Nama : Muhammad Agus Saputra
NIM : 6161 20 039
Kriptografi

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

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

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

= 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, ..., 114, 0, 116, ..., 190, 3, 192, ..., 212, 1, 4, ..., 253, 254, 255]

Iterasi 5

i = 4

j = 191

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

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

= (195 + k[4]) mod 256

= (195 + 116) mod 256

j = 55

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

Iterasi 6

i = 5

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 + 119) mod 256

j = 179

swap S[i], S[j] = S[5], S[179]

Iterasi 7

i = 6

j = 179

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

= (179 + 6 + k[6 mod 8]) mod 256

= (186 + k[6]) mod 256

j = (186 + 97) mod 256

j = 21

swap S[i], S[j] = S[6], S[21]

Iterasi ke 8

i = 7

j = 21

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

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

= (28 + k[7]) mod 256

= (28 + 49) mod 256

j = 77

swap s[i], s[j] = s[7], s[77]

S = [115, 213, 71, 191, 55, 174, 21, 77, 8, 9, ..., 19, 20, C, 22, ..., 52, 53, 54, A, [illegible]
..., 75, 76, 7, 78, ..., 113, 114, 0, 116, ..., 172, 173, 5, 175, ..., 190, 3, 192, 211, 212, 1,
214, ..., 253, 254, 255, [illegible]]

PRGA

p = 2039

Iterasi 1

i = 0

j = 0

i = (0 + 1) mod 256

i = 1

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

= (0 + s[1]) mod 256

= 0 + 213 mod 256

j = 213

swap s[1], s[j] = s[213], s[[illegible]]

t = s[1] + s[j]

t = 1 + 213 = 214

u = s[214]

= 214 ⊕ p[0]

= 214 ⊕ 2

= 11010110

00110010 ⊕

11100100 = 228 = ä

Iterasi 2

i = 1

j = 213

i = (1 + 1) mod 256

i = 2

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

= (213 + s[2]) mod 256

= (213 + 71) mod 256

= 284 mod 256

j = 28

swap s[1], s[j] = s[2], [28]

t = s[1], s[j]

= 71 + 28

= 99

u = s[99]

= 99 ⊕ p[1]

= 99 ⊕ 0

= 01100011

00110000 ⊕

01010011 = 83 = S

Iterasi 3

i = 2

j = 28

i = (2 + 1) mod 256

i = 3

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

= (28 + s[3]) mod 256

= (28 + 191) mod 256

= 219

swap s[i], s[j] = s[3], s[219]

t = s[i] + s[j]

= 219 + 191 = 410 mod 256 = 154

u = s[154]

= 154 ⊕ p[2]

= 154 ⊕ 3

= 10011010

00110011

10101001 = 169 = ©

Iterasi 4.

i = 3

j = 219

i = (3+1) mod 256

= 4

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

= (28 + s[4]) mod 256

= (28 + 55) mod 256

= 83 mod 256

= 83

swap s[i], s[j] = s[4], s[83]

t = s[i] + s[j]

= 83 + 55

= 138

u = s[138]

= 138 ⊕ p[3]

= 138 ⊕ 9

= 10001010

00011001 ⊕

10110011 = 179 = ³