PRGA

Array S = [115, 213, 71, 191, 55, 174, 21, 77, 8, ..., 20, 6, 22, 23, ..., 54, 4, 56, 57, ..., 70, 2, 72, 73, ...,
76, 7, 78, 79, ..., 114, 0, 116, 117, ..., 173, 5, 175, 176, ..., 190, 3, 192, 193, ..., 212, 1, 214, 215, ...
253, 254, 255]

Iteras: 1 Plaintext = 2056 , S = [115, 213, 71, 191, 55, 174, 21, 77]

i = 0

j = 0

For Index = 0 to length (P) - 1
= 0 to (4) - 1 = 0 to 3

i = (0 + 1) mod 256
= 1

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

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

S# = 214

U = S[214]

C = 214 ⊕ P[0]
= 214 ⊕ 2
= 11010110
00110010 ⊕
11100100 = 228 = ä

Iteras: 2

i = 1

j = 213

For Index = 0 to (3)

i = (i + 1) mod 256
= (1 + 1) mod 256
= 2

j = (i + S[i]) mod 256
= (213 + S[2]) mod 256
= (213 + 71) mod 256

j = 284 mod 256
= 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 = 99

U = S[99]
= U ⊕ P[1]
= 99 ⊕ 0
= 01100011
00110000 ⊕
= 01010011 = 83 = S

Iterasi 3

i = 2

j = 28

For index = 0 to (3)

i = (i + 1) mod 256

= (2 + 1) mod 256

= 3

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

= (28 + S[3]) mod 256

= (28 + 191) mod 256 = 219 mod 256

= 219

Swap S[i], S[j] : S[3], S[219]

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

= (191 + 219) mod 256

= 410 mod 256

= 154

u = S[154]

= 154 ⊕ 6

= 1 0 0 1 1 0 1 0

0 0 1 1 0 1 0 1 ⊕

1 0 1 0 1 1 1 1 = 175 = −

Iterasi 4

i = 3

j = 219

For index = 0 to (3)

i = (i + 1) mod 256

= (3 + 1) mod 256

= 4

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

= (219 + S[4]) mod 256

= (219 + 55) mod 256

= 274 mod 256

= 18

Swap S[i], S[j] : S[4], S[18]

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

= (55 + 18) mod 256

= 73 mod 256

= 73

→ u = S[73]

= 73 ⊕ 6

= 0 1 0 0 1 0 0 1

0 0 1 1 0 1 1 0 ⊕

0 1 1 1 1 1 1 1 = 127 =