Nama : Syadad Rifo'ah Syaifullah
NIM : E1E120093
Kelas : Ganjil

* Algoritma KSA

kunci : Saputra1 , len(k) = 8
Array S = [0, 1, 2, 3, 4, 5, 6, 7, 8, ..., 100, 101, 102, 103, ..., 253, 254, 255]

* Iterasi 1 = i = 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
j = 115
Swap (S[i], S[j])
Swap (S[0], S[115])

Array S = [115, 1, 2, 3, 4, 5, 6, 7, ..., 100, 101, 112, 113, 114, 0, 116, 117, ...,
199, 200, 201, 202, 203, 204, 205, ..., 250, 251, 252, 253, 254, 255]

* Iterasi 2 = 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
j = 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 3 = i = 2

j = 213

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

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

= (217 + 2 + k [2]) % 256

= (215 + "p" ) % 256 => desimal 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, 71, 72, ..., 112, 113, 114, 0, 116, ..., 210, 211, 212, 1, 214, ..., 250, 251, 252, 253, 254, 255]

* Iterasi i = 3

j = 71

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

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

= (74 + "u" ) % 256 => desimal dari "u" = 117

= (74 + 117) % 256

= 191 % 256

j = 191

Swap = (s [3], s [j])

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

Array s = [115, 213, 7, 191, 4, 5, 6, 7, ..., 69, 70, 71, 72, 73, ..., 112, 113, 114, 0, 116, ..., 189, 190, 3, 192, ..., 210, 211, 212, 1, 214, ..., 250, 251, 252, 253, 254, 55]

* Iterasi s i = 4

j = 191

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

= (191 + s [4] + k [4 % 8 ]) % 256

= (191 + 4 + k [4]) % 256

= (195 + "t" ) % 256 => desimal "t" = 116

= (195 + 116 ) % 256

= 311 % 256

j = 55

Swap (s[i], s[j])
Swap (s[4], s[55])
Array S = [115, 213, 71, 191, 55, 5, 6, 7, 8, ..., 53, 54, 4, 56, 57, ...
69, 70, 2, 72, 73, ..., 113, 114, 0, 116, 117, ..., 189, 190,
3, 192, ..., 211, 212, 1, 214, ..., 250, 251, 252, 253, 254, 25

* Iterasi 6 = i = 5
j = 55
j = (j + s[i] + k[i % len(k)]) % 256
= (55 + s[5] + k[5 % 8]) % 256
= (55 + 5 + k[5]) % 256
= (60 + "r") % 256 => desimal "r" = 114
= (60 + 114) % 256
= 174 % 256
= 174
Array S = [115, 213, 71, 191, 55, 174, 6, 7, 8, ..., 53, 54, 4, 56, 57, ...
69, 70, 2, 72, 73, ..., 113, 114, 0, 116, 117, ..., 172, 173,
5, 175, 176, ..., 189, 190, 3, 192, 193, ..., 211, 212,
1, 214, 215, ..., 250, 251, 252, 253, 254, 255.]

* Iterasi 7 = i = 6
j = 174
j = (j + S[i] + k[i % len(k)]) % 256
= (174 + S[6] + k[6 % 8]) % 256
= (174 + 6 + k[6]) % 256
= (180 + "a") % 256 => desimal "a" = 97
= (180 + 97) % 256
= 277 % 256
j = 21
Swap (S[i], S[j])
Swap (S[6], S[174])
Array S = [115, 213, 71, 191, 55, 174, 21, 7, 8 ..., 19, 20,
6, 22, 23, ..., 53, 54, 4, 56, 57, ..., 69, 70,
2, 72, 73, ..., 113, 114, 0, 116, 117, 172, 173, 5,
175, 176, ..., 189, 190, 3, 192, 193, ..., 211, 212,
214, 215, 250, 251, 252, 253, 254, 255.]

* Iterasi 8 - 1 - 7

J = 4

J = (J + S[i] + K[i % len(K)]) % 256

= (21 + S[7] + K[7 % 8]) % 256

= (21 + 7 + K[7]) % 256

= (28 + "1") % 256 → decimal "1" = 49

= (28 + 49) % 256

= 77 % 256

J = 77

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

Swap (S[7], S[77])

Array S = [115, 213, 71, 191, 55, 221, 77, 8, ..., 19, 20, 6, 22, 23, ...
53, 54, 4, 56, 57, ..., 69, 170, 2, 72, 73, 74, 75, 76,
7, 78, ..., 113, 114, 0, 116, 117, ..., 172, 173, 8, 175,
176, ..., 189, 190, 3, 192, 193, ..., 211, 212, 1, 214, 215
..., 248, 249, 250, 251, 252, 253, 254, 255]