Nama : Ageng Arya khrysna DwiPangga

NIM : E1E120056

kelas : Genap

kriPtografi

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

key: SaPutra1

KSA

Iterasi 1

1=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

1 = 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]

S = [115 , 213, 2, 3, 4, ..., 113 ,114, 0, 116, ..., 211, 212, 1, 214, ..., 253, 254, 255]

Iterasi 3

1 = 2

J= 213

J= (J + S[i] +k [i mod length (k)]) mod 256

=(~~115~~213 + 1 +k [2 mod 8]) mod 256

=(116 + k [12]) mod 256

=327 mod 256

J= 71

→ S= [115,213,71, 3, ..., 70, 2, 73, 74, ..., 211, 212
1, 214, ..., 253, 254, 255]

Iterasi 4

i = 3 (u)

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

= 74 + 117 mod 256

= 191 mod 256

j = 191

Swap : S[i], S[j] = S[3], S [191]

S = [115, 213, 71, 191, 4, . . . , 70, 2, 72, 73, . . . , 114, 0, 116, 117, . . . , 190, 3, 192, 193, . . . , 212, 1, 214,
215, . . . , 253, 254, 255]

Iterasi 5

i = 4 (t)

j = 191

j = (j + S [i] + ~~e~~ k [i mod length (k)]) mod 256

= (191 + ~~3~~4 + k [~~3~~4 mod 8]) mod 256

= (195 + k [4]) mod 256

= 195 + 116 mod 256

= ~~311~~ 311 mod 256

= 55

Swap S[i], S[j] = S[4, S [55]

S = [115, 213, 71, 191, 55, ~~8~~5, 6, 7, . . . , 54, 4, ~~55~~, 56, 57, . . , 70, 2, 72, 73, . . . , 114, 0, 116, 117, . . .
190, 3, 192, 193, . . . , 212, 1, 214, 215, . . . , 253, 254, 255]

Iterasi 6

i = 5 (r)

j = 55

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

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

= (60 + k [5]) mod 256

= 60 + 114 mod 256

= 174 mod 256

= 174

Swap : S [i], S[j] = S [5], S [174]

S = [115, 213, 71, 191, 55, 174, 6, 7, . . . , 54, 4, ~~55~~, 56, 57, . . . , 70, 2, 72, 73, . . . , 114, 0, 116, 117, . . . ,
173, 5, 175, 176, . . . , 190, 3, 192, 193, . . . , 212, 1, 214, 215, . . . , 253, 254, 255]

Iteras: 7

i = 6 (a)

j = 174

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

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

= (180 + k[6]) mod 256

= 180 + 97 mod 256

= 277 mod 256

j = 21

Swap S[i]. S[j] . S[6], S[21]

S = [115, 213, 71, 191, 55, 174, 21, 7, 8, ..., 20, 6, 22, 23, ..., 54, 4, 56, 57, ..., 70, 2, 72, 73, ..., 114, 0, 116,
117, ..., 173, 5, 175, 176, ..., 190, 3, 192, 193, ..., 212, 1, 214, 215, ..., 253, 254, 255]

iterasi 8

i = 7 (1)

j = 21

j = (j + s[i] + k[i mod lengt (k)] mod 256

= (21 + 7 + k[7 mod 8]) mod 256

= (28 + k[7]) mod 256

= 28 + 49 mod 256

j = 77 mod 256

~~Swap~~ = 77

swap S[i] . S[j] = S[7], S[77]

S = [115, 213, 71, 191, 55, 174, 21, 77, 8, ..., 20, 6, 22, 23, ..., 54, 4, 56, 57, ..., 70, 2, 72, 73, ..., 76, 7,
78, 79, ..., 114, 0, 116, 117, ..., 173, 5, 175, 176, ..., 190, 3, 192, 193, ..., 212, 1, 214, 215, ..., 253, 254,
255]