Kriptografi Kunci Rahasia & Kunci Publik

- Transposition Cipher
- Substitution Cipher

Overview

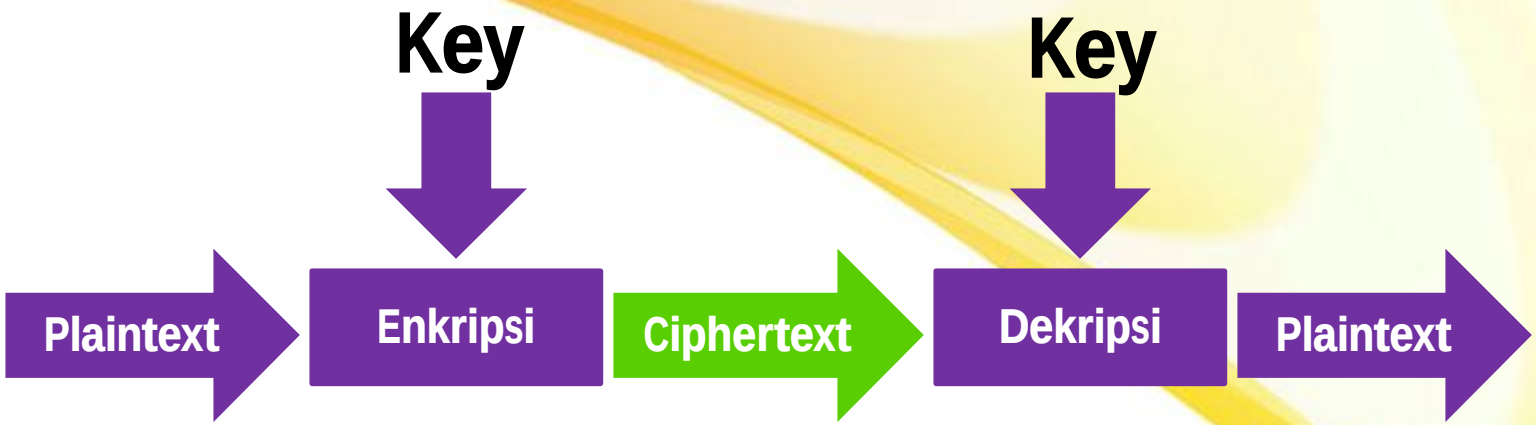
Kriptografi :

- Seni menulis pesan rahasia
- Teks yang dibuat yang hanya bisa dibaca oleh orang yang berhak
- Teknik yang digunakan untuk mengubah informasi ke dalam format alternatif dan diubah kembali ke format semula

Cryptography Modern

- Kriptografi modern selain algoritma juga menggunakan Kunci (Key) untuk memecahkan masalah tersebut
- Proses enkripsi dan dekripsi menggunakan kunci ini
- Setiap anggota memiliki kuncinya yang digunakan untuk proses yang akan dilakukannya
- Namun ada juga algoritma tanpa kunci: *unkeyed cryptosystem.* Co: Fungsi Hash

Cryptography Modern



Picture Explanation

- Ciphertext → Format Alternatif disebut juga text rahasia
- Plaint Text → Informasi/Pesan
- Key → Variable tambahan yang disuntikkan untuk merubah Plaintext ke Ciphertext dan sebaliknya
- Enkripsi → Proses pengubahan format Plaintext menjadi Cypertext
- Dekripsi → Proses pengembalian format Ciphertext menjadi Plaintext

Jenis Kunci Cryptography

- Kriptografi Simetrik (Kunci Rahasia)
- Kriptografi Asimetrik (Kunci Publik)
- Perbedaan utama di antara keduanya terletak pada : Sama dan tidaknya kunci yang digunakan dalam proses enkripsi dengan kunci yang digunakan pada proses dekripsi

Symmetric Cryptography

- Kriptografi simetrik (*symmetric cryptography*) atau dikenal pula sebagai kriptografi kunci rahasia (*secret key cryptography*)
- Merupakan kriptografi yang menggunakan kunci yang sama baik untuk proses enkripsi maupun dekripsi.
- Kriptografi simetrik sangat menekankan pada kerahasiaan kunci yang digunakan untuk proses enkripsi dan dekripsi. Oleh karena itulah kriptografi ini dinamakan pula sebagai kriptografi kunci rahasia
- Contoh algoritma simetrik adalah : OTP, DES (Data Encryption Standard), RC2, RC4 (Ron's Code), Rc5, RC6, IDEA (International Data Encryption Algorithm), Twofish, Magenta, Rijndael (AES-Advanced Encryption Standard), Blowfish, GOST, dan lain – lain
- Block cipher : IDEA, AES, DES
- Stream cipher : RC4

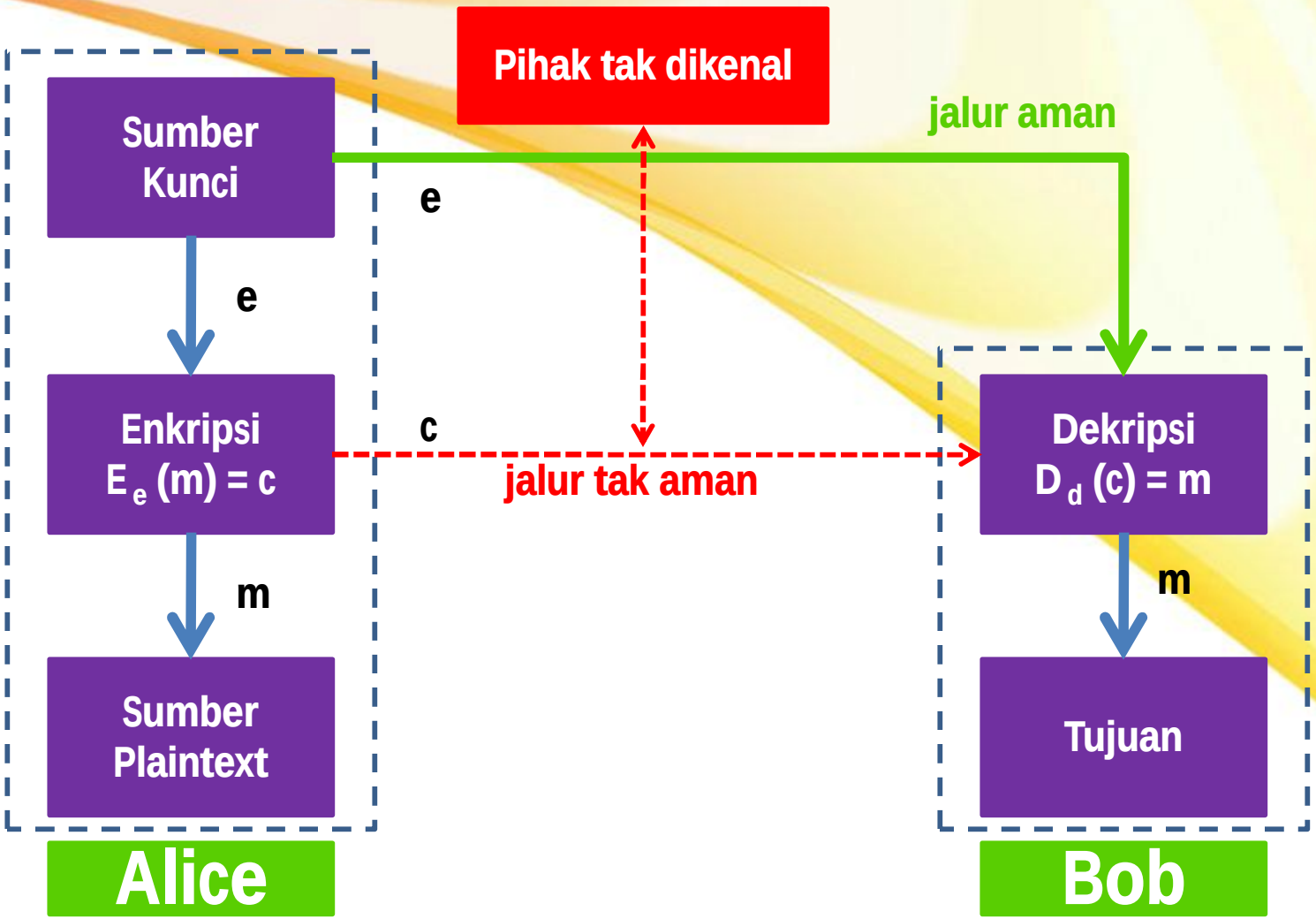
Symmetric Cryptography

- $e = d = k$
- $E_k(m) = c$
- $D_k(c) = m$

Mekanisme Kerja Symmetric Cryptography

- Alice dan Bob menyetujui algoritma simetrik yang akan digunakan
- Alice dan Bob menyetujui kunci yang akan dipakai
- Alice membuat pesan plaintext yang akan dikirimkan kepada Bob, lalu melakukan proses enkripsi dengan menggunakan kunci dan algoritma yang telah disepakati sehingga menghasilkan ciphertext
- Alice mengirimkan ciphertext tersebut kepada Bob
- Bob menerima ciphertext, lalu melakukan dekripsi dengan menggunakan kunci dan algoritma yang sama sehingga dapat memperoleh plaintext tersebut

Mekanisme Kerja Symmetric Cryptography



Kelemahan Symmetric Cryptography

- Harus ada jalur aman (*secure channel) dahulu yang memungkinkan* Bob dan Alice melakukan transaksi kunci
- Hal ini menjadi masalah karena jika jalur itu memang ada, tentunya kriptografi tidak diperlukan lagi dalam hal ini. Masalah ini dikenal sebagai masalah persebaran kunci (*key distribution problem)*
- Kelemahan lainnya adalah bahwa untuk tiap pasang pelaku sistem informasi diperlukan sebuah kunci yang berbeda. Dengan demikian bila terdapat n pelaku sistem informasi, maka agar tiap pasang dapat melakukan komunikasi diperlukan kunci sejumlah total $n(n - 1)/2$ kunci. Untuk jumlah n yang sangat besar, penyediaan kunci ini akan menjadi masalah, yang dikenal sebagai masalah manajemen kunci (*key management problem)*

Keuntungan Symmetric Cryptography

- Dibandingkan dengan kriptografi asimetrik, kriptografi simetrik memiliki kecepatan operasi yang jauh lebih cepat.

Secret Key Cryptosystem

- Block Cipher
  - Transposition Cipher
  - Substitution Cipher
- Stream Cipher
- Polyalphabetic substitutions and Vigenere ciphers
- Polyalphabetic cipher machines and rotors
- Cryptanalysis of classical ciphers

Transposition ciphers

Transposition cipher melakukan proses enkripsi dan dekripsi dengan cara :

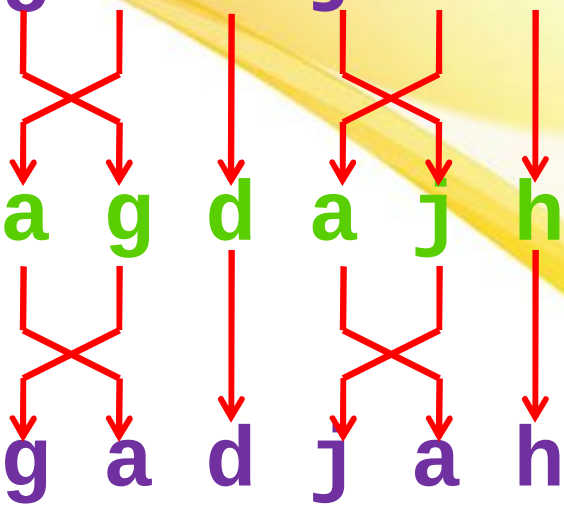
- Mengganti urutan huruf pada Plaintext (enkripsi) dan Ciphertext (dekripsi) dengan aturan tertentu
- Aturan ini membentuk kunci yang di pakai dalam Enkripsi / Dekripsi

Contoh Transposition Cipher

- Misalkan Plaintext “gadjah” dan Kunci “pakai blok berukuran tiga, tukar huruf pertama dengan huruf kedua, huruf ketiga dibuat tetap”.
- Plaintext dibagi beberapa blok dengan ukuran sesuai informasi Kunci, kemudian penukaran Kunci dipakai. Dalam contoh ini Plaintext “gadjah” di enkrip menjadi “agdajh”

Contoh Transposition Cipher

Plaintext : g a d j a h



Enkripsi

Ciphertext : a g d a j h

Dekripsi

Plaintext : g a d j a h

Substitution ciphers

- Dalam *Substitution Cipher* satu huruf Plaintext akan diganti (disubstitusi) dengan huruf lain
- Kriptosistem *Caesar Cipher* dari masa Romawi bisa menjelaskan ide ini dengan baik

Contoh Subtitution Cipher

- Dalam *Caesar Cipher* kita menghitung pengganti sebuah huruf dengan menggeser posisi urutanya sesuai dengan Kunci
- Misalkan Plaintext "gadjah" dan Kunci sama dengan 6
- Kita mulai dengan menggeser secara siklus alfabet asli sebanyak 6 posisi ke kanan

Contoh Subtitution Cipher

Asymetric Cryptography

- Menggunakan kunci enkripsi dan kunci dekripsi yang berbeda
- Kunci enkripsi dapat disebarkan kepada umum dan dinamakan sebagai kunci publik (*public key*) sedangkan kunci dekripsi disimpan untuk digunakan sendiri dan dinamakan sebagai kunci pribadi (*private key*).
- Oleh karena itulah itulah, kriptografi ini dikenal pula dengan nama kriptografi kunci publik (*public key cryptography*)
- Pada kriptosistem asimetrik, setiap pelaku sistem informasi memiliki sepasang kunci, yaitu kunci publik dan kunci pribadi. Kunci public didistribusikan kepada umum, sedangkan kunci pribadi disimpan untuk diri sendiri.
- Contoh algoritma asimetrik adalah : RSA (Rivest Shamir Adleman), DSA (Digital Signature Algorithm), Diffie Hellman, ElGamal, dan lain –lain.

Mekanisme Kerja Asymetric Cryptography

- Alice mengambil kunci publik milik Bob yang didistribusikan kepada umum
- Alice melakukan enkripsi terhadap plaintext dengan kunci publik Bob tersebut sehingga menghasilkan ciphertext
- Alice mengirimkan ciphertext kepada Bob
- Bob yang menerima ciphertext tersebut melakukan proses dekripsi dengan menggunakan kunci pribadi miliknya sehingga mendapatkan plaintext semula

Sekian

&

Terimakasih