NAMA : FADILA HAIRUL NISA
NIM : E1E1 20 066
TUGAS 2

* Algoritma RC4
  1. KSA (Key Scheduling Algorithm)
  2. PRGA (Pseudo Random Generation Algorithm)

1. KSA
   K = Saputra1
   ⇒ K_0 = S, K_1 = a, K_2 = P, K_3 = u
   K_4 = t, K_5 = r, K_6 = a, K_7 = 1 ⇒ Lenght (K) = 8
   Array S = [0, 1, 2, 3, ..., 10, 11, 12, 13, ..., 100, 101, 102, ..., 200, 201, 202, ..., 255]

* Iterasi Pertama
  i = 0
  j = 0
  ⇒ j = (j + S[i] + K[i mod len(K)]) mod 256
  = (0 + S[0] + K[0 mod 8]) mod 256
  = (0 + 0 + K[0]) mod 256
  = (0 + 0 + "S") mod 256 ⇒ ascii S = 115 (desimal)
  = (0 + 115) mod 256
  = 115 mod 256
  j = 115
  swap (S[i], S[j])
  swap (S[0], S[115])
  Array S = [115, 1, 2, 3, ..., 110, 111, 112, 113, 114, 0, ..., 250, 251, 252, 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 mod 8]) mod 256
  = (115 + 1 + K[1]) mod 256
  = (116 + "a") mod 256 ⇒ ascii a = 97 (desimal)
  = (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, ..., 114, 0, 116, ..., 210, 211, 212, 1, 214, ..., 255]

* Iterasi ketiga

i = 2

j = 213

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

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

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

= (215 + "p") mod 256 ⇒ ascii p = 112 (desimal)

= (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, ..., 70, 2, 73, 74, ..., 114, 0, 116, ..., 210, 1, 214, ..., 255]

* Iterasi keempat

i = 3

j = 71

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

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

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

= (74 + "u") mod 256 ⇒ ascii u = 117 (desimal)

= (74 + 117) mod 256

= 191 mod 256

j = 191

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

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

Array S = [115, 215, 71, 191, 4, ..., 70, 2, 73, ..., 114, 0, 116, ..., 190, 3, 192, ..., 255]

* Iterasi kelima

i = 4

j = 71

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

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

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

= (195 + "t") mod 256

= (195 + 116) mod 256

= 311 mod 256

j = 55

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

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

Array S = [115, 213, 71, 191, 55, 5, ..., 54, 4, 56, ..., 70, 2, 72, ..., 114, 0, 116, ..., 255]

* Iterasi kelima

i = 5

j = 55

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

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

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

= (60 + "r") mod 256 → ascii r = 114 (desimal)

= (60 + 114) mod 256

= 174 mod 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, ...
170, 171, 172, 173, 5, 175, ..., 255]

* Iterasi ketujuh

i = 6

j = 174

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

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

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

= (180 + "a") mod 256 → ascii a = 97 (desimal)

= (180 + 97) mod 256

= 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, ..., 20, 6, 22, ..., 54, 4, 56, ..., 70, 2, 72, ...
114, 0, 116, ..., 172, 173, 5, 175, ..., 255]

* Iterasi kedelapan

i = 7

j = 21

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

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

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

= (28 + "1") mod 256 ⇒ ascii 1 = 49 (desimal)

= (28 + 49) mod 256

= 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, 0, ..., 20, 6, 22, ..., 54, 4, 56, ..., 61, 62...
70, 2, 72, 73, 74, 75, 76, 7, 78, ..., 114, 0, 116, ..., 173, 5, 175, ..., 255]

2. PROSES

Plainteks : 2066

Array S = [115, 213, 71, 191, 55, 174, 21, 77, 0, 20, 6, 22, ..., 54, 4, 56, ..., 61, 62, 63, ...
70, 2, 72, 73, 74, 75, 76, 7, 78, ..., 114, 0, 116, ..., 173, 5, 175, ..., 255]

* Iterasi Pertama

i = 0

j = 0

for index = 0 to len(P) - 1

= 0 to (4) - 1 = 0 to (3)

i = (i + 1) mod 256

= (0 + 1) mod 256

i = 1

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

= (1 + 213) mod 256

t = 214

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

= (0 + S[1]) mod 256

= (0 + 213) mod 256

j = 213

u = S[t]

= 214

swap (S[i], S[j]) mod 256

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

C = u ⊕ P[0]

= u ⊕ 2

= 214 ⊕ 2

11010110
00110010 ⊕
11100100 → 228 = ä

* Iterasi kedua

i = 1

j = 213

i = (i + 1) mod 256
= (1 + 1) mod 256
= 2 mod 256
i = 2

t = (z[i] + s[j]) mod 256
= (s[2] + s[213]) mod 256
= (28 + 71) mod 256
= 99 mod 256
t = 99

j = (j + s[i]) mod 256
= (213 + s[2]) mod 256
= (213 + 71) mod 256
= 284 mod 256
j = 28

u = s[t]
= 99

c = u ⊕ P[1]
= 99 ⊕ P[0]
= 99 ⊕ 0
= 01100011
00110000 ⊕
01010011 → 83 = S

swap (s[i] . s[j])
swap (s[2] . s[28])

* Iterasi ketiga

i = 2

j = 28

i = (i + 1) mod 256
= (2 + 1) mod 256
= 3 mod 256
i = 3

t = (z[i] + s[j]) mod 256
= (s[3] + s[219]) mod 256
= (219 + 191) mod 256
= 410 mod 256
t = 154

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

u = s[t]
= 154

c = u ⊕ P[2]
= 154 ⊕ P[6]
= 154 ⊕ 006
= 10011010
00110110 ⊕
10101100 → 172 = ¬

swap (s[i] . s[j])
swap (s[3] . s[219])

* Iterasi keempat

i = 3

j = 219

i = (i + 1) mod 256
= (3 + 1) mod 256
= 4 mod 256

i = 4

j = (j + S[i]) mod 256
= (219 + S[4]) mod 256
= (219 + 55) mod 256
= 274 mod 256

j = 10

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

swap (S[4], S[10])

t = (S[i] + S[j]) mod 256
= (S[4] + S[274]) mod 256
= (10 + 55) mod 256
= 73 mod 256

t = 73

u = S[t]
= 73

C = u ⊕ P[3]
= 73 ⊕ 6
= 01001001
  00110110 ⊕
  01111111 → 127 = DEL (Delete)

Hasil = äS7