SISTEM KRIPTOGRAFI

Mata kuliah Jaringan KomputerJurusan Teknik Informatika

Irawan Afrianto, MT

Materi :

- Kriptografi
- Kriptografi dan Sistem Informasi
- Mekanisme Kriptografi
- Keamanan Sistem Kriptografi

Kriptografi

- Keamanan data baik di komputer maupun di dalam jaringan
- Proses Penyandian data (Enkripsi)
- Kriptografi : Seni atau ilmu untuk menjaga agar pesan rahasia tetap aman.
- Merupakan cabang ilmu matematika
- Penggemar kriptografi – Cryptographer
- Proses Memecahkan sandi kriptografi – Cryptanalyst
- Algoritma kriptografi berkembang dari masa kemasa. Dari algoritma sederhana ke algoritma yang kompleks

Kriptografi dan Sistem Informasi

- Keamanan untuk Sistem Informasi
- Informasi ditujukan untuk segolongan tertentu
- SI dengan kriptografi
- 4 Aspek Fundamental dari Sistem Kriptografi
  - Kerahasiaan (Confidentiality)
  - Integritas Data (Data Integrity)
  - Otentifikasi (Authentication)
  - Ketiadaan Penyangkalan (Non-Repudiation)

Mekanisme Kriptografi

- Mekanisme sistem kriptografi bekerja dengan cara menyandikan pesan menjadi kode rahasia yang dimengerti oleh pelaku sistem informasi saja.
- Istilah umum yang digunakan pada kriptografi :
  - Plaintext
  - Chiphertext
  - Cipher
  - Enkripsi
  - Dekripsi
  - Kriptosistem

Enkripsi

- Kerahasian Pesan yang akan disampaikan
- Tiga kategori Enkripsi
  - Kunci enkripsi rahasia, terdapat sebuah kunci untuk meng-enkripsi dan seklaligus mendekripsi informasi
  - Kunci ekripsi Public – terdapat dua kunci , satu untuk proses enkripsi, satu untuk proses dekripsi
  - Fungsi One-Way – informasi di enkripsi untuk menciptakan “signature” dari informasi asli yang digunakan untuk proses autentifikasi

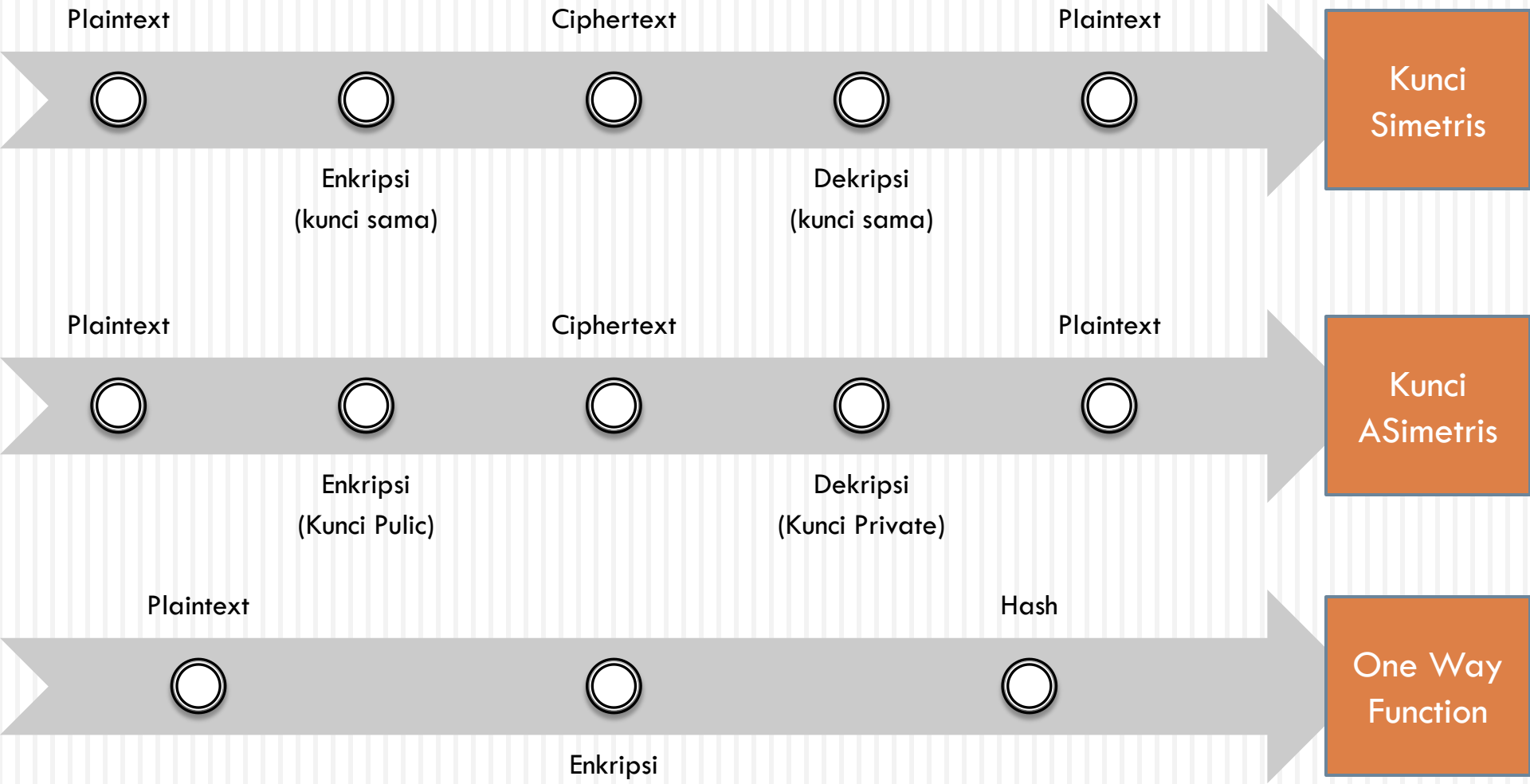
Enkripsi

- Enkripsi Dibentuk berdasar suatu algoritma yang akan mengacak suatu informasi menjadi bentuk yang tidak dapat dibaca / di lihat
- Dekripsi adalah proses dengan algoritma yang sama untuk mengembalikan pesan kebentuk aslinya
- Algoritma yang digunakan harus terdiri dari susunan prosedur yang direncanakan secara hati-hati dan efektif.

Enkripsi

- Enkripsi Dibentuk berdasar suatu algoritma yang akan mengacak suatu informasi menjadi bentuk yang tidak dapat dibaca / di lihat
- Dekripsi adalah proses dengan algoritma yang sama untuk mengembalikan pesan kebentuk aslinya
- Algoritma yang digunakan harus terdiri dari susunan prosedur yang direncanakan secara hati-hati dan efektif.
- Muncul algoritma kriptografi Simetris, Asimetris dan Single Way

Enkripsi


Plaintext
Ciphertext
Plaintext
Enkripsi
(kunci sama)
Dekripsi
(kunci sama)
Kunci
Simetris
Plaintext
Ciphertext
Plaintext
Enkripsi
(Kunci Pulic)
Dekripsi
(Kunci Private)
Kunci
ASimetris
Plaintext
Hash
Enkripsi
One Way
Function

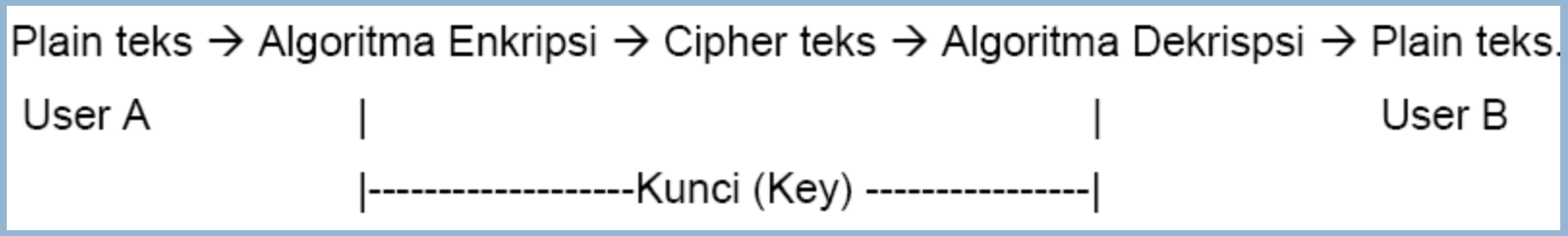
Cara Kerja Enkripsi

- Enkripsi digunakan untuk menyandikan data-data atau informasi
- Data dapat disandikan dengan menggunakan sebuah kunci
- Untuk membukanya dapat digunakan kunci yang sama (Private Key) atau dengan kunci yang berbeda (Public Key)
- Faktor-faktor yang mepengaruhi kuat lemah suatu enkripsi :
  - Algoritma Enkripsinya
  - Kekuatan Kuncinya
- Model yang banyak digunakan didasarkan pada Data Encryption Standard (DES)

Cara Kerja Enkripsi

- Enkripsi digunakan untuk menyandikan data-data atau informasi
- Data dapat disandikan dengan menggunakan sebuah kunci
- Untuk membukanya dapat digunakan kunci yang sama (Private Key) atau dengan kunci yang berbeda (Public Key)
- Faktor-faktor yang mepengaruhi kuat lemah suatu enkripsi :
  - Algoritma Enkripsinya
  - Kekuatan Kuncinya
- Model yang banyak digunakan didasarkan pada Data Encryption Standard (DES)

Enkripsi Konvensional



•Informasi asal yang dapat di mengerti di simbolkan oleh Plain teks, yang kemudian oleh algoritma Enkripsi diterjemahkan menjadi informasi yang tidak dapat untuk dimengerti yang disimbolkan dengan cipher teks. Proses enkripsi terdiri dari dua yaitu algoritma dan kunci.

•Kunci biasanya merupakan suatu string bit yang pendek yang mengontrol algoritma. Algoritma enkripsi akan menghasilkan hasil yang berbeda tergantung pada kunci yang digunakan. Mengubah kunci dari enkripsi akan mengubah output dari algortima enkripsi.

•Sekali cipher teks telah dihasilkan, kemudian ditransmisikan. Pada bagian penerima selanjutnya cipher teks yang diterima diubah kembali ke plain teks dengan algoritma dan dan kunci yang sama.

Enkripsi Public-Key

•Salah satu yang menjadi kesulitan utama dari enkripsi konvensional adalah perlunya untuk mendistribusikan kunci yang digunakan dalam keadaan aman. Sebuah cara yang tepat telah diketemukan untuk mengatasi kelemahan ini dengan suatu model enkripsi yang secara mengejutkan tidak memerlukan sebuah kunci untuk didistribusikan

•dimungkinkan untuk membangun suatu algoritma yang menggunakan satu kunci untuk enkripsi dan pasangannya, kunci yang berbeda, untuk dekripsi. Lebih jauh lagi adalah mungkin untuk menciptakan suatu algoritma yang mana pengetahuan tentang algoritma enkripsi ditambah kunci enkripsi tidak cukup untuk menentukan kunci dekrispi

Enkripsi Public-Key

Teknik Yang Digunakan pada Enkripsi Public Key:

1. Masing – masing dari sistem dalam network akan menciptakan sepasang kunci yang digunakan untuk enkripsi dan dekripsi dari informasi yang diterima.
2. Masing – masing dari sistem akan menerbitkan kunci enkripsinya (public key) dengan memasang dalam register umum atau file, sedang pasangannya tetap dijaga sebagai kunci pribadi (private key).
3. Jika A ingin mengirim pesan kepada B, maka A akan mengenkripsi pesannya dengan kunci publik dari B.
4. Ketika B menerima pesan dari A maka B akan menggunakan kunci privatenya untuk mendeskripsi pesan dari A.

public-key memecahkan masalah pendistribusian karena tidak diperlukan suatu kunci untuk didistribusikan. Semua partisipan mempunyai akses ke kunci publik (public key) dan kunci pribadi dihasilkan secara lokal oleh setiap partisipan sehingga tidak perlu untuk didistribusikan. Selama sistem mengontrol masing – masing private key dengan baik maka komunikasi menjadi komunikasi yang aman. Setiap sistem mengubah private key pasangannya public key akan menggantikan public key yang lama.

Aspek Penting Pada Enkripsi Konvensional dan Public Key

Enkripsi Konvensional

Yang dibutuhkan untuk bekerja :
Algoritma yang sama dengan kunci yang sama dapat digunakan untuk proses dekripsi – enkripsi.
Pengirim dan penerima harus membagi algoritma dan kunci yang sama.

Y**ang dibutuhkan untuk keamanan :**
Kunci harus dirahasiakan.
Adalah tidak mungkin atau sangat tidak praktis untuk menerjemahkan informasi yang telah dienkripsi.
Pengetahuan tentang algoritma dan sample dari kata yang terenkripsi tidak mencukupi untu menentukan kunci.

Enkripsi Public Key.

Yang dibutuhkan untuk bekerja :
Algoritma yang digunakan untuk enkripsi dan dekripsi dengan sepasang kunci, satu untuk enkripsi satu untuk dekripsi.
Pengirim dan penerima harus mempunyai sepasang kunci yang cocok.

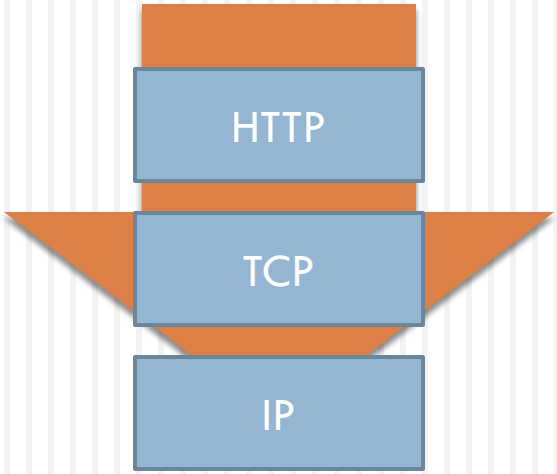
Yang dibutuhkan untuk keamanan :
Salah satu dari kunci harus dirahasiakan.
Adalah tidak mungkin atau sangat tidak praktis untuk menerjemahkan informasi yang telah dienkripsi.
Pengetahuan tentang algoritma dan sample dari kata yang terenkripsi tidak mencukupi untu menentukan kunci.

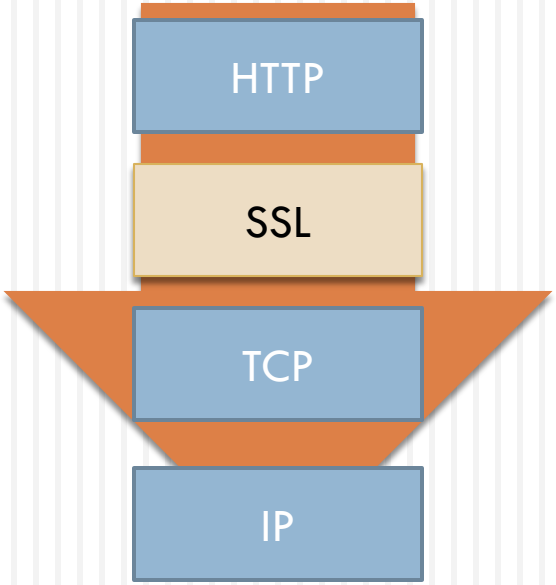
Keamanan Sistem Kriptografi

- Keamanan pada sistem kriptografi merupakan masalah fundamental
- Dengan sistem terbuka, sistem kriptografi akan lebih mudah dianalisa
- Sistem kriptografi dirancang untuk menjadi plainteks supaya tidak dapat dibaca oleh pihak-pihak yang tidak berwenang yang sering disebut Attacker
- Tipe serangan paling umum terhadap kriptografi adalah kriptanalisis yaitu upaya-upaya untuk membongkar cipherteks menjadi plainteks tanpa memiliki informasi tentang kunci yang digunakan

Penggunaan Sistem Kriptografi

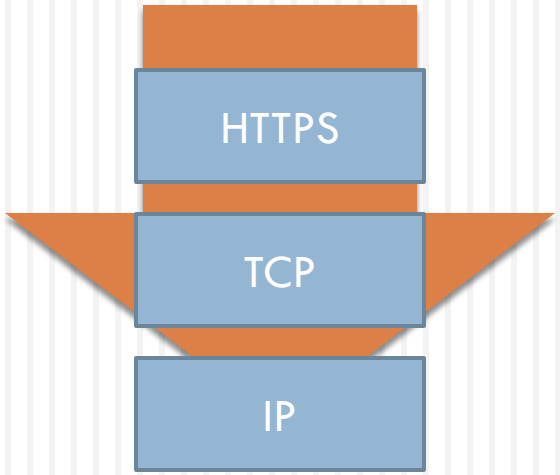
- Sistem kriptografi pada era informasi digunakan dalam mengamanan sistem informasi
- Pada jaringan komputer TCP/IP memanfaatkan kriptografi pada protocol S/HTTP
- Protocol S/HTTP (Secure HyperText Transfer Protocol) digunakan dengan mekanisme kriptografi untuk menyandikan pesan yang dikirimkan





Penggunaan Sistem Kriptografi

- Penambahan Satu layer baru yang dinamakan SSL (Secure Socket Layer) yang berfungsi untuk melaksanakan mekanisme kriptografi terhadap informasi sebelum dilakukan enkapsulasi dan pengiriman data
- Penambahan Prrotocol SSL menyebabkan terbentuknya protocol baru yang dinamakan HTTPS, menggantikan protokol HTTP untuk transaksi yang aman (mis. E-Commerce)



TERIMA KASIH

Jaringan Komputer Teknik Informatika