Tugas 2

No.

Date :

KRIPTOGRAFI

Nama : Athenisya Dhea Rimeanta Putri Kelas : Ganjil

Nim : E1E1 20 063 Jurusan : Teknik Informatika

• Algoritma : Key - Scheduling Algorithm (KSA)

Kunci : "Saputra!"

Array S : [0, 1, 2, 3, 4, 5, 6, 7, 8, 9, ..., 99, 100, 101, 102, ..., 250, 251, 252, 253, 254, 255]

* j = 0 , i = 0 /iterasi 1

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

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

= (K[0]) mod 256

= (S) mod 256 ↔ desimal S = 115

= 115 mod 256

j = 115

swap (S[i], S[j]) ⇒ swap (S[0], S[115])

∴ Array S : [115, 1, 2, 3, 4, 5, 6, ..., 111, 112, 113, 114, 0, 116, ..., 250, 251, 252, 253, 254, 255]

* j = 115, i = 1 /iterasi 2

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

= (115 + S[i] + K[i mod 8]) mod 256

= (115 + 1 + K[i]) mod 256

= (116 + a) mod 256 ↔ desimal a = 97

= (116 + 97) mod 256

= 213 mod 256

j = 213

swap (S[i], S[j]) ⇒ swap (S[1], S[213])

∴ Array S = [115, 213, 2, 3, 4, 5, ..., 112, 113, 114, 0, 116, ..., 211, 212, 1, 214, ..., 254, 255]

* j = 213 , i = 2 /iterasi 3

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

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

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

= (215 + p) mod 256 ↔ desimal p = 112

= (215 + 112) mod 256

= 327 mod 256

j = 71

swap (S[i], S[j]) ⇒ swap (S[2], S[71])

∴ Array S : [115, 213, 71, 3, 4, ..., 69, 70, 2, 72, ..., 113, 114, 0, 116, ... 212, 1, 214, ..., 255]

No.

Date :

* j = 71, i = 3 / Iterasi 4

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

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

= (74 + 4) mod 256 ⇔ nilai desimal 4 = 117

= (74 + 117) mod 256

= 191 mod 256

j = 191

swap (S[i], S[j]) ⇒ swap (S[3], S[191])

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

* j = 191, i = 4 / Iterasi 5

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

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

= (195 + t) mod 256

= (195 + 116) mod 256 ⇒ desimal t = 116

= 311 mod 256

j = 55

swap (S[i], S[j]) ⇒ swap (S[4], S[55])

∴ Array S = [115, 213, 71, 191, 55, 5, 6, ..., 53, 54, 4, 56, 57, ..., 69, 70, 2, 72, 73, ..., 114, 0, 116, 117,
..., 189, 190, 3, 192, 193, ..., 211, 212, 1, 214, ... 253, 254, 255]

* j = 55, i = 5 / Iterasi 6

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

= (60 + 114 + k[5]) mod 256

= (60 + r) mod 256 ⇔ desimal r = 114

= (60 + 114) mod 256

= 174 mod 256

j = 174

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

* j = 174, i = 6 / Iterasi 7

j = (174 + S[6] + k[6 mod 8]) mod 256

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

= (180 + a) mod 256

= (180 + 97) mod 256 ⇒ desimal a = 97

= 277 mod 256

j = 21

swap (s[i], s[j]) ⇒ swap (S[6], S[21])

∴ Array S = [115, 213, 71, 191, 55, 174, 21, 7, 8, ..., 18, 19, 20, 6, 22, 23, ..., 53, 54, 4, 56, 57, ...,
69, 70, 2, 72, ..., 113, 114, 0, 116, 117, ..., 172, 173, 5, 175, 176, ..., 190, 3, 192, ...,
211, 212, 1, 214, ..., 251, 252, 253, 254, 255]

* j = 21, i = 7 / iterasi 8

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

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

= (28 + 1) mod 256

= (28 + 49) mod 256 ⇒ desimal 1 = 49

= 77 mod 256

j = 77

swap (S[i], s[j]) ⇒ swap (s[7], S[77])

∴ Array S = [115, 213, 71, 191, 55, 174, 21, 77, 8, 7, 10, ..., 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 ...,
189, 190, 3, 192, 193, ..., 211, 212, 1, 214, 215, ..., 251, 252, 253, 254, 255].

" ~ "

• Algoritma : Pseudo-random Generation Algorithm (PRGA

Array S : [115, 213, 71, 191, 55, 174, 21, 77, 8, 9, 10, ..., 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, ...,
189, 190, 3, 192, 193, ..., 211, 212, 1, 214, 215, ..., 251, 252, 253, 254, 255]

Plainteks : "2063"

* i = 0 / iterasi pertama

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

swap (S[i], S[j]) ⇒ swap (S[1], S[213])

Array S = [115, 1, 71, 191, 55, 174, 21, 77, 8, 9, 10, ..., 19, 20, 6, 22, ..., 53, 54, 4, 56, 57, ...,
69, 70, 2, 72, 73, 74, 75, 76, 7, 78, ..., 113, 114, 0, 116, ..., 172, 173, 5, 175, ..., 189, 190, 3,
192, 193, ..., 212, 213, 214, ..., 253, 254, 255]

No.

Date :

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

⇒ u = S[t]
= S[214] = '214' = 11010110

⇒ c = u ⊕ p[idx]
= u ⊕ p[0]
= u ⊕ "2" ⇒ '2' = 110010
= 11010110
00110010 ⊕
11100100

c = "ä", didesimalkan menjadi 228

* idx = 1 / iterasi ke 2
i = 1
j = 213
⇒ i = (i + 1) mod 256
= (1 + 1) mod 256
= 2 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, ..., 26, 27, 71, 29, ..., 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, ..., 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 ⊕ → "S" desimal = 83
1010011

* idx = 2 / iterasi ke 3

i = 2

j = 28

⇒ i = (i + 1) mod 256 ⇒ j = (j + s[i]) mod 256

= (2 + 1) mod 256 = (28 + s[3]) mod 256

= 3 mod 256 = (28 + 191) mod 256

= 3 = 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, ... ; 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]) mod 256

= (s[3] + s[219]) mod 256

= (219 + 191) mod 256

= 154

⇒ u = s[t]

= s[154]

= 154 ⇒ biner 154 = 10011010

⇒ c = u ⊕ p[idx]

= u ⊕ p[2]

= u ⊕ 6 ⇒ biner 6 = 0110110

= 10011010

00110110 ⊕ ⇒ c = 7, 7 desimal = 172

10101100

* idx = 3 / iterasi ke 4

i = 3

j = 28

⇒ i = (i + 1) mod 256 j = (j + s[i]) mod 256

= (3 + 1) mod 256 = (219 + s[4]) mod 256

= 4 = (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, 174, 21, 77, 8, ..., 16, 19, 55, 69, 20, 6, 22, 23, 24, 25, 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]

KIKY

$\Rightarrow t = (S[i] + S[j]) \bmod 256$

$= (S[4] + S[18]) \bmod 256$

$= (18 + 55) \bmod 256$

$= 73 \bmod 256 = 73$

$u = S[t]$

$= S[73]$

$= 73 \Rightarrow$ biner $73 = 1001001$

$c = u \oplus p[idx]$

$= u \oplus p[3]$

$= u \oplus 3 \Rightarrow$ biner $3 = 110011$

$= 1001001$

$0110011 \oplus \quad \Leftrightarrow z$, desimal $z = 122$

1111010