Nama : Muh. Mujib Nur Sunandar
NIM : E1E120079

S = [0, 1, 2, 3, 4, 5 ..., 251, 252, 253, 254, 255]

KSA

Iterasi 1

i = 0
j = 0
j = (j + S[i] + K[i mod length(K)]) mod 256
  = (0 + 0 + K[0 mod 8]) mod 256
  = (0 + K[0]) mod 256
  = 0 + 115 mod 256
j = 115
swap S[i], S[j] = S[0], S[115]
S = [115, 2, 3, 4, 5, ..., 112, 113, 114, 0, 116, ..., 253, 254, 255]

Iterasi 2

i = 1
j = 115
j = (j + S[i] + K[i mod length K]) mod 256
  = (115 + 1 + K[1 mod 8]) mod 256
  = (116 + K[1]) mod 256
  = 116 + 97 mod 256
j = 213
swap S[i], S[j] = S[1], S[213]

Iterasi 3

i = 2
j = 213
j = (j + S[i] + K[i mod length K]) mod 256
  = (213 + 2 + K[2 mod 8]) mod 256
  = (215 + K[2]) mod 256
  = 327 mod 256
j = 71
swap S[i], S[j] = S[2], S[71]
S = [115, 213, 71, 3, ... 70, 2, 72, ... 212, 1, 214 ..., 253, 254, 255]

Iterasi 4

i = 3

j = 71

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

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

= (74 + K[3] mod 256

= 191 mod 256

j = 191

swap S[i], S[j] = S[3], S[191]

S = [115, 213, 191, 4, ..., 70, 2, 72, ..., 114, 0, 116, ..., 190, 3, 192, ..., 212, 1, 214, ..., 253, 254, 255]

## PRGA

Array S = [115, 213, 71, 191, 55, 174, 21, 77, 8, 9, 10, ..., 20, 6, 22, ..., 54, 4, 56, ...,
70, 2, 72, ..., 76, 7, 78, ..., 114, 0, 116, ..., 173, 5, 175, ..., 190, 3, 192,
..., 212, 1, 214, ..., 254, 255]

Plainteks / P = @ 2095

Iterasi 1

i = 0, j = 0

For index = 0 to length (P) - 1

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

i = (i + 1) mod 256

i = (0 + 1) mod 256

i = 1

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

j = (0 + S[i]) mod 256

j = (0 + 213) mod 256 = 213 mod 256

j = 213

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

t = (S[i] + S[213]) mod 256

t = 1 + 213 mod 256 = 214 mod 256

t = 214

u = S[214]

C = u ⊕ P[0]

= 214 ⊕ 2

= 11010110

00110010 ⊕

11100100 = 228 = ä

Iterasi 2

i = 1 , j = 213

For index = 0 to (3)

i = (i+1) mod 256

i = (1+1) mod 256

i = 2

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

j = (213 + S[2]) mod 256

j = (213 + 71) mod 256 = 284 mod 256

j = 28

Iterasi 3

i = 2

j = 28

For index = 0 to 3

i = (i+1) mod 256

i = (2+1) mod 256

i = 3 mod 256

i = 3

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

j = (28 + S[3]) mod 256

j = (28 + 191) mod 256

j = 219

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

(S[3], S[219])

t = (S[i] + S[219]) mod 256

t = (219 + 191) mod 256 = 410 mod 256

t = 154

u = S[154]

C = u ⊕ P[2]

= 154 ⊕ 6

= 10011010

00110110 ⊕

10101100

= 172

Iterasi 4

i = 3  j = 219

For index = 0 to (3)

i = (i+1) mod 256

i = (3+1) mod 256

i = 4

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

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

j = (219 + 55) mod 256 = 274 mod 256

j = 18

swap (S[i], S[j]) = S[4], S[18]

t = (S[4] + S[18]) mod 256

t = (18 + 55) mod 256 73 mod 256

t = 73

u = S[73]

C = 48 ⊕ P[3]

= 73 ⊕ 7

= 01001001

01000111

01111110

= 96