NAMA : SITTI NUR HALIZA

NIM : E1E120051

KELAS : GANJIL

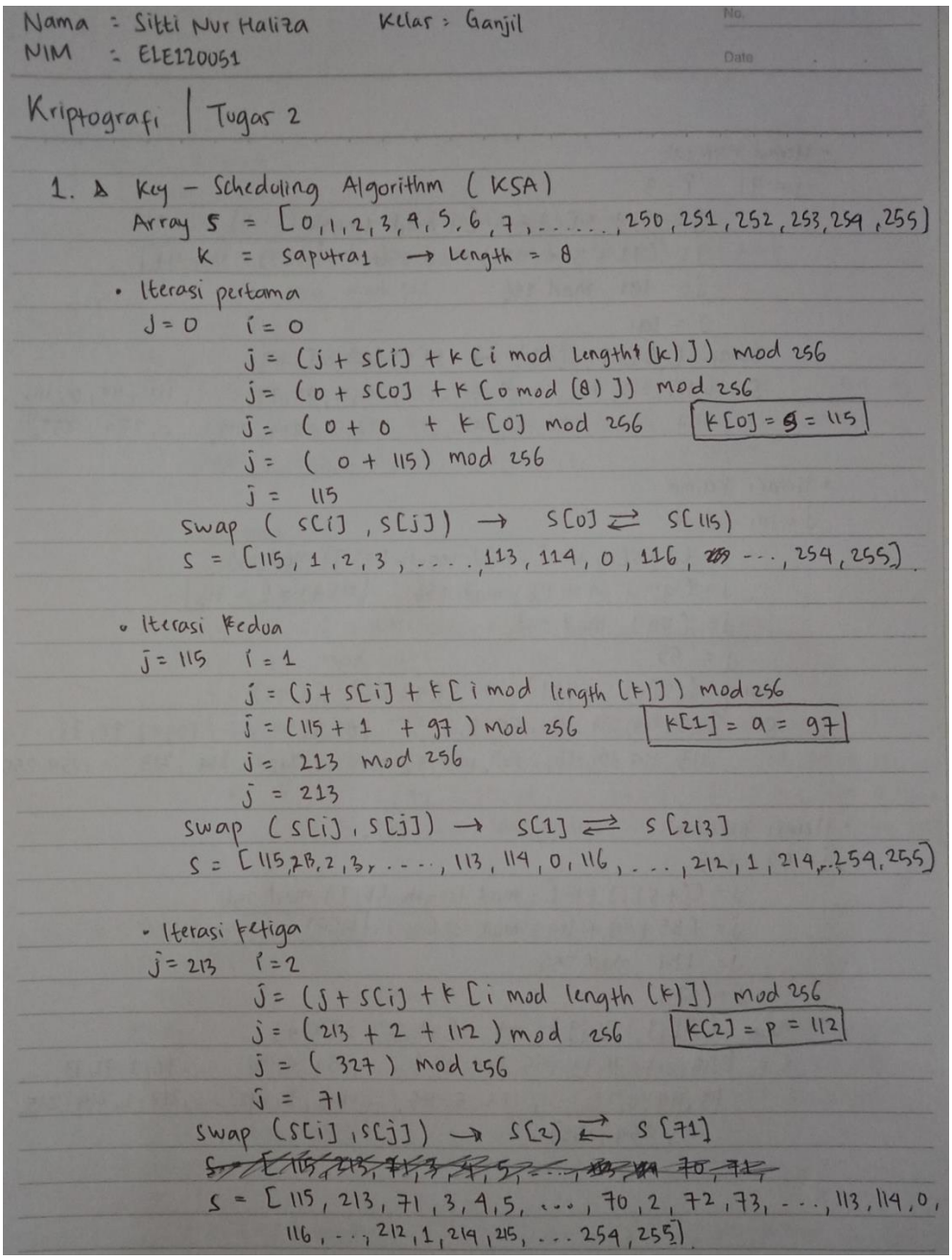
MATA KULIAH KRIPTOGRAFI

Tugas 2

1. Kerjakan KSA dan PRGA dengan kunci ‘saputra1’ dan plaintext ‘2(3 angka terakhir NIM)’. Tulis tangan!
2. Buat Program python dengan algoritma RC4 (untuk kelas ganjil) bagian sub-proses KSA!

JAWAB

1. **Sub-proses *Key-Scheduling Algorithm* (KSA)**



• Iterasi keempat

j = 71 i = 3

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

j = (71 + 3 + 117) mod 256 K[3] = U = 117

j = 191 mod 256

j = 191

Swap (S[i], S[j]) → S[3] ⇄ S[191]

S = [115, 213, 71, 191, 4, 5, ..., 70, 2, 72, 73, ..., 113, 119, 0, 116, 117, ..., 190, 3, 192, ..., 212, 1, 214, 215, ..., 254, 255]

• Iterasi kelima

j = 191 i = 4

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

j = (191 + 4 + 116) mod 256 K[4] = t = 116

j = (311) mod 256

j = 55

Swap (S[i], S[j]) → S[4] ⇄ S[55]

S = [115, 213, 71, 191, 55, 5, 6, ..., 54, 4, 56, ..., 70, 2, 72, 73, ..., 113, 119, 0, 116, ..., 190, 3, 192, ..., 212, 1, 214, 215, ..., 254, 255]

• Iterasi Kesnam

j = 55 i = 5

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

j = (55 + 5 + 119) mod 256 K[5] = r = 119

j = 179 mod 256

j = 179

Swap (S[i], S[j]) → S[5] ⇄ S[179]

S = [115, 213, 71, 191, 55, 179, 6, 7, ..., 54, 4, 56, ..., 70, 2, 72, 73, ..., 113, 119, 0, 116, ..., 173, 5, 175, ..., 190, 3, 192, ..., 212, 1, 214, 215, ..., 254, 255]

• Iterasi ketujuh

j = 179 i = 6

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

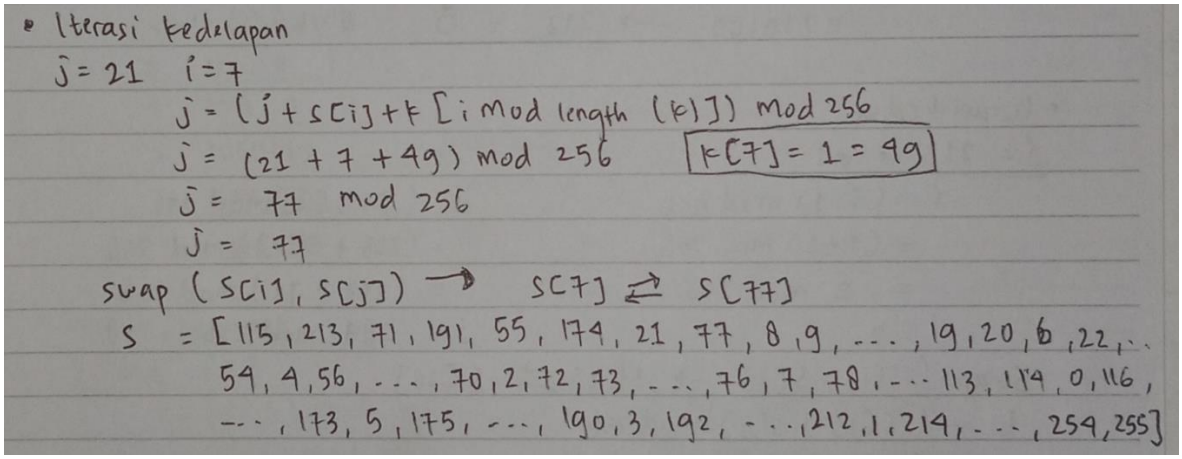
j = (179 + 6 + 97) mod 256 K[6] = a = 97

j = (277) mod 256

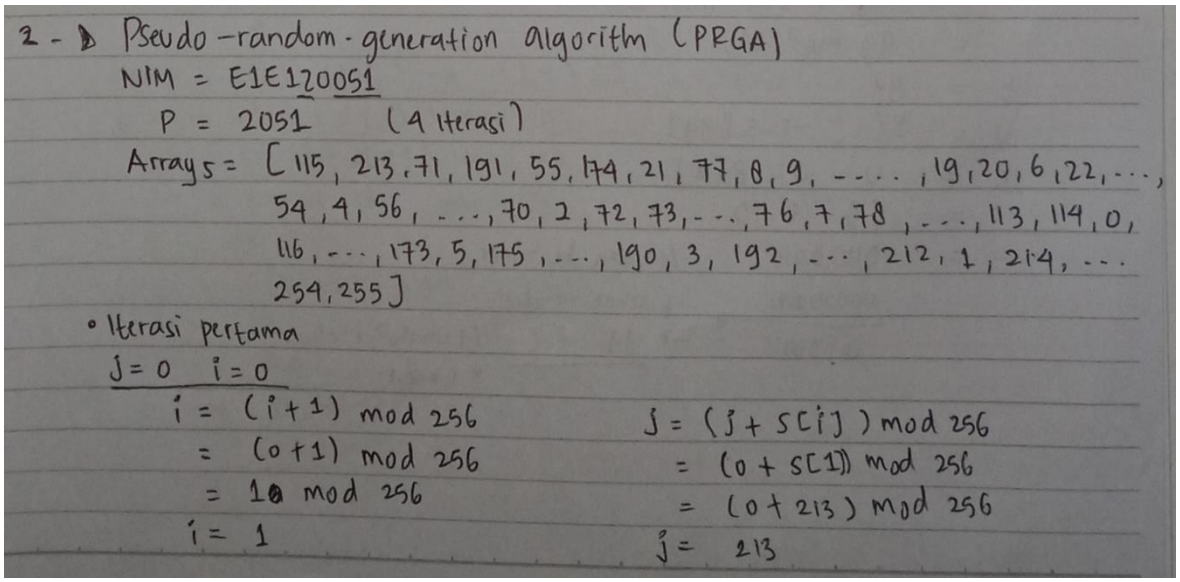
j = 21

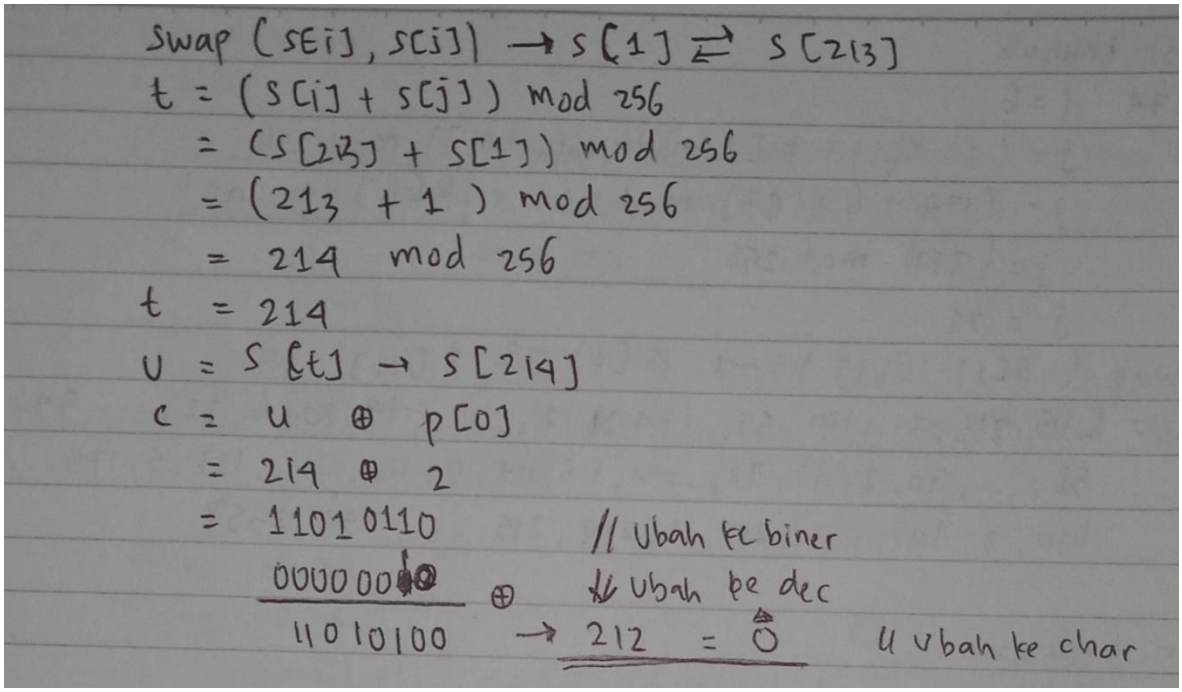
Swap (S[i], S[j]) → S[6] ⇄ S[21]

S = [115, 213, 71, 191, 55, 179, 7, ..., 19, 20, 6, 22, ... 54, 4, 56, ..., 70, 2, 72, 73, ..., 113, 119, 0, 116, ..., 173, 5, 175, ..., 190, 3, 192, ..., 212, 1, 214, 215, ..., 254, 255]



Sub-proses *Pseudo-Random Generation Algorithm* (PRGA)





- Iterasi kedua

j = 213 i = 01

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

j = (j + 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[i] + s[j]) mod 256
= (s[28] + s[2]) mod 256
= (71 + 28) mod 256
= 99 mod 256

t = 99

u = s[t] → s[99]

c = u ⊕ p[1]
= 99 ⊕ 0
= 01100011 // ubah ke biner
00000000b
01100011 → 99 = c // ubah ke char
* c kecil.

- Iterasi ~~kempat~~ tiga

j = 28 i = 2

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

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

Swap (S[i], S[j]) → S[3] ⇄ S[219]

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

U = S[t] → S[154]

C = U ⊕ P[2]
= 154 ⊕ 5
= 10011010 // ubah ke biner
00000101 ⊕
10011111 → 159 = Ÿ // ubah ke char
(ubah ke dec)

- Iterasi kecempat

J = 219 i = 3

i = (i + 1) mod 256
= (3 + 1) mod 256
= 4 mod 256
i = 4

j = (j + S[i]) mod 256
= (219 + S[4]) mod 256
= (219 + 55) mod 256
j = 274 mod 256 = 18

Swap (S[i], S[j]) → S[4] ⇄ S[18]

t = (S[i] + S[j]) mod 256
= (S[18] + S[4]) mod 256
= (55 + 18) mod 256
t = 73

U = S[t] → S[73]

C = U ⊕ P[5]
= 73 ⊕ 1
= 01001001 // ubah ke biner
00000001 ⊕
01001000 → 72 = H // ubah ke char.
(ubah ke dec)

2. **Program python KSA**

```
#E1E120051_SITTI NUR HALIZA_KSA
s = []
k = ['s','a','p','u','t','r','a','1']

panjangk = len(k)
for i in range(256):
    s.append(i)
print("s = ",s)

j = 0
for i in range(256):
    key_index = k[i % panjangk]
    j = (j + s[i] + ord(key_index)) % 256

    temp = s[i]
    s[i] = s[j]
    s[j] = temp
print()
print("s = ",s)
```

HASIL OUTPUT KEY-SCHEDULING ALGORITHM (KSA)

Larik Awal : Array S dari index 0 - 255

Key : saputra1

Hasil Permutasi : Dapat dilihat pada foto

Hasil Screenshot: