TUGAS 2 KRIPTOGRAFI

MUH NUR IHSAN EIE120036

Key scheduling Algorithm

S = [0, 1, 2, 3, ..., 255]

k = "saputra1"

Iteras 1

i = 0

j = 0

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

= (0 + S[0] + k[0 mod 8]) mod 256

= 0 + 0 + k[0] mod 256

= 115 mod 256

= 115

swap S[i], S[j] : swap S[0], S[115]

=> [115, 1, 2, 3, 4, ..., 114, 0, 116, ..., 255]

Iteras 2

i = 1

j = 115

=> j = (115 + 1 + k[1 mod 8]) mod 256

= (115 + 1 + k[1]) mod 256

= 116 + 97 mod 256

= 213

swap S[1], S[213]

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

Iteras 3

i = 2

j = 213

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

= 213 + 122 mod 256

= 71 -> swap S[2], S[71]

Iteras 4

i = 3

j = 71

j = (71 + 3 + k[3 mod 8]) mod 256

= (71 + 117) mod 256

= 191

=> swap S[3], S[191]

Iterasi 5

i = 4

j = 191

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

= (191 + 116) mod 256

= 55 -> swap s[4], s[55]

Iterasi 6

i = 5

j = 55

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

= (55 + 114) mod 256

= 179

=> swap s[5], s[21]

Iterasi 7

i = 6

j = 179

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

j = (179 + 97) mod 256

= 21 => swap s[6], s[21]

Iterasi 8

i = 7

j = 21

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

= (21 + 99) mod 256

= 77 => swap s[7], s[77]

Iterasi dilanjutkan iterasi hingga i = 255

Pseudo-Random Generation Algorithm

Arrays = [118, 213, 71, 49, 174, ... 200, 25]

Hasil dari 256 iterasi KSA

P = "2036"

Iterasi 1

i = 0

j = 0

i = (0+1) mod 256

= 1 mod 256

= 1

j = (0 + S[1]) mod 256

= 213

swap -> S[1], S[213]

t = (S[1] + S[213]) mod 256

t = (201 + 213) mod 256

t = 158

u = S[158]

C = 148 ⊕ P[0]

= 50 -> Char: '2'

Iterasi 2

i = 1

j = 213

i = (1+1) mod 256 = 2

j = (213 + S[2]) mod 256 = 28

swap S[2], S[28]

t = (S[2] + S[28]) mod 256

= (106 + 171) mod 256

u = S[227]

= 241

C = 241 ⊕ P[1]

= 98 -> Char: 'á'

Iterasi 3

i = 2

j = 28

i = (2+1) mod 256 = 3

j = (28 + S[3]) Mod 256 = 77

swap S[3], S[77]

t = (S[3] + S(77)) mod 256

= (196 + 49) Mod 256

u = S[195]

c = 145 ⊕ P[2]

= 51 → char: 3

Iterasi 4

i = 3

j = 77

i = (3 + 1) mod 256

= 4

j = (77 + S[4]) mod 256

= 108

Swap ⇒ S[4], S[108]

t = (S[4] + S[108]) mod 256

= 149 + 31 mod 256

u = S[180]

= 70

c = 70 ⊕ P[3]

= 54 → Char: '6'