Nama : Muh Fikri Haikal B.
NIM : E1E120040

No.: Date:

* Key - Scheduling Algorithm

Kunci : "saputra1" . len(k) = 8
Array s : [0, 1, 2, 3, 4, ..., 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
= 115 % 256 → nilai desimal dari "s" = 115
j = 115
swap (s[i], s[j])
swap (s[0], s[115])
Array s : [115, 1, 2, 3, ..., 113, 114, 0, 116, 117, ..., 253, 254, 255]

* Iterasi kedua → i = 1

j = 115
⇒ j = (j + s[i] + k[i mod len(k)]) mod 256
= (115 + s[1] + k[1 % 8]) % 256
= (115 + 1 + k[1]) % 256
= (116 + "a") % 256
= (116 + 97) % 256 → nilai desimal dari "a" = 97
= 213 % 256
j = 213
swap (s[i], s[j])
swap (s[1], s[213])
Array s : [115, 213, 2, 3, 4, ..., 112, 113, 114, 0, 116, ..., 210, 211, 212, 1, 214,
...., 253, 254, 255]

KIKY You were born to shine

No.: Date:

* Iterasi kebiga → i = 2

j = 213

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

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

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

= (215 + "p") % 256

= (215 + 112) % 256 → nilai desimal dari "p" = 112

= 327 % 256

j = 71

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

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

Array S : [115, 213, 71, 3, 4, ..., 70, 2, 72, ..., 114, 0, 116, ..., 212, 1, 214, ..., 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 % 8]) % 256

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

= (74 + "u") % 256

= (74 + 117) % 256 → nilai desimal dari "u" = 117

= 191 % 256

j = 191

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

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

Array S : [115, 253, 71, 191, 4, ..., 70, 2, 72, ..., 114, 0, 116, ..., 190, 3, 192, ..., 212, 1, 214, ..., 253, 254, 255]

No.: Date:

* Iterasi kelima → i = 4

j = 191

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

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

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

= (195 + "t") % 256

= (195 + 116) % 256 → nilai desimal dari "t" = 116

= 311 % 256

j = 55

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

swap (S[4], S[55])

Array S : [115, 213, 71, 191, 55, 5, 6, ..., 54, 4, 56, ..., 70, 2, 72, ...,
114, 0, 116, ..., 190, 3, 192, ..., 212, 1, 214, ..., 254, 255]

* Iterasi keenam → i = 5

j = 55

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

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

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

= (60 + "r") % 256

= (60 + 114) % 256 → nilai desimal dari "r" = 114

= 174 % 256

j = 174

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

swap (S[5], S[174])

Array S : [115, 213, 71, 191, 55, 174, 6, ..., 54, 4, 56, ..., 70, 2, 72,
...., 114, 0, 116, ..., 173, 5, 175, ..., 190, 3, 192, ..., 212,
1, 214, ... 253, 254, 255]

No.: Date:

* Iterasi kebujuh → i = 6

j = 174

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

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

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

= (180 + "a") % 256

= (180 + 97) % 256 → nilai desimal dari "a" = 97

= 277 % 256

j = 21

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

swap (S[6], S[21])

Array S: [115, 243, 71, 191, 55, 174, 21, 7, 8, ..., 20, 6, 22, ..., 54, 4, 56, ..., 70, 2, 72, ..., 114, 0, 116, ..., 173, 5, 175, ..., 190, 3, 192, ... 212, 1, 214, ..., 253, 254, 255]

* Iterasi kedelapan → i = 7

j = 21

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

j = (j + S[7] + k[7 % 8]) % 256

= (21 + 7 + k[7]) % 256

= (28 + "1") % 256

= (28 + 49) % 256 → nilai desimal dari "1" = 49

= 77 % 256

j = 77

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

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

Array S: [115, 243, 71, 191, 55, 174, 21, 77, 8, ..., 20, 6, 22, ..., 54, 4, 56, ..., 70, 2, 72, 73, 74, 75, 76, 7, 78, ..., 114, 0, 116, ..., 173, 5, 175, ..., 190, 3, 192, ... 212, 1, 214, ..., 253, 254, 255]

KIKY Follow your own path

No.: Date:

* Algoritma : Pseudo-Random Generation Algorithm

Array s : [115, 213, 71, 191, 55, 174, 21, 77, 8, ..., 20, 6, 22, ..., 54, 4, 56, ..., 70, 2, 72, 73, 74, 75, 76, 7, 78, ..., 114, 0, 116, ..., 173, 5, 175, ..., 190, 3, 192, ..., 212, 1, 214, ..., 253, 254, 255]

Plainteks : "2040"

* 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, ..., 20, 6, 22, ..., 54, 4, 56, ..., 70, 2, 72, 73, 74, 75, 76, 7, 78, ..., 114, 0, 116, ..., 173, 5, 175, ..., 190, 3, 192, ..., 212, 213, 214, ..., 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 = 11010110

KIKY You were born to shine

No.: Date:

⇒ c = u ⊕ P[idx]
= u ⊕ P[0]
= u ⊕ "2" → biner "2" = 110010
= 1101011 0

01100010 ⊕
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, 174, 21, 77, 0, ..., 20, 6, 22, ..., 27, 71, 29, ..., 54, 4, 56, ..., 70, 2, 72, 73, 74, 75, 76, 7, 78, ..., 114, 0, 116, ..., 173, 5, 175, ..., 190, 3, 192, ..., 213, 214, 215, ..., 254, 255]
⇒ k = (s[i] + s[j]) % 256
= (s[2] + s[28]) % 256
= (28 + 71) % 256
= 99 % 256
= 99

No.: Date:

⇒ u = S[t]
= S[99]
= 99 → biner 99 = 1000011
⇒ C = u ⊕ P[idx]
= u ⊕ P[1]
= u ⊕ "0" → biner "0" = 110000
= 1100011
110000 ⊕
1010011
C = "S", desimal = 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, 174, 21, 77, 8, ..., 20, 6, 22, ..., 27, 71, 29, ..., 54, 4, 56, ..., 70, 2, 72, 73, 74, 75, 76, 7, 78, ..., 114, 0, 116, ..., 173, 5, 171, ..., 190, 3, 192, ..., 243, 244, 245, 246, 247, 248, 191, 220, ..., 253, 254, 255]
⇒ t = (S[i] + S[j]) % 256
= (S[3] + S[219] % 256
= (219 + 191) % 256

KIKY Follow your own path

No.: Date:

= 410 % 256

= 146

⇒ U = S[t]

= S[146]

= 146 → biner 146 = 10010010

⇒ C = U ⊕ P[idx]

= U ⊕ P[2]

= U ⊕ "4" → biner "4" = 110100

= 10010010

110100 ⊕

10100110

C = "¡", desimal = 166

* Iterasi keempat → 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, 174, 21, 77, 8, ..., 17, 55, 19, 20, 6, 22, ..., 27, 71, 29, ..., 54, 4, 56, ..., 70, 2, 72, 73, 74, 75, 76, 7, 78, ..., 114, 0, 116, ..., 173, 5, 175, ..., 190, 3, 192, ..., 212, 213, 214, 215, 216, 217, 218, 191, 220, ..., 253, 254, 255]

KIKY Follow your own path

No.: Date:

⇒ t = (S[i] + S[0]) % 256
= (S[4] + S[18]) % 256
= (10 + 55) % 256
= 73

⇒ u = S[t]
= S[73]
= 73 → biner 73 = 1001001

⇒ c = u ⊕ P[idx]
= u ⊕ P[3]
= u ⊕ "0" → biner "0" = 110000
= 1001001
110000 ⊕
1111001

c = "y", desimal = 121