Untuk syadad : NIM 2093

Metode PRGA

iterasi pertama

•> p = 2093
i = 0
j = 0

for index = 0 to length (p) - 1
for index = 0 to (4) - 1

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

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

swap S[i], S[j]
S[1], S[213]

t = S[213] + S[1] => isi index
t = 213 + 1
t = 214.

u = S[214]
C = 214 ⊕ P[idx]
= 214 ⊕ P[0]
= 214 ⊕ 2
= 11010110
00110010
⊕
11100100 => 228 = ä

iterasi kedua

$i = 1$

$j = 213$

for index = 0 to length (p) - 1

= 0 to (4) - 1

$i = (i + 1) \bmod 256$

$i = (1 + 1) \bmod 256$

$i = 2 \bmod 256$

$i = 2$

$j = (j + S[i]) \bmod 256$

$j = (213 + S[2]) \bmod 256$

$j = (213 + 71) \bmod 256$

$j = 284 \bmod 256$

$j = 28$.

swap $S[i], S[j]$

$S[2], S[28]$

$t = S[2] + S[28]) \bmod 256$

$t = (28 + 71)$

$= 99$

$u = S[99]$

$C = u \oplus P[1]$

$= 99 \oplus 0$

$= 01100011$

00110000

01010011 $\oplus$

$= 83 \Rightarrow$ S (capital s).

Iterasi ketiga

$i = 2$, $j = 28$

for index = 0 to (3)

$i = (i+1) \bmod 256$

$i = (2+1) \bmod 256$

$i = 3$

$j = (j + S[i]) \bmod 256$

$j = (28 + S[3]) \bmod 256$

$j = (28 + 191) \bmod 256$

$j = (219) \bmod 256$

swap ($S[3]$, $S[219]$)

$t = (S[3] + S[219]) \bmod 256$

$t = 219 + 191 \bmod 256$

$t = 154$

$u = S[154]$

$= u \oplus P[2]$

$= 154 \oplus 9$

$= 10011010$

00111001

$\oplus$

$10100011 \Rightarrow 163 = £$

iteran keempat

$i = 3, j = 219$

for index = 0 to (3)

$i = (i+1) \bmod 256$

$= (3+1) \bmod 256$

$i = 4$

$j = (j + S[i]) \bmod 256$

$j = (219 + S[4]) \bmod 256$

$j = (219 + 55) \bmod 256$

$j = 274 \bmod 256$

$j = 18.$

swap $(S[i], S[j])$

$(S[4], S[18])$

$t = S[4] + S[18]$

$= 98 + 55 \bmod 256$

$t = 73$

$U = S[73]$

$C = U \oplus P[3]$

$= 73 \oplus 3$

$= 01001001$

00000011

$+$ (122 ⇒ z)

$01111010 \Rightarrow z = (\text{small } z)$