Nama : Dhea Angellena Engel
Nim : E1E120005
Kelas : Ganjil

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

* Iterasi pertama → 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
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, 0, 116, 117, ..., 199, 200, 201, 202, 203, 204, 205, ...
250, 251, 252, 253, 254, 255]

* Iterasi kedua i = 1
j = 115
⇒ j = (j + S[1] + 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[1], 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 ketiga → 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 + 112) % 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, 2, 72, ... 112, 113, 114, 0, 116, ..., 210, 211, 212, 1, 214, ... 250, 251, 252, 253, 254, 255]

* Iterasi keempat 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 ⇒ desimal dari "u" = 117

= (74 + 117) % 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]

* Iterasi kelima → 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, 255]

※ Iterasi keenam → 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
j = 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, 254, 255]

※ Iterasi kedupuh → 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, 1, 214, 215, ..., 250, 251, 252,
... 253, 254, 255]

* Iterasi kedelapan → i=7

j = 21

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

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

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

= (28 + "1") % 256 → desimal "1" - 49

= (28 + 49) % 256

= 77 % 256

= 77

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

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

Array S [115, 213, 71, 191, 55, 21, 77, 8, ..., 19, 20, 6, 22, 23, ... 53, 54, 4, 56, 57 ...,
69, 70, 2, 72, 73, 74, 75, 76, 7, 78, ..., 113, 114, 0, 116, 117, ... 172, 5, 175,
176, ... 189, 190, 3, 192, 193, ... 211, 212, 1, 214, 215, ..., 250, 251, 252,
253, 254, 255]

P = 2005

Array S = [115, 213, 71, 191, 55, 174, 21, 77, 8, 9, 10, ..., 20, 6, 22, ..., 54, 4, 56, 70, 2, 72, ...
76, 7, 78, ..., 114, 0, 116, ..., 173, 5, 175, ..., 190, 5, 192, ... 212, 1, 214, ... 254, 255]

Plaintext / P = 2005

✱ Iterasi Pertama → i = 0 j = 0

for index = 0 to lenght (P) - 1
= 0 to (-4) - 1 = 0 to (3)

i = (i+1) mod 256
i = (0 + 1) mod 256
i = 1

j = (j + S[i]) mod 256
j = (0 + S[1]) mod 256
j = (0 + 213) mod 256 = 213 mod 256
j = 213

Swap (S[i], S[j]) = (S[1], S[213])

t = (S[1] + S[213] mod 256
t = 1 + 213 mod 256 = 214 mod 256
t = 214
u = S[214]
c = u ⊕ P[0]
= 214 ⊕ 2
= 11010110
00110010 ⊕
11100100 = 220 = a

* Iteran kedua

i = 1 , j = 213

For index = 0 to (3)

i = (i + 1) mod 256

i = (1 + 1) mod 256

i = 2

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

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

j = (213 + 71) mod 256 = 284 mod 256

j = 28

Swap (S[i], S[j]) = (S[2], S[28])

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

t = (28 + 71) mod 256 = 99 mod 256

t = 99

u = S[99]

c = u ⊕ p[1]

= 99 ⊕ 0

= 0 11 000 11

00 11 0000 ⊕

01010011 = 83 = S (capital s)

* Iteran ketiga

i = 2, j = 28

for index = 0 to (3)

i = (i + 1) mod 256

i = (2 + 1) mod 256

i = 3

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

j = (28 + S[3]) mod 256

j = 219

Swap (S[i], S[j]) = (S[3], S[219])

t = (S[3] + S[219]) mod 256

t = (219 + 191) mod 256 = 410 mod 256

t = 154

u = S[154]

c = u ⊕ p[2]

= 154 ⊕ 0

10011010

60110000 ⊕

10101010 = 170

* Iterasi keempat

i = 3 j = 219

for index = 0 to (3)

i = (i+1) mod 256

i = 4

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

j = (219 + s[3]) mod 256

j = (219 + 55) mod 256 = 274 mod 256

j = 18

Swap (s[i], s[j]) = (s[4], s[18])

t = (s[4] + s[18]) mod 256

t = (18 + 55) mod 256 = 73 mod 256

t = 73

~~u = s[x]~~

~~[illegible]~~

u = s[73]

C = u ⊕ p[3]

= 73 ⊕ 5 = 01001001 ⊕ 00000101 = 01001001 ⊕ 00000101 = 01001100 = 76 L

= '

~~Hasil Array s = [115, 1, 20~~