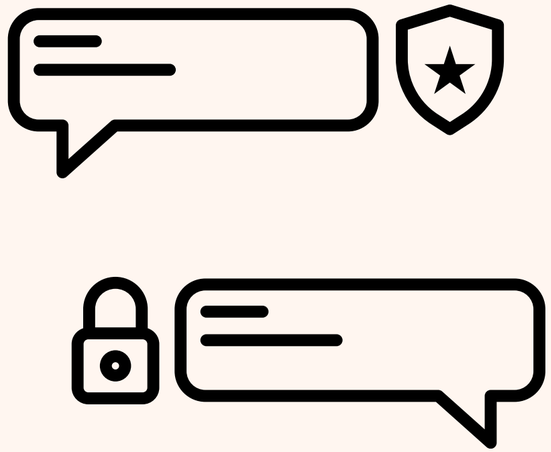
Copy.nugra21

Model enkripsi RC4

Sebuah model Encripsi lama Yang di kembangkan oleh Ron Rivest pada tahun 1987.



Copy.nugra21

Stream Cipher dan Block Cipher

Stream Cipher

metode enkripsi yang mengenkripsi data satu bit atau satu byte dalam satu waktu

Block Cipher

mengenkripsi data dalam blok-blok dengan ukuran tetap

Simmetric Cipher dan Asymmetric Cipher

Simmetric Cipher

Menggunakan satu kunci untuk proses enkripsi

Asymmetric Cipher

Menggunakan pasangan kunci (kunci publik dan kunci privat)

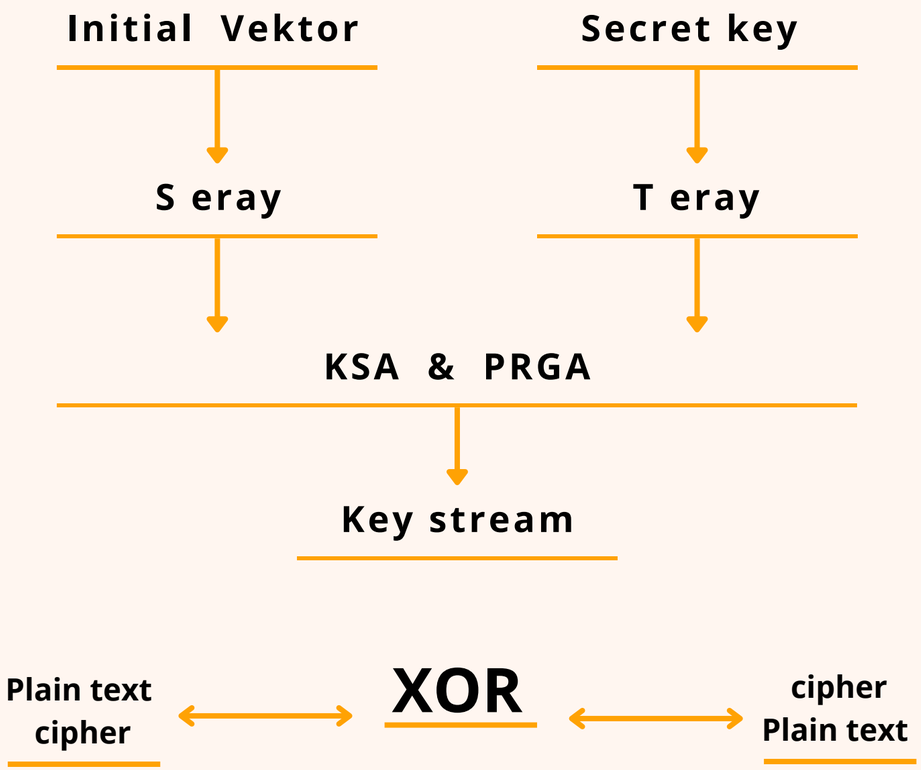
RC4 Encryption

- RC4 adalah algoritma stream cipher
- Perancang Ron Rivest pada tahun 1987. dan di publickaskasikan pada tahun 1994
- sering digunakan untuk aplikasi

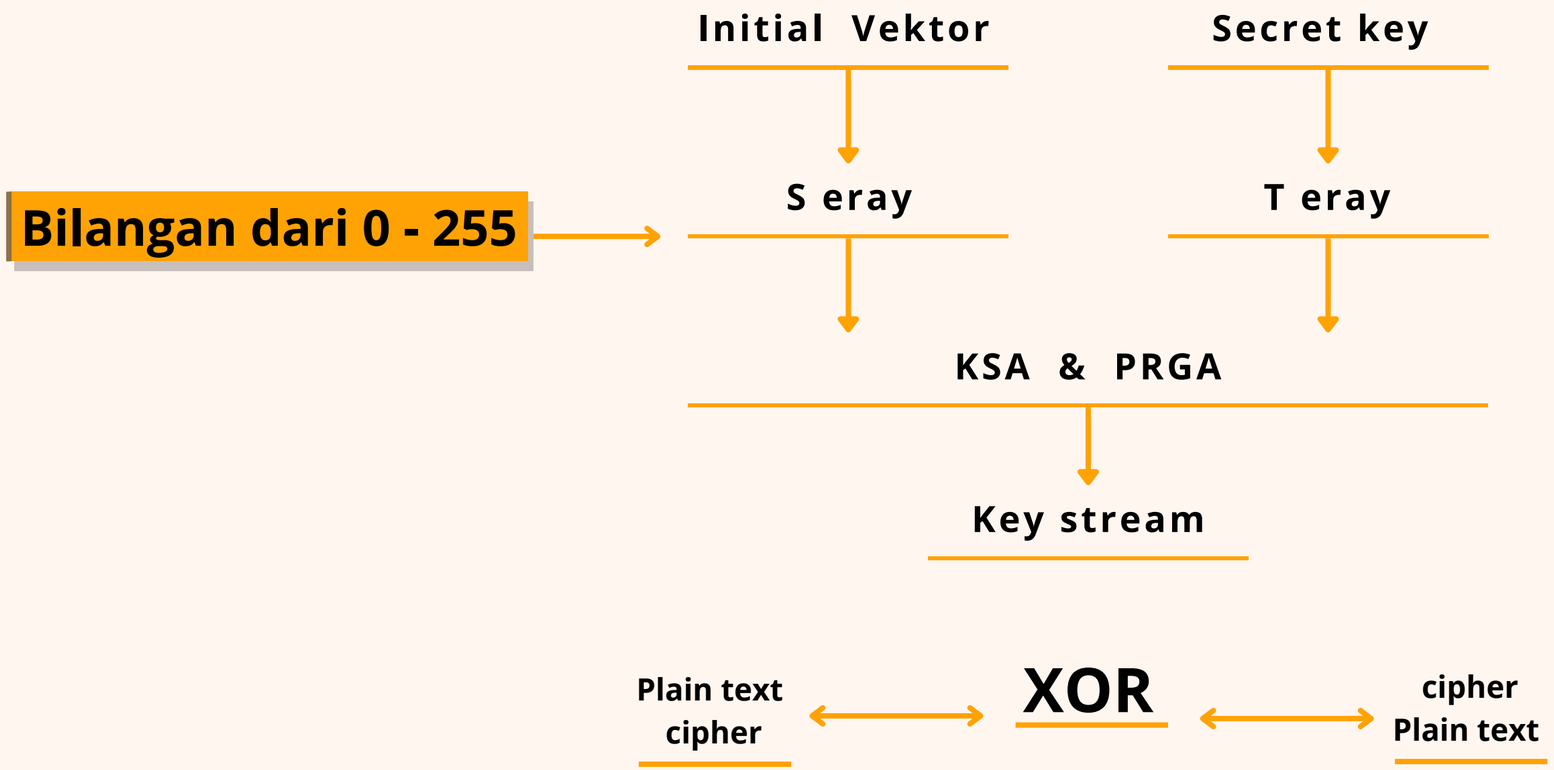
SSL / TLS (Secure socket ,transport layer)

WEP / WPA (Wired Equivalen Privacy ,Wi-Fi Protected Access)

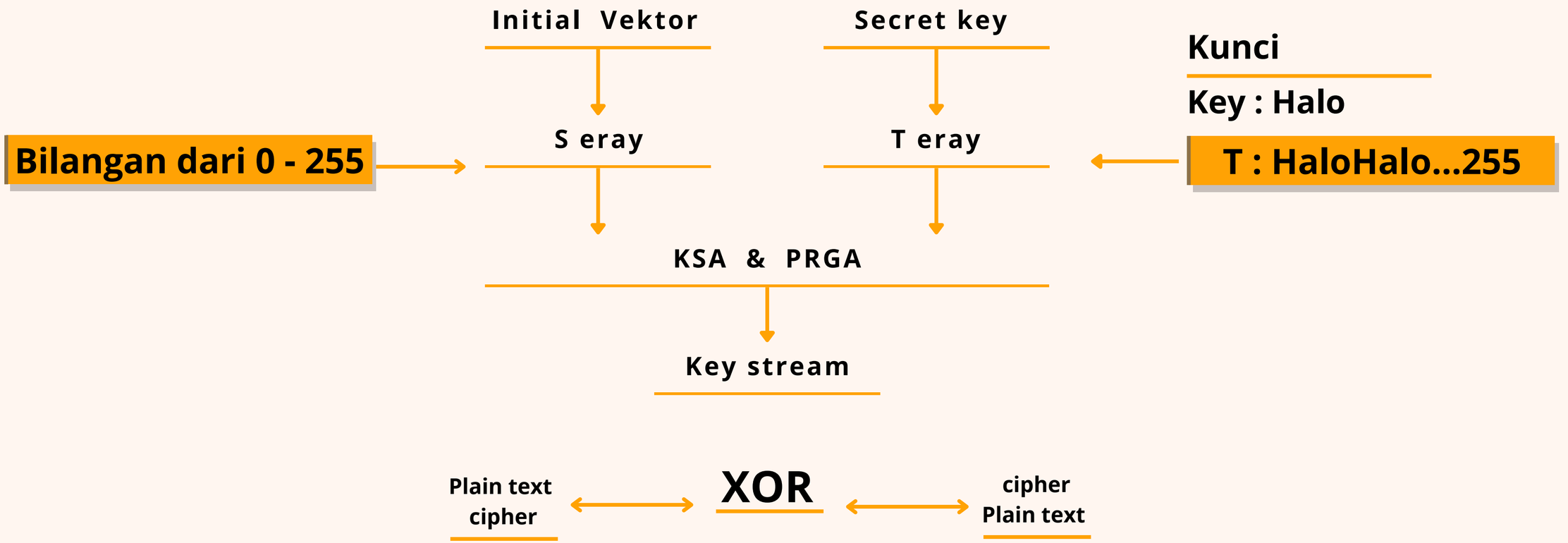
Cara kerjanya



Cara kerjanya



Cara kerjanya



Algoritma RC4

- **Membuat sequence S**

  S: S0 = 0, S1 = 1, S2 = 2, ... S255 = 255,

- **Membuat sequence T**

  T : HaloHaloHaloHalo...255

- **Lakukan permutasi pada nilai S (KSA)**

  Pengacakan pada eray S untuk mendapatkan nilai secara ack ssuwai nilai dari T

```
let j = 0;
for (let i = 0; i < 256; i++) {
  j = (j + S[i] + key.charCodeAt(i % keyLength)) % 256;
  [S[i], S[j]] = [S[j], S[i]]; // Swap
}
```

copy.nugra21

Algoritma RC4

- **Langkah Pengacakan dengan PRGA**

Inisialisasi Indeks i dan j

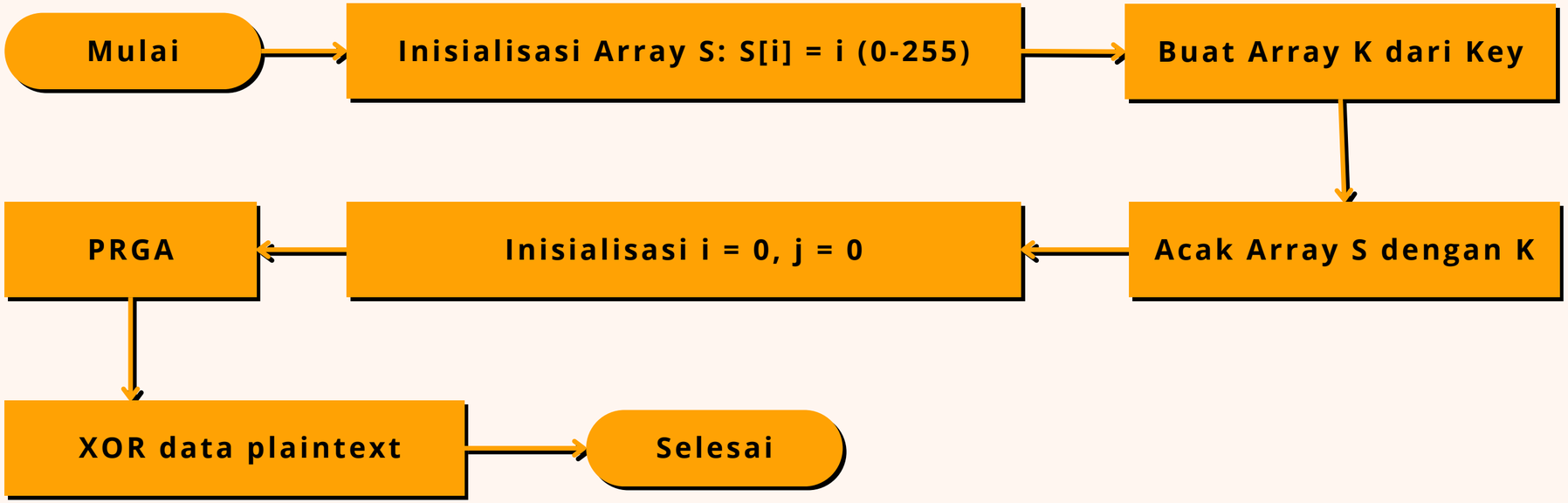
```
// Step 2: Pseudo-Random Generation Algorithm (PRGA)
let i = 0;
j = 0;
const result = [];
for (let char of input) {
  i = (i + 1) % 256;
  j = (j + S[i]) % 256;
  [S[i], S[j]] = [S[j], S[i]]; // Swap
  const k = S[(S[i] + S[j]) % 256];
  result.push(String.fromCharCode(char.charCodeAt(0) ^ k)); // XOR operation
}
```

Algoritma RC4

- **Proses Enkripsi dan Dekripsi**

  Data plaintext dienkripsi dengan XOR byte demi byte dengan keystream k.

Bentuk alir sederhana



Implementasi

Html & css

Js

Copy.nugra21

Video penjelasan lengkap ada di youtube

Link Youtube

Perpustakaan

Link Wikipedia https://en.wikipedia.org/wiki/RC4