Nama : Muhammad Ilham Prayogi
Nim : 616120083

* Algoritma : Key - Scheduling Algorithm (KSA)

Kunci : "Saputral" . len (k) = 8
Array S : [0,1,2,3,4,5,6,7,8 .. 100, 101, 102, 103, . . . , 253, 254, 255]

* Iterasi I → i = 0
j = 0
⇒ j = (j + S [i] + k [i mod len (k)]) mod 256
= (0 + 0 + k [0 % 8]) % 256
= (k [0]) % 256
= ("S") % 256 ⇒ nilai desimal dari "S" = 115
= 115 % 256
= 115
j = 115
Swap (S [i] , S [j])
Swap (S [0] , S [115])
Array S : [115, 1, 2, 3, 4, 5, 6, 7, ... 110, 111, 112, 113, 114, 0, 116, 117, ...
199, 200, 201, 202, 203, 204, 205, . . . , 250, 251, 252, 253, 254,
255]

* Iterasi II → i = 1
j = 115
→ j = (j + S [i] + k [i % len (k)]) % 256
= (115 + S [1] + k [1 % 8]) % 256
= (115 + 1 + k [1]) % 256
= (116 + "a") % 256 ⇒ desimal dari "a" = 97
= (116 + 97) % 256
= 213 % 256
= 213
Swap = (S [i]) , S [j])
Swap (S [1] , S [213]
Array S : [115, 213, 2, 3, 4, 5, 6, 7, ... , 112, 113, 114, 0, 116, . . . , 210, 211,
212, 1, 214, . . . , 250, 251, 252, 253, 254, 255]

Iterasi III → i = 2

j = 213

⇒ j = (j + s[i] + k[i % len(k)]) % 256

= (213 + s[2] + k[2 % 8] % 256

= (213 + 2 + k[2]) % 256

= (215 + "p") % 256 ⇒ desimel dari "p" = 112

= (215 + 112) % 256

= 327 % 256

j = 71

Swap (s[i], s[j])

Swap (s[2], s[71])

Array S = [115, 213, 71, 3, 4, 5, 6, 7, ..., 69, 70, 2, 72, ..., 112,
113, 114, 0, 116, ..., 210, 211, 212, 1, 214, ...,
250, 251, 252, 253, 254, 255]

Iterasi IV → i = 3

j = 71

⇒ j = (j + s[i] + k[i % len(k)]) % 256

= (71 + s[3] + k[3 % 8]) % 256

= (71 + 3 + k[3]) % 256

= (74 + "U") % 256

= 191 % 256

j = 191

Swap (s[i], s[j])

Swap (s[3], s[191])

Array S = [115, 213, 71, 191, 4, 5, 6, 7, ..., 69, 70, 2, 72, ...,
112, 113, 114, 0, 116, ..., 189, 190, 3, 192, ..., 210, 211,
212, 1, 214, ..., 250, 251, 252, 253, 254, 255]