Nama : Afdhalul Rahmat Septyo
Nim : E1E120029

1. KSA
   - Plainteks : 20029
   - Kunci : saputra

k_0 = s = 115		k_4 = t = 116	
k_1 = a = 97		k_5 = r = 114	
k_2 = p = 112		k_6 = a = 97	
k_3 = u = 117		k_7 = 1 = 99	

   - S = [0, 1, 2, 3, 4, 5, ..., 252, 253, 254, 255]

```
J = 0
for i = 0 to 255 do
    j = (j + S[i] + k[i % length(k)]) % 256
    swap (S[i], S[j])
end
```

* i = 0, j = 0
  j = (j + S[i] + k[i % length(k)]) % 256
  = (0 + 0 + k[0 % 8]) % 256
  = (0 + 0 + k[0]) % 256
  = (0 + 0 + 115) % 256
  = 115
  swap (S[0], S[115])
  S = [115, 1, 2, 3, 4, 5, ..., 110, 111, 112, 113, 114, 0, 116, 117, ..., 255]

* i = 1, j = 115
  j = (j + S[i] + k[i % length(k)]) % 256
  = (115 + 1 + k[1 % 8]) % 256
  = (115 + 1 + 97) % 256
  = 213 % 256
  = 213
  swap (S[1], S[213])
  S = [115, 213, 2, 3, 4, 5, ..., 210, 211, 212, 1, 214, 215, ..., 255]

* i = 2, j = 213
j = (j + S[i] + K[i % length(K)]) % 256
= (213 + S[2] + K[2 % 8]) % 256
= (213 + 2 + 112) % 256
= 327 % 256
= 71
swap(S[2], S[71])
S = [115, 213, 71, 3, 9, 5, ..., 70, 2, 72, 73, ..., 255]

* i = 3, j = 71
j = (j + S[i] + K[i % length(K)]) % 256
= (71 + S[3] + K[3 % 8]) % 256
= (71 + 3 + 117) % 256
= 191 % 256
= 191
swap(S[3], S[191])
S = [115, 213, 71, 191, 9, 5, ..., 190, 3, 192, 193, ..., 255]

* i = 9, j = 191
j = (j + S[i] + K[i % length(K)]) % 256
= (191 + S[9] + K[9 % 8]) % 256
= (191 + 9 + 116) % 256
= 311 % 256
= 55
swap(S[9], S[55])
S = [115, 213, 71, 191, 55, 5, 6, ..., 50, 51, 52, 53, 54, 9, 56, ... 255]

* i = 5, j = 55
j = (j + S[i] + K[i % length(K)]) % 256
= (55 + S[5] + K[5 % 8]) % 256
= (55 + 5 + 119) % 256
= 179 % 256
= 179
swap(S[5], S[179])
S = [115, 213, 71, 191, 55, 179, 6, 7, ..., 173, 5, 175, 176, ..., 255]

* i = 6 , j = 179

j = (j + S[i] + K[i % length(K)]) % 256

= (179 + S[6] + K[6 % 8]) % 256

= (179 + 6 + 97) % 256

= (277) % 256

= 21

swap(S[6], S[21])

S = [115, 213, 71, 191, 55, 179, 21, 7, 8, ..., 20, 6, 22, ..., 255]

* i = 7 , j = 21

j = (j + S[i] + K[i % length(K)]) % 256

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

= (21 + 7 + 99) % 256

= 77 % 256

= 77

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

S = [115, 213, 71, 191, 55, 179, 21, 77, 8, 9, ..., 2, 72, 73, 79, 75, 76, 7, 78, ..., 255]

2. PRGA

- plaintext : 2029
- kunci : saputra1
- S : [115, 213, 71, 191, 55, 179, 21, 77, 8, 9, ..., 253, 254, 255]

```
i = 0
j = 0
for idx = 0 to length(P)-1:
    i = (i+1) % 256
    j = (j + S[i]) % 256
    swap(S[i], S[j])
    t = (S[i] + S[j]) mod 256
    u = S[t]
    c = u ⊕ P[idx]
end
```

* i = 0 , j = 0

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

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

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

t = (S[i] + S[j]) % 256
= (S[213] + S[1]) % 256
= (213 + 1) % 256
= 214

u = S[t]
= S[214]

c = u ⊕ P[0] = 214 ⊕ 2

= 1 1 0 1 0 1 1 0
0 0 0 0 0 0 1 0 ⊕
1 1 0 1 0 1 0 0 → 212 → Ô (chr)

8 i = 1 , j = 213

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

j = (j + S[i]) % 256
= (213 + S[2]) % 256
= (213 + 71) % 256
= 284 % 256 = 28

swap (S[i], S[j])
swap (S[2], S[28])

t = (S[i] + S[j]) % 256
= (S[28] + S[2]) % 256
= (71 + 28) % 256
= 99 % 256
= 99

u = S[t]
= S[99]

c = u ⊕ P[1]
= 99 ⊕ P[1]
= 9 ⊕ 0
= 0 1 1 0 0 1 1
0 0 0 0 0 0 0 0 ⊕
0 1 1 0 0 1 1 → 99 = "c"

* i = 2 , j = 28

i = (i + 1) % 256
= (2 + 1) % 256
= 3

j = (j + S[i]) % 256
= (28 + S[3]) % 256
= (28 + 191) % 256
= 219

swap (S[i], S[j])
swap (S[3], S[219])

t = (S[i] + S[j]) % 256
= (S[219] + S[3]) % 256
= (219 + 191) % 256
= 410 % 256
= 154

u = S[t]
= S[154]

c = u ⊕ P[2]
= 154 ⊕ 2
= 1 0 0 1 1 0 1 0
0 0 0 0 0 0 1 0 ⊕
1 0 0 1 1 0 0 0 → 152 = "L"

* i = 3, j = 219

i = (i+1) % 256
= (3+1) % 256
= 9

j = (j + S[i]) % 256
= (219 + S[9]) % 256
= (219 + 55) % 256
= 274 % 256 = 18

swap(S[i], S[j])
swap(S[9], S[18])

t = (S[i] + S[j]) % 256
= (S[18] + S[9]) % 256
= (18 + 55) % 256
= 73

u = S[t]
= S[73]

C = u ⊕ P[3]
= 73 ⊕ 9
= 1001001
0000100 ⊕
1001101 → 77 = "M"