Bab 1

Pengantar Kriptografi

1.1 Tujuan Pembelajaran

Setelah mempelajari bab ini, mahasiswa mampu:

- Menjelaskan sejarah singkat dan motivasi kriptografi.
- Mendefinisikan kriptografi dan tujuan keamanannya (kerahasiaan, integritas, keaslian, nir-sangkal).
- Membedakan primitif-primitif dasar dan model ancaman tingkat tinggi.
- Menggambarkan konsep kriptografi konvensional (simetris) secara umum.

1.2 Sejarah Singkat

Kriptografi telah digunakan sejak zaman kuno, misalnya sandi Caesar pada Romawi dan sandi Vigenère pada abad ke-16. Revolusi besar terjadi pada abad ke-20 melalui karya Claude Shannon dan perkembangan mesin Enigma pada Perang Dunia II, diikuti munculnya kriptografi modern berbasis teori kompleksitas komputasi pada tahun 1970-an (Diffie–Hellman dan RSA). Rujukan modern yang komprehensif dapat dilihat pada (**???**).

1.3 Definisi dan Tujuan Keamanan

Definisi 1.1 (Kriptografi)**.** Kriptografi adalah ilmu dan seni merancang mekanisme yang memungkinkan pihak-pihak berkomunikasi dengan aman di hadapan penyerang, dengan tujuan utama seperti kerahasiaan, integritas, keaslian/origin, dan nir-sangkal.

Tujuan keamanan umum:

- **Kerahasiaan**: hanya pihak berwenang yang mengetahui isi pesan.
- **Integritas**: perubahan pesan dapat dideteksi.
- **Otentikasi/Keaslian**: jaminan identitas pihak pengirim/penyusun pesan.
- **Nir-sangkal**: pengirim tidak dapat menyangkal telah mengirim pesan (umum pada tanda tangan digital).

1.4 Model Dasar Sistem Kriptografi

Sebuah skema kriptografi tipikal melibatkan pesan asli (plaintext), kunci, algoritma enkripsi menghasilkan ciphertext, serta algoritma dekripsi untuk memulihkan plaintext. Keamanan

dinilai terhadap model penyerang (misalnya penyerang yang mengetahui ciphertext saja, atau memiliki akses ke orakel enkripsi/dekripsi) (**?**).

1.5 Kriptografi Konvensional (Simetris)

Kriptografi simetris menggunakan satu kunci rahasia bersama untuk enkripsi dan dekripsi. Keluarga utama: *sandi blok* (block cipher) dan *sandi alir* (stream cipher). Keunggulan utama adalah efisiensi; kelemahannya adalah pendistribusian kunci rahasia ke semua pihak yang berkomunikasi (**?**).

1.6 Contoh Sederhana: Sandi Geser

Misal alfabet Latin dan pergeseran 3 (sandi Caesar). Enkripsi: ganti setiap huruf dengan huruf ke-3 berikutnya secara siklik. Dekripsi: geser balik 3. Sandi klasik ini mudah dipecahkan (misal analisis frekuensi) sehingga tidak aman secara modern.

1.7 Latihan

1. Terapkan sandi Caesar dengan pergeseran 7 untuk mengenkripsi dan mendekripsi sebuah kalimat. Diskusikan kelemahan utamanya.
2. Sebutkan perbedaan tujuan *integritas* dan *otentikasi*. Berikan contoh skenario.
3. Uraikan mengapa distribusi kunci adalah masalah utama pada kriptografi simetris.

1.8 Bacaan Lanjutan

- (**?**) untuk pengantar menyeluruh sistem klasik dan modern.
- (**?**) untuk landasan formal dan definisi keamanan.
- (**?**) sebagai referensi terbuka yang kaya dengan detail teknis.