

Bab III

Algoritma

Algorithm 3 Prosedur inisialisasi *state-array*.

```
1: procedure INISIALISASI STATEARRAY
2:   Start
3:   For  $i = 0 : 255$  do                                     ▷ Pemberian nilai awal
4:      $S[i] = i$ 
5:      $K[i] = key[i \bmod key.length()]$ 
6:   EndFor
7: end procedure
```

3.0.1 Pembangkitan Kunci Enkripsi

Setelah memiliki *state-array* yang teracak, maka selanjutnya adalah melakukan PRGA untuk menghasilkan kunci enkripsi yang nantinya digunakan untuk di-XOR-kan dengan *plain*. Pertama *increment* nilai i dan dapatkan nilai j dari hasil j ditambahkan dengan array S ke- i , lalu tukar $S[i]$ dan $S[j]$. lalu simpan *byte* kunci ke dalam $B[n]$, B merupakan array *byte* kunci dan n merupakan iterasi $0 \leq n \leq 255$, hasil dari array S indeks ke $S[i] + S[j]$. Algoritmanya seperti contoh algoritma 10 dibawah ini.

Algorithm 4 Prosedur *key-scheduling*.

```
1: procedure KEYSCHEDULINGALGORITMA
2:    $j = 0$ 
3:   For  $j = 0 : 255$  do                                     ▷ Pemberian nilai awal
4:      $j = (j + S[i] + K[i]) \bmod 256$ 
5:     Swap ( $S[i], S[j]$ )
6:   EndFor
7: end procedure
```

Setelah mendapatkan *byte* kunci, nanti akan di-XOR-kan dengan *byte* pesan atau data yang akan disisipkan.