# Buku Ajar Kriptografi

Program Studi S1 Matematika
FMIPA Universitas Bale Bandung

Tim Pengajar Kriptografi

6 Oktober 2025

# Daftar Isi

# 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 [Stallings, 2016, Katz and Lindell, 2020, Menezes et al., 1996].

## 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) [Katz and Lindell, 2020].

## 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 [Stallings, 2016].

## 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

- [Stallings, 2016] untuk pengantar menyeluruh sistem klasik dan modern.
- [Katz and Lindell, 2020] untuk landasan formal dan definisi keamanan.
- [Menezes et al., 1996] sebagai referensi terbuka yang kaya dengan detail teknis.

# Bab 2

# Lanskap Primitif Modern: Kunci Publik, Tanda Tangan, Hash, Sertifikat

## 2.1 Tujuan Pembelajaran

Mahasiswa mampu membedakan sistem kunci publik dan privat (simetris), menjelaskan fungsi hash, tanda tangan digital, serta konsep sertifikat digital dan infrastruktur kunci publik (PKI).

## 2.2 Sistem Kunci Publik vs. Kunci Privat

**Kunci privat/simetris**: satu kunci rahasia bersama. Contoh penggunaan: AES dalam mode operasi yang aman. Keunggulan: sangat cepat; kelemahan: distribusi kunci.

**Kunci publik/asimetris**: pasangan kunci (publik, privat). Publik untuk enkripsi atau verifikasi, privat untuk dekripsi atau penandatanganan. Memudahkan distribusi kunci, tetapi relatif lebih lambat [Katz and Lindell, 2020, Stallings, 2016].

## 2.3 Fungsi Hash Kriptografis

**Definisi 2.1** (Fungsi Hash)**.** Pemetaan deterministik dari string panjang ke nilai tetap (digest) dengan sifat tahan tabrakan, tahan pra-citra, dan tahan pra-citra kedua (secara ideal).

Penggunaan: ringkas pesan, membangun MAC dan tanda tangan, verifikasi integritas [Menezes et al., 1996].

## 2.4 Tanda Tangan Digital

Skema tanda tangan menjamin keaslian dan nir-sangkal. Pihak penandatangan menggunakan kunci privat untuk menghasilkan tanda tangan atas pesan (sering atas hash pesan); pihak verifikator menggunakan kunci publik untuk memverifikasi [Katz and Lindell, 2020].

## 2.5 Sertifikat Digital dan PKI

Sertifikat mengikat identitas dengan kunci publik menggunakan tanda tangan dari *Certificate Authority* (CA). PKI menyediakan prosedur penerbitan, pencabutan, dan validasi sertifikat. Keamanannya bergantung pada kebijakan dan keandalan CA [Stallings, 2016].

## 2.6 Latihan

1. Jelaskan mengapa fungsi hash harus tahan tabrakan. Apa dampaknya pada tanda tangan digital jika tidak?
2. Bandingkan model distribusi kunci pada sistem simetris vs. asimetris.
3. Berikan contoh penggunaan sertifikat digital pada protokol TLS.

# Bab 3

# Aritmetika Bilangan Bulat dan Kongruensi

## 3.1 Tujuan Pembelajaran

Mahasiswa memahami FPB/GCD, keterbagian, kongruensi, ring $\mathbb{Z}_n$, Algoritma Euklid dan Euklid diperluas, serta penerapannya untuk invers modulo.

## 3.2 Keterbagian, FPB, dan Algoritma Euklid

**Definisi 3.1** (FPB/GCD)**.** FPB dari bilangan bulat $a$ dan $b$, ditulis $\gcd(a, b)$, adalah pembagi bersama terbesar. Algoritma Euklid menghitung $\gcd(a, b)$ secara efisien dengan pembagian berulang [Rosen, 2012].

**Teorema 3.1** (Identitas Bezout)**.** *Untuk $a, b \in \mathbb{Z}$ tidak keduanya nol, terdapat $x, y \in \mathbb{Z}$ sehingga $ax + by = \gcd(a, b)$. Nilai $x, y$ dihitung dengan Algoritma Euklid diperluas [Hoffstein et al., 2014].*

## 3.3 Kongruensi dan Ring $\mathbb{Z}_n$

**Definisi 3.2** (Kongruensi)**.** Untuk $n \geq 2$, dua bilangan bulat $a, b$ kongruen modulo $n$, ditulis $a \equiv b \pmod{n}$, jika $n \mid (a - b)$. Kelas sisa modulo $n$ membentuk ring $\mathbb{Z}_n$ [Hoffstein et al., 2014].

## 3.4 Invers Perkalian Modulo

Elemen $[a] \in \mathbb{Z}_n$ memiliki invers perkalian jika dan hanya jika $\gcd(a, n) = 1$. Algoritma Euklid diperluas menghasilkan invers $a^{-1} \bmod n$.

**Contoh.** Cari invers dari $a = 17$ modulo $n = 43$. Dengan Euklid diperluas diperoleh $17 \cdot 38 \equiv 1 \pmod{43}$, sehingga $17^{-1} \equiv 38 \bmod 43$.

## 3.5 Latihan

1. Hitung $\gcd(414, 662)$ dan koefisien Bezout-nya.
2. Tentukan semua solusi dari $15x \equiv 6 \pmod{21}$.
3. Temukan invers dari 11 modulo 97, jika ada.

# Bab 4

# Sistem Kongruensi Linier, CRT, dan Teorema Kecil Fermat

## 4.1 Tujuan Pembelajaran

Mahasiswa menguasai penyelesaian kongruensi linier, Teorema Sisa Tiongkok (CRT), fungsi phi Euler, medan hingga $\mathbb{Z}_p$, dan Teorema Kecil Fermat beserta aplikasinya.

## 4.2 Kongruensi Linier dan Fungsi $\varphi$ Euler

Persamaan $ax \equiv b \pmod{n}$ memiliki solusi jika dan hanya jika $\gcd(a, n) \mid b$. Jumlah kelas sisa invertibel di $\mathbb{Z}_n$ adalah $\varphi(n)$. Untuk $n = \prod p_i^{e_i}$, $\varphi(n) = \prod p_i^{e_i-1}(p_i - 1)$ [Hoffstein et al., 2014].

## 4.3 Teorema Sisa Tiongkok (CRT)

Jika $n_1, \ldots, n_k$ saling bebas, maka sistem

$$x \equiv a_i \pmod{n_i}, \quad i = 1, \ldots, k$$

mempunyai solusi unik modulo $N = \prod n_i$. CRT penting untuk percepatan perhitungan modular (misal implementasi RSA) [Menezes et al., 1996].

## 4.4 Medan Hingga $\mathbb{Z}_p$ dan FLT

Untuk prima $p$, $\mathbb{Z}_p$ adalah medan: setiap elemen non-nol memiliki invers.

**Teorema 4.1** (Teorema Kecil Fermat)**.** *Jika $p$ prima dan $a \not\equiv 0 \pmod{p}$, maka $a^{p-1} \equiv 1 \pmod{p}$. Secara umum, $a^p \equiv a \pmod{p}$ untuk semua $a \in \mathbb{Z}$ [Rosen, 2012].*

Aplikasi: menguji invertibilitas, menyederhanakan perpangkatan modular, dan fondasi RSA [Rivest et al., 1978].

**Contoh.** Selesaikan $7x \equiv 1 \pmod{19}$. Karena $7^{18} \equiv 1$, maka $7^{-1} \equiv 7^{17} \bmod 19$. Perhitungan cepat (eksponeniasi biner) memberi $7^{-1} \equiv 11 \bmod 19$.

## 4.5 Latihan

1. Selesaikan sistem: $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$, $x \equiv 2 \pmod 7$.
2. Hitung $\varphi(2^4 \cdot 3^2 \cdot 5)$.
3. Buktikan atau beri argumen mengapa $a^{\varphi(n)} \equiv 1 \pmod n$ jika $\gcd(a, n) = 1$ (Teorema Euler).

# Bab 5

# Akar Primitif, Residu Kuadratik, dan Logaritma Diskrit

## 5.1 Tujuan Pembelajaran

Mahasiswa memahami akar primitif di $\mathbb{Z}_p$, residu kuadratik, simbol Legendre, dan masalah logaritma diskrit beserta implikasi keamanannya.

## 5.2 Akar Primitif di $\mathbb{Z}_p$

Untuk prima $p$, himpunan $\mathbb{Z}_p^\times$ membentuk grup abelian siklik orde $p-1$. Sebuah elemen $g$ disebut *akar primitif* jika $\langle g \rangle = \mathbb{Z}_p^\times$. Keberadaan akar primitif di $\mathbb{Z}_p$ terjamin; perhitungan generator penting untuk kriptografi berbasis grup siklik [Hoffstein et al., 2014].

## 5.3 Residu Kuadratik dan Simbol Legendre

Bilangan $a \in \mathbb{Z}_p$ disebut *residu kuadratik* jika ada $x$ sehingga $x^2 \equiv a \pmod{p}$. Simbol Legendre didefinisikan $\left(\frac{a}{p}\right) \in \{-1, 0, 1\}$ dengan nilai 1 jika residu kuadratik non-nol, 0 jika $p \mid a$, dan -1 selain itu. Kriteria Euler: $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$ [Hoffstein et al., 2014].

## 5.4 Masalah Logaritma Diskrit

Diberi $g$ generator dan $h \in \langle g \rangle$, masalah mencari $x$ dengan $g^x \equiv h$ disebut *logaritma diskrit*. Diyakini sulit pada banyak grup, dan menjadi dasar skema Diffie–Hellman dan ElGamal [Diffie and Hellman, 1976, Hoffstein et al., 2014].

## 5.5 Latihan

1. Tentukan apakah 3 adalah akar primitif modulo $p = 7$. Jika tidak, temukan satu generator.
2. Hitung $\left(\frac{5}{11}\right)$ menggunakan Kriteria Euler.
3. Diberi $g = 2$ modulo $p = 29$ dan $h = 18$, carilah $x$ sehingga $2^x \equiv 18 \pmod{29}$ dengan pencarian kecil (baby-step).

# Bab 6

# Sandi Blok dan Sandi Alir; DES

## 6.1 Tujuan Pembelajaran

Mahasiswa memahami perbedaan sandi blok dan sandi alir, struktur tinggi DES, dan isu keamanannya.

## 6.2 Sandi Blok vs. Sandi Alir

Sandi blok memproses blok tetap (mis. 64/128 bit) dengan kunci rahasia, memerlukan mode operasi (ECB, CBC, CTR, GCM). Sandi alir menghasilkan keystream untuk di-XOR dengan plaintext. Pemilihan mode sangat krusial bagi keamanan [Stallings, 2016, Menezes et al., 1996].

## 6.3 Data Encryption Standard (DES)

DES adalah sandi blok 64-bit dengan kunci efektif 56-bit, menggunakan struktur Feistel 16 putaran. Kini DES dianggap tidak aman karena ruang kunci kecil (serangan brute force) dan kelemahan desain historis [National Institute of Standards and Technology, 1999, Stallings, 2016].

**Ringkas Struktur.** DES menggunakan permutasi awal/akhir, ekspansi, S-box nonlinier, dan P-box permutasi. Desain Feistel memastikan dekripsi menggunakan algoritma yang sama dengan urutan subkunci terbalik.

## 6.4 Isu Keamanan dan Penggantinya

Serangan pencarian kunci menyeluruh dan teknik kriptoanalisis modern melemahkan DES. Triple-DES dan akhirnya AES menggantikan DES pada standar internasional [National Institute of Standards and Technology, 1999, 2001].

## 6.5 Latihan

1. Jelaskan perbedaan konseptual antara sandi blok dan sandi alir.
2. Mengapa kunci 56-bit dianggap tidak memadai saat ini?

3. Sebutkan keuntungan struktur Feistel untuk desain sandi blok.

# Bab 7

# DES dan Variannya; AES; IDEA

## 7.1 Tujuan Pembelajaran

Mahasiswa memahami varian DES (iterated DES, DESX), prinsip AES, dan gambaran IDEA.

## 7.2 Varian DES

**Triple-DES** mengaplikasikan DES tiga kali (mis. EDE) untuk memperpanjang keamanan. **DESX** menambahkan whitening kunci untuk memperluas ruang kunci efektif. Meskipun lebih aman dari DES tunggal, performanya kalah dari AES [Stallings, 2016].

## 7.3 Advanced Encryption Standard (AES)

AES (Rijndael) adalah sandi blok 128-bit dengan ukuran kunci 128/192/256-bit. Bukan Feistel, melainkan transformasi putaran: SubBytes, ShiftRows, MixColumns, AddRoundKey yang didefinisikan atas medan hingga $\mathbb{F}_{2^8}$. AES adalah standar de facto saat ini [National Institute of Standards and Technology, 2001].

## 7.4 IDEA

International Data Encryption Algorithm menggunakan operasi campuran penjumlahan modulo $2^{16}$, XOR, dan perkalian modulo $2^{16}+1$. Desain ini menyeimbangkan difusi dan konfusi dengan operasi heterogen [Stallings, 2016].

## 7.5 Latihan

1. Bandingkan keamanan relatif DES, 3DES, dan AES.
2. Mengapa AES menggunakan $\mathbb{F}_{2^8}$ pada operasi S-box?
3. Beri contoh peran whitening pada DESX.

# Bab 8

# LFSR, Vigenère, SEAL, RC4

## 8.1 Tujuan Pembelajaran

Mahasiswa memahami LFSR, sandi Vigenère, dan sandi alir modern SEAL dan RC4 beserta aspek keamanannya.

## 8.2 Linear Feedback Shift Register (LFSR)

LFSR menghasilkan deret biner melalui umpan balik linear atas $\mathbb{F}_2$. Banyak dipakai sebagai komponen pembangkit keystream; tetapi lineritas memudahkan kriptoanalisis jika digunakan tanpa pengacakan tambahan [Menezes et al., 1996].

## 8.3 Sandi Vigenère

Sandi klasik polialfabetik menggunakan kunci kata untuk menentukan pergeseran siklik per posisi. Rentan terhadap analisis Kasiski dan indeks koincidensi; tidak aman secara modern [Stallings, 2016].

## 8.4 SEAL

SEAL adalah sandi alir berkecepatan tinggi berbasis fungsi pseudo-acak yang dipetakan dari kunci dan nonce, dirancang untuk efisiensi perangkat lunak [Rogaway and Coppersmith, 1994].

## 8.5 RC4

RC4 adalah sandi alir terkenal dengan inisialisasi KSA dan PRGA yang menghasilkan keystream. Ditemukan berbagai bias pada keluaran awal sehingga butuh pembuangan byte awal; banyak standar modern tidak lagi merekomendasikan RC4 [Mantin and Shamir, 2001, Stallings, 2016].

## 8.6 Latihan

1. Jelaskan mengapa LFSR murni tidak cocok sebagai sandi alir modern.

2. Demonstrasikan enkripsi dan dekripsi singkat dengan sandi Vigenère.
3. Mengapa RC4 tidak direkomendasikan pada protokol modern seperti TLS?

# Bab 9

# Kunci Publik: Fermat Kecil dan RSA

## 9.1 Tujuan Pembelajaran

Mahasiswa memahami konsep sistem kunci publik, peran Teorema Kecil Fermat/Euler, dan konstruksi RSA beserta aspek keamanannya.

## 9.2 Konsep Sistem Kunci Publik

Model asimetris menggunakan kunci publik untuk enkripsi dan kunci privat untuk dekripsi. Keuntungan utama: distribusi kunci menjadi sederhana; kelemahan: efisiensi lebih rendah dibanding simetris [Katz and Lindell, 2020].

## 9.3 Teorema Kecil Fermat dan Euler

FLT: untuk prima $p$ dan $a \not\equiv 0 \pmod{p}$, $a^{p-1} \equiv 1 \pmod{p}$. Generalisasi: $a^{\varphi(n)} \equiv 1 \pmod{n}$ jika $\gcd(a, n) = 1$. Identitas ini digunakan dalam pembuktian kebenaran RSA [Hoffstein et al., 2014, Rosen, 2012].

## 9.4 Skema RSA

**Pembangkit kunci.** Pilih prima besar $p, q$, hitung $n = pq$, $\varphi(n) = (p-1)(q-1)$. Pilih $e$ koprima dengan $\varphi(n)$, lalu hitung $d \equiv e^{-1} \pmod{\varphi(n)}$. Kunci publik: $(n, e)$, kunci privat: $d$.

**Enkripsi/Dekripsi.** Enkripsi: $c \equiv m^e \bmod n$. Dekripsi: $m \equiv c^d \bmod n$. Benar karena $ed \equiv 1 \pmod{\varphi(n)}$ dan Teorema Euler [Rivest et al., 1978].

## 9.5 Praktik Aman RSA

Gunakan padding aman semisal OAEP; hindari eksponen kecil tanpa mitigasi, lindungi terhadap serangan waktu dan side-channel; gunakan CRT untuk percepatan dekripsi dengan hati-hati [Katz and Lindell, 2020, Menezes et al., 1996].

## 9.6 Latihan

1. Bangkitkan contoh kecil RSA dengan $p = 53$, $q = 59$, pilih $e = 17$, hitung $d$.
2. Tunjukkan bahwa dekripsi memulihkan pesan dengan Teorema Euler.
3. Jelaskan peran padding OAEP pada keamanan semantik.

# Bab 10

# Tanda Tangan Digital: Konsep, RSA, Ong–Schnorr–Shamir

## 10.1 Tujuan Pembelajaran

Mahasiswa memahami tujuan dan cara kerja tanda tangan digital, skema RSA, serta gambaran skema Ong–Schnorr–Shamir.

## 10.2 Konsep dan Model Keamanan

Tanda tangan digital menyediakan otentikasi, integritas, dan nir-sangkal. Keamanan formal: unforgeability under chosen-message attack (UF-CMA). Praktik: menandatangani *hash* pesan, bukan pesan mentah [Katz and Lindell, 2020].

## 10.3 Tanda Tangan RSA

Kunci seperti RSA enkripsi. Tanda tangan atas pesan $m$ biasanya pada digest $H(m)$: $\sigma \equiv H(m)^d \bmod n$. Verifikasi: cek $H(m) \equiv \sigma^e \bmod n$. Gunakan padding dan skema standar seperti RSA-PSS [Katz and Lindell, 2020, Stallings, 2016].

## 10.4 Ong–Schnorr–Shamir (OSS)

OSS adalah keluarga skema tanda tangan awal berbasis gagasan trapdoor, menawarkan efisiensi tertentu namun jarang digunakan dibanding ECDSA/RSA modern. Fokus pembelajaran: struktur umum tanda tangan dan verifikasi batch [Stallings, 2016].

## 10.5 Verifikasi Batch

Untuk kelas skema tertentu (mis. tanda tangan yang bersifat homomorfik), beberapa tanda tangan dapat diverifikasi sekaligus guna efisiensi. Perlu analisis keamanan untuk mencegah serangan yang mengeksploitasi penggabungan [Katz and Lindell, 2020].

## 10.6 Latihan

1. Uraikan perbedaan RSA-PKCS#1 v1.5, RSA-PSS, dan implikasi keamanannya.
2. Mengapa tanda tangan dilakukan atas hash, bukan pesan asli?
3. Berikan sketsa bagaimana verifikasi batch dapat menghemat waktu untuk tanda tangan bergaya RSA.

# Bab 11

# Distribusi Kunci dan Manajemen Kunci

## 11.1 Tujuan Pembelajaran

Mahasiswa memahami latar belakang, konsep, metode distribusi kunci rahasia dan publik, usia kunci, pengendalian pemakaian, serta peran pihak ketiga tepercaya.

## 11.2 Latar Belakang dan Konsep Dasar

Distribusi dan manajemen kunci adalah fondasi keamanan praktis. Tanpa pengelolaan yang benar, primitif yang kuat sekalipun menjadi rentan [Stallings, 2016].

## 11.3 Metode Distribusi Kunci Rahasia

Pertukaran kunci secara fisik, protokol berbasis *key exchange* (mis. Diffie–Hellman), dan penggunaan *key wrapping*. Tantangan: autentikasi pihak dan mitigasi serangan MITM [Diffie and Hellman, 1976, Katz and Lindell, 2020].

## 11.4 Distribusi Kunci Publik

Menggunakan direktori publik, sertifikat digital dalam PKI, atau *web of trust*. Validasi dan pencabutan sertifikat (CRL/OCSP) menjadi bagian penting [Stallings, 2016].

## 11.5 Usia Kunci dan Pengendalian Pemakaian

Kebijakan rotasi kunci, masa berlaku, cakupan penggunaan (key usage), dan penanganan kompromi kunci. Audit dan logging untuk *non-repudiation* dan forensik [Menezes et al., 1996].

## 11.6 Layanan Pihak Ketiga Terpercaya

CA, TSA (Time-Stamping Authority), dan KDC (Key Distribution Center) pada sistem tertentu. Keamanan keseluruhan bergantung pada keandalan dan tata kelola layanan ini.

## 11.7 Latihan

1. Bandingkan PKI berbasis hierarki CA dan *web of trust*.
2. Jelaskan mitigasi serangan MITM pada pertukaran kunci Diffie–Hellman.
3. Rancang kebijakan rotasi kunci untuk layanan web berskala menengah.

# Bab 12

# Fungsi Hash dan Kode Otentikasi Pesan

## 12.1 Tujuan Pembelajaran

Mahasiswa memahami fungsi hash kriptografis, MAC, dan konsep *unconditionally secure authentication code*.

## 12.2 Fungsi Hash

Hash kriptografis memetakan pesan ke digest berdimensi tetap dengan sifat tahan tabrakan, tahan pra-citra, dan tahan pra-citra kedua. Banyak skema dibangun di atas hash (tanda tangan, komitmen, integritas berkas) [Menezes et al., 1996].

## 12.3 Message Authentication Code (MAC)

MAC memberikan otentikasi dan integritas berbasis kunci rahasia bersama. Contoh konstruksi: HMAC yang menggabungkan fungsi hash dengan kunci rahasia dan memiliki analisis formal luas [Katz and Lindell, 2020].

## 12.4 Unconditionally Secure Authentication Code

Kode otentikasi bersyarat tak-terikat (unconditional) menjamin keamanan informasi-teoretik tanpa asumsi komputasional, biasanya memerlukan kunci sepanjang pesan/overhead lebih besar, dan cocok pada skenario khusus [Menezes et al., 1996].

## 12.5 Latihan

1. Jelaskan perbedaan jaminan keamanan MAC vs. tanda tangan digital.
2. Tunjukkan skema HMAC pada tingkat tinggi dan mengapa tahan terhadap tabrakan hash tertentu.
3. Berikan contoh skenario di mana kode autentikasi tak-terikat lebih tepat.

# Bab 13

# Kerberos, PGP, dan Sistem Pembayaran Elektronik

## 13.1 Tujuan Pembelajaran

Mahasiswa memahami peran Kerberos, PGP, dan gambaran sistem pembayaran elektronik universal.

## 13.2 Kerberos

Kerberos adalah protokol otentikasi jaringan berbasis tiket yang mengandalkan KDC (AS dan TGS). Prinsip: otentikasi mutual, tiket sementara (TGT), dan sesi kunci sementara untuk layanan [Kohl and Neuman, 1993, Stallings, 2016].

## 13.3 Pretty Good Privacy (PGP)

PGP menggabungkan kriptografi simetris dan asimetris: enkripsi pesan dengan kunci sesi simetris (mis. AES), lalu kunci sesi dienkripsi dengan kunci publik penerima; juga menyediakan tanda tangan dan manajemen kunci ala *web of trust* [Zimmermann, 1995, Stallings, 2016].

## 13.4 Sistem Pembayaran Elektronik

Gagasan sistem pembayaran elektronik universal mencakup aspek privasi, otentikasi, integritas, dan non-repudiation. Contoh komponen: token, tanda tangan, bukti tanpa pengungkapan penuh, serta infrastruktur sertifikat. Rancang bangun membutuhkan regulasi dan tata kelola tambahan.

## 13.5 Latihan

1. Jelaskan alur tiket Kerberos mulai dari AS hingga layanan akhir.
2. Uraikan bagaimana PGP menggabungkan kunci simetris dan asimetris.
3. Identifikasi tantangan keamanan dan regulasi pada sistem pembayaran elektronik berskala besar.

# Bab 14

# Analisis Sistem Kripto Sederhana

## 14.1 Tujuan Pembelajaran

Mahasiswa mampu melakukan analisis dasar terhadap sistem kripto sederhana dan mengidentifikasi kelemahannya.

## 14.2 Metodologi Analisis

Langkah-langkah umum: model ancaman, asumsi penyerang, enumerasi ruang kunci, analisis statistik (mis. frekuensi), dan serangan yang memanfaatkan struktur (linearitas, periode pendek, bias) [Stallings, 2016].

## 14.3 Contoh: Analisis Sandi Substitusi Tunggal

Sandi substitusi tunggal mempertahankan distribusi frekuensi huruf. Serangan analisis frekuensi, bigram/trigram, dan heuristik bahasa dapat memulihkan pemetaan kunci secara bertahap.

## 14.4 Contoh: Analisis RC4 Awal

Bias pada byte awal keystream RC4 memungkinkan kebocoran informasi kunci pada protokol tertentu jika *nonce* berulang, sehingga mitigasi dengan pembuangan byte awal tidak cukup pada banyak skenario modern [Mantin and Shamir, 2001].

## 14.5 Latihan

1. Lakukan analisis frekuensi pada pesan terenkripsi dengan substitusi tunggal untuk menebak sebagian kunci.
2. Identifikasi asumsi penyerang pada analisis yang Anda lakukan.
3. Usulkan perbaikan desain untuk menutup celah yang ditemukan.

# Bibliografi


Whitfield Diffie and Martin E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654, 1976.

Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman. *An Introduction to Mathematical Cryptography*. Springer, 2 edition, 2014.

Jonathan Katz and Yehuda Lindell. *Introduction to Modern Cryptography*. CRC Press, 3 edition, 2020.

John T. Kohl and B. Clifford Neuman. The kerberos network authentication service (v5). RFC 1510, 1993.

Itsik Mantin and Adi Shamir. The indistinguishability of the rc4 stream cipher. In *Proceedings of the International Workshop on Fast Software Encryption*, 2001.

Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 1996. URL https://cacr.uwaterloo.ca/hac/.

National Institute of Standards and Technology. Data encryption standard (des). FIPS 46-3, 1999. URL https://csrc.nist.rip/publications/fips/archive/fips46-3/fips46-3.pdf.

National Institute of Standards and Technology. Advanced encryption standard (aes). FIPS 197, 2001. URL https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf.

R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.

Phil Rogaway and Don Coppersmith. Seal: A high-speed stream cipher. *RSA Laboratories Bulletin*, 1994.

Kenneth H. Rosen. *Discrete Mathematics and Its Applications*. McGraw-Hill, 7 edition, 2012.

William Stallings. *Cryptography and Network Security: Principles and Practice*. Pearson, 7 edition, 2016.

Philip R. Zimmermann. Pretty good privacy (pgp), 1995. URL https://www.philzimmermann.com/EN/essays/WhyPGP.html.