**Naskah**

Link ppt [Canva](https://youtu.be/oocm0fDqDKY?si=1oP3Djgcrcgic7v0)

Yow di sini saya akan menjelaskan tentang model kriptografi untuk mengenkripsi dengan metode RC4

Nah sebelum itu disclaimer dulu di encripsi ada yang di sebut dengan

**Stream Cipher dan Block Cipher**

yang pertama ada Stream Cipher

metode enkripsi yang mengenkripsi data satu bit

atau satu byte dalam satu waktu

Biasanya lebih cepat dan digunakan untuk data dengan ukuran besar atau transmisi data secara langsung atau (real-time). Kunci digunakan untuk menghasilkan "keystream" yang dikombinasikan dengan data plaintext menggunakan operasi XOR.

Berikutnya ada Block Cipher

mengenkripsi data dalam blok-blok dengan

ukuran tetap

misalnya 64-bit atau 128-bit). Data yang kurang dari ukuran blok di-padding agar sesuai. Blok-blok ini dienkripsi satu per satu menggunakan algoritma dan kunci tertentu.

**Habis itu ada juga yang di maksut dengan Simmetric Cipher dan Asymmetric Cipher**

Simmetric Cipher

Menggunakan satu kunci untuk proses enkripsi

jadi hanya satu kunci saja

Asymmetric Cipher

Menggunakan pasangan kunci (kunci publik dan

kunci privat)

Kunci publik digunakan untuk enkripsi, sementara kunci privat untuk dekripsi. Metode ini lebih lambat tetapi lebih aman untuk pertukaran kunci.

**RC4 Encryption**

**RC4 adalah algoritma stream cipher**

Ini adalah sebuah algoritma untuk mengenkripsi dengan muda pada zamanya

dan Perancang Ron Rivest pada tahun 1987. dan di publickaskasikan pada tahun 1994 untuk RSA Security dan dikenal karena efisiensi dan kecepatan prosesnya.

sering digunakan untuk aplikasi

* SSL / TLS ( Secure socket ,transport layer ) Biasanya di gunakan pada kemananan website atau yang lebih di kenal dengan HTTPS
* WEP / WPA ( Wired Equivalen Privacy ,Wi-Fi Protected Access ) Ini lebih sering di gunakan untuk jaringan seperti wifi atau aksespoin

Perbaikan :

**[Narator 1 – Pembukaan]**

“Oke, di sini saya akan menjelaskan tentang model kriptografi untuk mengenkripsi dengan metode RC4.

Nah, sebelum masuk ke pembahasan utama, ada baiknya kita mengenal beberapa istilah dalam enkripsi, yaitu **Stream Cipher** dan **Block Cipher**”

**[Narator 1 – Stream Cipher dan Block Cipher]**

“Yang pertama, ada **Stream Cipher**. Ini adalah metode enkripsi yang mengenkripsi data satu bit atau satu byte dalam satu waktu.

Biasanya, metode ini lebih cepat dan digunakan untuk data dengan ukuran besar atau transmisi data secara langsung (real-time). Kunci digunakan untuk menghasilkan ‘keystream’ yang dikombinasikan dengan data plaintext menggunakan operasi XOR.

Berikutnya, ada **Block Cipher**. Metode ini mengenkripsi data dalam blok-blok dengan ukuran tetap, misalnya 64-bit atau 128-bit. Jika data kurang dari ukuran blok, maka akan di-padding agar sesuai. Blok-blok ini dienkripsi satu per satu menggunakan algoritma dan kunci tertentu.”

**[Narator 1 – Symmetric dan Asymmetric Cipher]**

“Setelah itu, ada juga yang dimaksud dengan **Symmetric Cipher** dan **Asymmetric Cipher**.

- **Symmetric Cipher** menggunakan satu kunci untuk proses enkripsi dan dekripsi. Jadi, hanya satu kunci saja yang digunakan.

- **Asymmetric Cipher** menggunakan pasangan kunci, yaitu kunci publik dan kunci privat. Kunci publik digunakan untuk enkripsi, sementara kunci privat untuk dekripsi. Metode ini lebih lambat tetapi lebih aman untuk pertukaran kunci.”

**[Narator 1 – Penjelasan RC4]**

“Selanjutnya, mari kita bahas **RC4 Encryption**.

RC4 adalah algoritma stream cipher. Ini adalah sebuah algoritma yang mudah digunakan pada zamannya. Algoritma ini dirancang oleh Ron Rivest pada tahun 1987 dan dipublikasikan pada tahun 1994 untuk RSA Security. RC4 dikenal karena efisiensi dan kecepatan prosesnya.

RC4 sering digunakan untuk aplikasi seperti:

- SSL/TLS (Secure Socket Layer / Transport Layer Security): Biasanya digunakan pada keamanan website atau yang lebih dikenal dengan HTTPS.

- WEP/WPA (Wired Equivalent Privacy / Wi-Fi Protected Access): Ini sering digunakan untuk jaringan seperti Wi-Fi atau akses poin.”

**[Narator 1 – Penutup]**

“Jadi, itulah pembahasan tentang RC4, mulai dari dasar kriptografi, metode Stream Cipher dan Block Cipher, hingga RC4 dan penerapannya. Semoga penjelasan ini bermanfaat!, Selanjutnya untuk implementasi akan dibahas oleh teman saya…sekian dari saya trimakasih”