Date

Nama : Abdull Amnur
NIM : E1E120055

1. Kerja KSA dan PRGA dengan plaintext nim dan kunci (Saputra1)

* Algorithma : Key Scheduling Algorithma (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
= 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, 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 + [1] + K[1 % 8]) % 256
= (115 + 1 + K[1]) % 256
= (116 + "a") % 256 => desimal dari "a" = 97
= (116 + 97) % 256
= 213 % 256
= 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]

KEY

Date

* 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

= 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,
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 + "4") % 256 ⇒ desimal dari "4" = 117

= 191 % 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]

KIKY

Date

* Iterasi keempat → 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
  = 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 Kelenam → i = 5
  j = 55
  => j = (j + s[i] + k[i % len(k)]) % 256
  = (55 + s[5] + k[5 % 8]) % 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, 117, ..., 172,
  173, 5, 175, 176, ..., 189, 190, 3, 192, 193, ..., 211, 212,
  1, 214, 215, ..., 250, 251, 252, 253, 254, 255]

* Iterasi Ketujuh → i = 6
  j = 174
  j = (j + s(i) + k[i % len(k)]) % 256
  = (174 + s(6) + k[6 % 8]) % 256
  = (180 + "a") % 256 => desimal "a" = 97
  = (180 + 97) % 256
  = 277 % 256
  j = 21

Date

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, ..., 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 % len 8]) % 256
= (21 + 7 + k[7]) % 256
= (28 + "1") % 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]

KRY

No.

Date :

Pseudo-random Generator Automaton (PRGA)

1.) iterasi Pertama → idx = 0

i = 0

j = 0

i = (i + 1) mod 256

= (0 + 1) mod 256

= 1 mod 256

= 1

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

= (0 + S[1]) mod 256

= 213 mod 256

= 213

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

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

Array S = [115, 128, 191, 55, 174, 21, 77, 8, ..., 206, 22, ...
27, 71, 28, 59, 4, 86, ..., 70, 2, 72, 73, 74, 76,
7, 70, ..., 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]) % 256

= (S[1] + S[213]) % 256

= (1 + 213) % 256

= 214

⇒ U = S[t]

= S[214] = 214 ⇒ biner 214 = 1101 0110

⇒ C = U ⊕ P[idx]

= U ⊕ P[0]

= U ⊕ "2" ⇒ Biner "2" = 1100 10

= 110 10 110

00110010 ⊕

11100100

C = "ä", didesimalkan menjadi 228

PAPERLINE

* 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, 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 => 6 mer 99 = 110011

=> C = U ⊕ P[idx]
= U ⊕ P[1]
= U ⊕ "0"
= 110000

110011
110000

100011
C = "S", desimal = 83

No.

Date :

* 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, 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, ..., 189, 190, 3, 192
193, ..., 212, 213, 214, 215, 216, 217, 218, 191, 220,
..., 253, 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 = 10011010

=> C = U ⊕ P[idx]
= U ⊕ P[2]
= U ⊕ "5" = 110101

= 10011010
00110101 ⊕
10101111

C = "_", decimal = 175

PAPER

No.

Date :

* Ubah: kompak → idx = 3

r = 3

0 = 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, 174, 21, 77, 8, ..., 16, 17, 55, 19
20, 6, 72, 23, 24, 25, 26, 27, 71, 29, 30, ..., 53,
54, 4, 56, 57, 69, 70, 2, 73, 74, 75, 76, 7, 78,
79, ..., 113, 104, 0, 116, 117, ..., 172, 173, 5, 95,
170, ..., 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 73 = 100 1001

⇒ C = U ⊕ P[idx]
= U ⊕ [3]
= U ⊕ "54" = 110101

1001001
0110101 ⊕
1111100

→ C = "|", desimal = 124

PAPERLINE