, 253, 254, 255]

plaintext = "2028"

* 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]) ⇒ [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]

No.

Date

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

⇒ u = S[t]
= S[214] = 214 ⇒ 214 = 11010110

⇒ C = u ⊕ P[idx]
= u ⊕ P[0]
= u ⊕ "ï" ⇒ biner "ï" = 11010
= 11010110
00110010 ⊕
11100100

C = "ä" diterjemahkan menjadi 228.

* Iterasi kedua → idx = 1
i = 1
j = 213
⇒ i = (i + 1) % 256
= (1 + 1) % 256
= 2
⇒ j = (j + S[1]) % 256
= (213 + S[2]) % 256
= (213 + 71) % 256
= 284 % 256
= 28
swap = (S[i], S[j]), ⇒ (S[2], S[28])

No.

Date

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]) % 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" ⇒ biner "0" = 110000
= 1100011
0110000 ⊕
1010011

c = "S" desimal = 83

* Iterasi ketiga ⟶ idx = 2
i = 2
j = 28

No.

Date

⇒ 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, 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, 28, 79, ..., 113, 114, 0, 116, 117,
..., 172, 173, 5, 175, 176, ..., 189, 190, 3, 192, 193,
..., 212, 213, 214, 215, 216, 217, 218, 191, 220, ...
254, 255]

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

⇒ u = S[t]
= S[154]
= 154 ⇒ biner 154 = 10011010

⇒ C = u ⊕ p(idx)
= u ⊕ p[2]
= u ⊕ "2" biner = 110010

10011010
00110010 ⊕
10101000

C = "¨" desimal = 168

* 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]) ⇒ (S[4], S[18])

array S = [115, 1, 28, 219, 18, 124, 2, 22, 8, ..., 16, 17, 55
, 19, 20, 6, 21, ..., 26, 27, 71, 29, 30, ..., 53, 54,
4, 56, 57, 69, 70, 273, 74, 75, 76, 77, 78, 79, ...
113, 114, 0, 116, 117, ..., 172, 173, 5, 175, 176,
..., 189, 190, 3, 192, 193, ..., 212, 213, 214, 215
, 216, 217, 218, 191, 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 = 1001001

⇒ C = u ⊕ P[idx]
= u ⊕ P[3]
= u ⊕ "8" biner = 111000
= 01001001
00111000 ⊕
01110001
C = "q" desimal 113