# KRIPTOGRAFI II: PROTOKOL, PKI, TLS/SSL, PRAKTIK PENGGUNAAN AMAN

**Disusun oleh:**
JORDI HILMI FEBRIAN 2344390005

**S1 SISTEM INFORMASI**
**FAKULTAS TEKNIK**
**UNIVERSITAS PERSADA INDONESIA YAI**
**JAKARTA PUSAT**
**2025**

## KATA PENGHANTAR

Perkembangan teknologi informasi yang pesat menuntut adanya mekanisme perlindungan data dan komunikasi yang andal. Kriptografi menjadi salah satu fondasi utama dalam menjaga kerahasiaan, integritas, dan keaslian data pada berbagai sistem digital. Melalui makalah ini, penulis berupaya menjelaskan konsep dan penerapan kriptografi dari sisi protokol, infrastruktur kunci publik (Public Key Infrastructure/PKI), serta mekanisme keamanan yang digunakan pada TLS/SSL dalam konteks penggunaan yang aman dan efektif.

serta kritik dan saran yang bersifat membangun sangat penulis harapkan demi perbaikan di masa mendatang. Semoga makalah ini dapat memberikan manfaat bagi para pembaca, khususnya dalam memahami pentingnya penerapan kriptografi dalam keamanan sistem informasi modern.

# DAFTAR ISI

# BAB I PENDAHULUAN

## 1.1 Latar Belakang

Perkembangan teknologi informasi dalam dua dekade terakhir telah mengubah secara drastis cara manusia berinteraksi, bertransaksi, dan mengelola data. Transformasi digital melahirkan berbagai sistem informasi yang saling terhubung dan bergantung pada jaringan internet. Namun, di balik kemajuan ini, muncul pula risiko besar terhadap keamanan data. Serangan siber seperti *ransomware*, *phishing*, *data breach*, dan *man-in-the-middle attack* semakin sering terjadi dan menimbulkan kerugian finansial maupun reputasi bagi individu dan organisasi.

Dalam konteks inilah, kriptografi berperan sebagai lapisan pertahanan utama. Kriptografi tidak hanya berfungsi untuk menyembunyikan informasi agar tidak terbaca oleh pihak yang tidak berhak, tetapi juga memastikan keaslian identitas, keutuhan data, dan ketidakmungkinan manipulasi tanpa izin. Menurut William Stallings (2022), kriptografi merupakan jantung dari seluruh sistem keamanan jaringan modern. Tanpa kriptografi, sistem seperti perbankan online, e-commerce, atau bahkan komunikasi sehari-hari melalui aplikasi pesan instan tidak akan bisa menjamin keamanan dan privasi penggunanya.

Di era industri 4.0, kebutuhan akan sistem keamanan yang kuat tidak hanya menjadi tanggung jawab teknis departemen IT, tetapi juga menjadi bagian dari strategi bisnis perusahaan. ISO/IEC 27001:2022 bahkan menjadikan pengelolaan risiko keamanan informasi sebagai aspek manajerial yang harus diintegrasikan ke dalam seluruh aktivitas organisasi. Oleh karena itu, pemahaman terhadap protokol kriptografi, PKI, dan TLS/SSL sangat penting untuk memastikan keamanan data dan kepercayaan pengguna terhadap sistem digital.

Selain itu, penerapan kriptografi dalam komunikasi jaringan tidak bisa dipisahkan dari Public Key Infrastructure (PKI) dan Transport Layer Security (TLS/SSL). Keduanya menjadi dasar dari keamanan komunikasi di internet modern. TLS/SSL memungkinkan data dikirim secara aman antara klien dan server, sementara PKI memastikan bahwa identitas digital yang digunakan benar dan dapat dipercaya. Pemahaman terhadap kedua konsep ini akan menjadi kunci dalam membangun sistem yang aman, efisien, dan sesuai standar global.

## 1.2 Rumusan Masalah

Berdasarkan latar belakang tersebut, rumusan masalah dalam makalah ini adalah sebagai berikut:

1. Apa pengertian kriptografi modern dan bagaimana perannya dalam keamanan informasi?
2. Bagaimana prinsip kerja Public Key Infrastructure (PKI) dalam sistem keamanan jaringan?
3. Bagaimana mekanisme kerja protokol TLS/SSL dalam mengamankan komunikasi data?
4. Apa saja praktik terbaik yang dapat diterapkan dalam penggunaan kriptografi agar tetap aman dan efisien?

## 1.3 Tujuan Penulisan

Tujuan penulisan makalah ini adalah:

1. Menjelaskan secara rinci konsep dasar dan perkembangan kriptografi modern.
2. Menganalisis fungsi dan komponen PKI dalam mendukung keamanan digital.
3. Menguraikan cara kerja protokol TLS/SSL sebagai sistem keamanan komunikasi.
4. Menjelaskan praktik terbaik dalam implementasi kriptografi agar sesuai dengan standar keamanan global seperti ISO/IEC 27001 dan NIST CSF.

# BAB II KRIPTOGRAFI

## 2.1 Pengertian Kriptografi

Kriptografi berasal dari bahasa Yunani, yaitu *kryptos* (tersembunyi) dan *graphein* (menulis), yang berarti seni menulis secara tersembunyi. Dalam konteks keamanan informasi, kriptografi adalah ilmu yang mempelajari teknik untuk melindungi data melalui proses penyandian (enkripsi) sehingga hanya pihak yang berwenang yang dapat membacanya.

Menurut Stallings (2022), kriptografi modern tidak lagi terbatas pada penyandian pesan, melainkan telah berkembang menjadi sistem matematis yang kompleks, mencakup teori bilangan, teori informasi, dan algoritma komputasi. Hal ini menjadikan kriptografi sebagai komponen utama dalam keamanan siber dan komunikasi digital.

ISO/IEC 27001:2022 mendefinisikan keamanan informasi sebagai perlindungan terhadap kerahasiaan, integritas, dan ketersediaan informasi. Dalam konteks ini, kriptografi berperan besar dalam menjaga kerahasiaan (*confidentiality*) dan integritas (*integrity*) data melalui mekanisme enkripsi dan tanda tangan digital.

Selain itu, Ross Anderson (2020) dalam *Security Engineering* menegaskan bahwa kriptografi hanyalah satu bagian dari sistem keamanan yang lebih luas. Keamanan sejati hanya dapat dicapai apabila kriptografi dikombinasikan dengan manajemen risiko, pengendalian akses, dan kebijakan organisasi yang tepat.

## 2.2 Prinsip-Prinsip Kriptografi Modern

Kriptografi modern beroperasi berdasarkan empat prinsip utama, yaitu:

1. Kerahasiaan (Confidentiality) menjaga agar informasi tidak dapat diakses oleh pihak yang tidak berwenang.
2. Integritas (Integrity) memastikan bahwa data tidak mengalami perubahan tanpa izin selama proses penyimpanan atau transmisi.
3. Autentikasi (Authentication) memastikan identitas pihak yang berkomunikasi benar dan dapat dipercaya.
4. Non-Repudiation (Penolakan Non-Repudiatif) menjamin bahwa pengirim tidak dapat menyangkal telah mengirim pesan.

Menurut Stallings & Brown (2017), empat prinsip tersebut menjadi pilar utama bagi semua sistem keamanan modern, termasuk protokol TLS/SSL yang digunakan untuk melindungi data pengguna di internet.

Selain itu, ada dua jenis utama kriptografi yang digunakan dalam implementasi praktis, yaitu:

- Kriptografi Simetris, di mana kunci yang sama digunakan untuk enkripsi dan dekripsi. Algoritma yang populer antara lain AES (Advanced Encryption Standard).
- Kriptografi Asimetris, yang menggunakan dua kunci berbeda, yaitu *public key* dan *private key*. Contoh algoritma: RSA, ECC, dan Diffie-Hellman.

Perpaduan antara kedua jenis kriptografi ini banyak digunakan dalam protokol keamanan modern, di mana enkripsi asimetris digunakan untuk pertukaran kunci, sementara enkripsi simetris digunakan untuk komunikasi data karena lebih efisien secara komputasi.

# BAB III PEMBAHASAN DAN ANALISIS

## 3.1 Public Key Infrastructure (PKI)

Public Key Infrastructure (PKI) merupakan fondasi utama dalam sistem keamanan berbasis kriptografi modern. PKI berfungsi sebagai sistem manajemen yang memungkinkan distribusi, verifikasi, dan pencabutan kunci publik dengan aman. Melalui PKI, dua pihak yang tidak saling mengenal dapat saling mempercayai identitas digital masing-masing tanpa perlu bertatap muka. Hal ini menjadi dasar dari keamanan komunikasi modern, terutama pada transaksi daring, sistem perbankan, dan layanan berbasis sertifikat digital seperti tanda tangan elektronik.

Secara umum, PKI terdiri dari beberapa komponen penting, yaitu:

1. Certificate Authority (CA) lembaga yang berwenang menerbitkan dan memverifikasi sertifikat digital. CA bertugas memastikan bahwa identitas yang tercantum dalam sertifikat benar-benar valid.
2. Registration Authority (RA) bertugas memverifikasi identitas pengguna sebelum CA menerbitkan sertifikat.
3. Certificate Repository tempat penyimpanan sertifikat digital yang telah diterbitkan agar dapat diakses publik.
4. Certificate Revocation List (CRL) daftar sertifikat yang sudah tidak berlaku atau dicabut karena alasan keamanan.

Menurut NIST SP 800-53 Rev.5 (2020), PKI menjadi bagian dari kontrol keamanan yang berfungsi menjaga integritas dan kepercayaan dalam komunikasi digital. Tanpa mekanisme PKI yang andal, tidak ada jaminan bahwa kunci publik yang digunakan benar-benar milik entitas yang sah.
Sebagai contoh, ketika seseorang mengunjungi situs web yang menggunakan HTTPS, browser akan melakukan verifikasi terhadap sertifikat digital situs tersebut. Proses ini memastikan bahwa koneksi yang dibuat memang menuju server asli, bukan ke pihak penyerang yang mencoba melakukan *spoofing*. Dengan demikian, PKI menjadi lapisan pertama dalam menciptakan kepercayaan digital (*digital trust*).

Selain itu, PKI juga digunakan dalam berbagai implementasi lain seperti sistem tanda tangan digital, enkripsi email menggunakan S/MIME, serta otentikasi perangkat dalam Internet of Things (IoT). Dalam konteks korporasi, PKI bahkan sering digunakan untuk mengamankan jaringan internal melalui sistem *Virtual Private Network (VPN)* dan otentikasi dua faktor berbasis sertifikat.

Namun, keberhasilan PKI tidak hanya bergantung pada kekuatan algoritma kriptografi, tetapi juga pada tata kelola sertifikat yang baik. Ross Anderson (2020) menekankan bahwa kelemahan dalam manajemen sertifikat misalnya penerbitan sertifikat palsu atau penggunaan CA yang tidak terpercaya dapat menyebabkan kebocoran data berskala besar. Oleh sebab itu, manajemen kunci dan sertifikat harus diatur secara ketat sesuai dengan kebijakan keamanan organisasi.

## 3.2 Protokol Transport Layer Security (TLS/SSL)

Transport Layer Security (TLS) merupakan penerus dari Secure Socket Layer (SSL) yang dikembangkan oleh Netscape pada tahun 1990-an. Protokol ini dirancang untuk mengamankan komunikasi antara klien dan server melalui jaringan publik seperti internet. TLS menjamin tiga aspek utama dalam keamanan komunikasi: kerahasiaan, integritas, dan autentikasi.

Menurut *NIST Cybersecurity Framework (CSF) 2.0* (2024), TLS termasuk dalam kontrol teknis pada fungsi “Protect”. Fungsi ini menitikberatkan pada perlindungan data selama proses transmisi untuk mencegah serangan seperti *eavesdropping* atau *man-in-the-middle attack*. Implementasi TLS

yang benar terbukti mampu mencegah pihak ketiga mengakses data sensitif seperti kredensial login, nomor kartu kredit, atau pesan pribadi.

Proses kerja TLS dimulai dari apa yang disebut sebagai TLS Handshake Protocol. Pada tahap ini, klien dan server saling berkomunikasi untuk menentukan algoritma enkripsi, menukar sertifikat digital, dan menghasilkan *session key* yang akan digunakan selama sesi komunikasi. Tahapan ini melibatkan mekanisme kriptografi asimetris untuk menjamin keaslian identitas, serta kriptografi simetris untuk efisiensi pertukaran data setelah koneksi aman terbentuk.
Secara garis besar, proses handshake TLS terdiri dari langkah-langkah berikut:

1. Client Hello: Klien mengirimkan permintaan ke server dengan menyertakan daftar versi TLS dan algoritma enkripsi yang didukung.
2. Server Hello: Server membalas dengan memilih versi TLS dan algoritma yang sesuai, serta mengirimkan sertifikat digitalnya.
3. Certificate Verification: Klien memverifikasi sertifikat yang diterima dengan memeriksa apakah sertifikat tersebut ditandatangani oleh CA terpercaya.
4. Key Exchange: Setelah verifikasi berhasil, klien dan server menukar kunci sementara untuk membentuk *session key*.
5. Finished Messages: Kedua pihak saling mengirim pesan tanda selesai dan komunikasi aman dimulai.

TLS 1.3, memperkenalkan sejumlah peningkatan keamanan dan performa dibandingkan versi sebelumnya. Salah satu fitur utamanya adalah penghapusan algoritma yang sudah tidak aman, seperti RSA key exchange dan SHA-1, serta penerapan *Perfect Forward Secrecy (PFS)* untuk memastikan bahwa jika suatu kunci jangka panjang bocor, data yang sudah terenkripsi tetap tidak bisa dibuka.

Menurut OWASP (2021), salah satu kesalahan umum yang sering ditemukan pada implementasi TLS adalah penggunaan konfigurasi lama yang sudah tidak aman, seperti TLS 1.0 atau cipher suite yang lemah. Karena itu, OWASP merekomendasikan penggunaan TLS 1.3 atau minimal TLS 1.2, dengan kombinasi algoritma AES-GCM dan ECDHE yang mendukung keamanan serta kinerja optimal.

## 3.3 Analisis Kelemahan dan Ancaman dalam Implementasi Kriptografi

Meskipun kriptografi memberikan perlindungan yang sangat kuat, bukan berarti sistem ini bebas dari risiko. Dalam praktiknya, berbagai kelemahan dan kesalahan konfigurasi seringkali dimanfaatkan oleh penyerang untuk membobol sistem yang seharusnya aman.

Salah satu kelemahan paling umum adalah kesalahan dalam manajemen kunci (key management). Banyak organisasi gagal melindungi kunci privat dengan baik, misalnya dengan menyimpannya dalam file tanpa enkripsi atau menggunakan kata sandi yang lemah. Hal ini dapat menyebabkan kebocoran data yang serius. Menurut ISO/IEC 27001:2022, kontrol terhadap penyimpanan dan distribusi kunci harus dilakukan secara ketat untuk mencegah penyalahgunaan.

Selain itu, terdapat pula ancaman yang bersifat teknis seperti serangan downgrade dan certificate spoofing. Serangan downgrade terjadi ketika penyerang memaksa klien dan server untuk menggunakan versi TLS yang lebih lama dan rentan. Sementara itu, certificate spoofing adalah upaya penyerang untuk memalsukan sertifikat digital agar tampak sah di mata pengguna.

Ross Anderson (2020) menekankan bahwa keamanan suatu sistem tidak hanya tergantung pada algoritma kriptografi yang kuat, tetapi juga pada bagaimana sistem tersebut diimplementasikan

dan dikelola. Dalam banyak kasus, serangan berhasil bukan karena kelemahan algoritma, melainkan karena kelalaian dalam konfigurasi atau kegagalan dalam memperbarui sistem keamanan secara rutin.

## 3.4 Hubungan Kriptografi dengan Standar Keamanan Informasi

Standar internasional seperti ISO/IEC 27001:2022, NIST SP 800-53 Rev.5, dan NIST Cybersecurity Framework 2.0 memberikan panduan komprehensif tentang bagaimana organisasi seharusnya menerapkan kontrol keamanan berbasis kriptografi.

ISO/IEC 27001 menempatkan kontrol kriptografi dalam kategori *Annex A.10*, yang berfokus pada perlindungan kerahasiaan dan integritas informasi melalui penggunaan algoritma yang sesuai. Sementara itu, NIST SP 800-53 memberikan panduan lebih teknis tentang bagaimana mengimplementasikan kontrol tersebut, termasuk dalam pengelolaan kunci, validasi sertifikat, dan proses otentikasi.

NIST CSF 2.0 (2024) membagi keamanan siber ke dalam lima fungsi utama: *Identify, Protect, Detect, Respond, dan Recover.* Dalam fungsi *Protect*, kriptografi menjadi komponen penting yang membantu organisasi menjaga data dari penyadapan dan modifikasi. Sedangkan OWASP menyediakan panduan teknis khusus untuk keamanan aplikasi web, termasuk penggunaan TLS, penyimpanan kunci, dan pengamanan sesi komunikasi.

Dengan mengacu pada standar-standar tersebut, organisasi dapat memastikan bahwa penerapan kriptografi tidak hanya aman secara teknis, tetapi juga memenuhi kepatuhan terhadap regulasi seperti GDPR (General Data Protection Regulation) dan peraturan lokal tentang perlindungan data pribadi.

# BAB IV TEKNOLOGI TLS/SSL DAN PRAKTIK PENGGUNAAN AMAN

## 4.1 Pengertian TLS/SSL

Transport Layer Security (TLS) dan pendahulunya, Secure Sockets Layer (SSL), merupakan protokol yang dirancang untuk menyediakan komunikasi aman melalui jaringan komputer, terutama internet. Keduanya bekerja pada lapisan transport (transport layer) dan berfungsi untuk mengenkripsi data yang dikirimkan antara dua sistem, seperti antara peramban web (browser) dengan server.

TLS pada dasarnya menggantikan SSL karena versi SSL yang lebih lama (SSL 2.0 dan SSL 3.0) telah diketahui memiliki banyak kelemahan keamanan. Versi TLS terbaru, yakni TLS 1.3, menghadirkan peningkatan besar dalam efisiensi serta penguatan enkripsi. TLS 1.3 menghapus algoritma lemah seperti SHA-1 dan RC4 serta mengurangi waktu yang diperlukan dalam proses handshake.

Menurut NIST Cybersecurity Framework (CSF 2.0, 2024), TLS dikategorikan sebagai salah satu kontrol utama dalam domain *Protect Function*, khususnya dalam kategori *Data Security (PR.DS)*, karena fungsinya untuk menjaga kerahasiaan data selama transmisi.

Fungsi utama TLS/SSL mencakup:

1. Kerahasiaan (Confidentiality)  data yang dikirim dienkripsi, sehingga pihak ketiga tidak dapat membacanya.
2. Integritas (Integrity)  pesan dilindungi dari perubahan yang tidak sah melalui *Message Authentication Code (MAC)*.
3. Otentikasi (Authentication)  memastikan bahwa pihak yang berkomunikasi adalah entitas yang sah melalui sertifikat digital.
4. Non-repudiasi (Non-repudiation)  menjamin bahwa pihak pengirim tidak dapat menyangkal telah mengirimkan pesan tertentu.

TLS/SSL telah menjadi standar de facto dalam pengamanan komunikasi web modern, ditandai dengan penggunaan protokol HTTPS pada alamat situs web. HTTPS tidak hanya menambah lapisan keamanan, tetapi juga meningkatkan kepercayaan pengguna terhadap situs yang dikunjungi.

## 4.2 Mekanisme Kerja TLS/SSL

TLS beroperasi melalui dua lapisan utama: Handshake Protocol dan Record Protocol.

- Handshake Protocol bertanggung jawab untuk membangun parameter keamanan antara klien dan server, termasuk autentikasi, negosiasi algoritma enkripsi, serta pembuatan *session key*.
- Record Protocol memastikan bahwa setiap data yang dikirim melalui sesi tersebut dienkripsi dan dijaga integritasnya.

Proses handshake dalam TLS melibatkan langkah-langkah sebagai berikut:

1. Client Hello:
   Klien mengirim pesan “Hello” ke server, berisi daftar algoritma enkripsi (cipher suite) yang didukung dan versi TLS yang diinginkan.
2. Server Hello:
   Server merespons dengan memilih cipher suite yang sesuai dan mengirimkan sertifikat digital berisi kunci publiknya. Sertifikat ini biasanya diterbitkan oleh Certificate Authority (CA) yang terpercaya.
3. Key Exchange:
   Klien dan server melakukan pertukaran kunci melalui algoritma seperti RSA atau Diffie-Hellman Ephemeral (DHE) untuk menghasilkan *session key* yang akan digunakan dalam komunikasi selanjutnya.

4. Handshake Completion: Setelah proses pertukaran kunci selesai, kedua pihak mengirimkan pesan Finished untuk memastikan bahwa sesi telah berhasil dibangun dan komunikasi aman siap dimulai.

Setelah handshake selesai, seluruh komunikasi antara klien dan server akan dienkripsi menggunakan algoritma simetris (misalnya AES-256) dengan *session key* yang telah disepakati.

William Stallings (2022) menegaskan bahwa keberhasilan TLS tidak hanya ditentukan oleh algoritma kriptografinya, tetapi juga oleh konfigurasi implementasi yang benar. Kesalahan kecil seperti penggunaan sertifikat kadaluwarsa, cipher suite lemah, atau konfigurasi port yang terbuka dapat menurunkan efektivitas proteksi TLS.

## 4.3 Evolusi dan Versi TLS

TLS mengalami beberapa versi penting:

- TLS 1.0 (1999): versi awal, sudah dianggap tidak aman.
- TLS 1.1 (2006): memperbaiki kelemahan pada enkripsi blok.
- TLS 1.2 (2008): mendukung algoritma enkripsi yang lebih kuat seperti AES dan SHA-256.
- TLS 1.3 (2018): versi terbaru yang menyederhanakan handshake dan memperkuat keamanan.

Versi TLS 1.3 menghapus banyak komponen lama yang dianggap rawan, termasuk dukungan untuk cipher lemah dan penghapusan *renegotiation*. Dengan hanya satu round-trip handshake, TLS 1.3 mempercepat koneksi dan meningkatkan privasi karena semua pesan handshake dienkripsi setelah tahap awal.

## 4.4 Praktik Penggunaan Aman TLS/SSL

Agar penerapan TLS/SSL benar-benar aman, organisasi dan pengembang harus memperhatikan praktik-praktik berikut:

1. Gunakan Versi Terbaru (TLS 1.3 atau Minimal 1.2) Versi lama seperti SSL dan TLS 1.0 1.1 tidak lagi direkomendasikan karena memiliki celah keamanan.
2. Hindari Cipher Lemah Jangan gunakan algoritma seperti RC4, DES, atau MD5 karena sudah terbukti mudah ditembus. Gunakan AES-GCM, ChaCha20-Poly1305, atau SHA-256.
3. Gunakan Sertifikat dari CA Terpercaya Pastikan sertifikat diterbitkan oleh otoritas tepercaya seperti DigiCert, GlobalSign, atau Let's Encrypt.
4. Terapkan HSTS (HTTP Strict Transport Security) Menginstruksikan browser agar selalu menggunakan koneksi HTTPS dan mencegah downgrade ke HTTP tidak aman.
5. Pantau Keamanan Secara Berkala Gunakan alat seperti Qualys SSL Labs atau Mozilla Observatory untuk menguji konfigurasi TLS dan mendeteksi potensi celah.
6. Implementasikan Perfect Forward Secrecy (PFS) Dengan PFS, kunci sesi yang bocor di masa depan tidak dapat digunakan untuk mendekripsi komunikasi masa lalu.

Menurut OWASP (2021), sebagian besar insiden keamanan web terjadi bukan karena kelemahan algoritma TLS, tetapi karena kesalahan konfigurasi (*security misconfiguration*). Oleh karena itu, audit berkala menjadi bagian penting dalam menjaga keamanan implementasi TLS.

## 4.5 Tantangan dan Serangan terhadap TLS/SSL

Meskipun TLS sangat kuat, masih ada sejumlah serangan yang menargetkan kelemahan implementasi:

- Man-in-the-Middle (MITM): penyerang memotong komunikasi antara klien dan server.
- TLS Downgrade Attack: pengguna dipaksa untuk menggunakan versi TLS yang lebih lemah.
- Heartbleed Bug (OpenSSL): kebocoran data memori akibat implementasi yang salah.
- BEAST dan POODLE Attack: eksploitasi terhadap cipher lama seperti CBC dan SSLv3.

Solusinya adalah menjaga perangkat lunak tetap diperbarui, menggunakan pustaka keamanan yang terpercaya, serta memantau sertifikat secara real-time melalui OCSP.

# BAB V STUDI KASUS DAN IMPLEMENTASI KRIPTOGRAFI

## 5.1 Studi Kasus: Implementasi TLS di Perbankan Digital

Sektor perbankan merupakan salah satu pengguna utama teknologi TLS karena sifat transaksinya yang sangat sensitif. Dalam sistem perbankan daring, TLS digunakan untuk melindungi komunikasi antara server bank dan aplikasi pengguna, termasuk pada saat login, transfer dana, dan permintaan saldo.

Sebagai contoh, bank-bank besar seperti BCA dan Mandiri telah menerapkan TLS 1.3 pada portal dan aplikasi mobile mereka. Setiap sesi komunikasi dimulai dengan verifikasi sertifikat digital yang diterbitkan oleh CA terpercaya. Selain itu, untuk meningkatkan keamanan, digunakan juga mutual authentication, di mana klien (aplikasi pengguna) memiliki sertifikat tersendiri untuk membuktikan identitasnya kepada server bank. Ini mencegah serangan phishing atau peniruan situs.

Berdasarkan pedoman NIST SP 800-53 (Rev.5), mekanisme seperti TLS harus dikombinasikan dengan sistem deteksi intrusi, enkripsi penyimpanan, dan autentikasi multifaktor untuk menghasilkan perlindungan menyeluruh.

## 5.2 Integrasi PKI dan Manajemen Sertifikat

Dalam perusahaan besar, penerapan Public Key Infrastructure (PKI) menjadi kunci dalam manajemen sertifikat digital. PKI tidak hanya digunakan untuk TLS, tetapi juga untuk autentikasi perangkat, tanda tangan digital, serta enkripsi email korporat.

PKI modern biasanya diintegrasikan dengan sistem direktori seperti Active Directory Certificate Services (AD CS) yang memungkinkan penerbitan sertifikat secara otomatis kepada pengguna dan perangkat yang telah terdaftar. Selain itu, sistem PKI juga menerapkan Online Certificate Status Protocol (OCSP) untuk memverifikasi status sertifikat secara real-time, menggantikan metode tradisional Certificate Revocation List (CRL) yang kurang efisien.

Ross Anderson (2020) menjelaskan bahwa keberhasilan PKI bergantung pada tingkat kepercayaan terhadap CA. Jika CA mengalami kompromi, seluruh ekosistem keamanan bisa terganggu. Oleh karena itu, praktik certificate pinning sering digunakan untuk membatasi sertifikat yang dapat dipercaya oleh aplikasi tertentu.

## 5.3 Implementasi Kriptografi di Aplikasi Web dan Mobile

Selain perbankan, kriptografi juga banyak diterapkan dalam platform e-commerce, media sosial, dan layanan pesan instan. Contohnya, WhatsApp dan Signal menggunakan end-to-end encryption (E2EE) yang berbasis pada Double Ratchet Algorithm dan Curve25519, memastikan hanya pengirim dan penerima yang dapat membaca pesan.

Sementara itu, situs e-commerce seperti Tokopedia dan Shopee mengandalkan TLS 1.3 untuk transaksi aman dan mengintegrasikannya dengan HSTS serta Content Security Policy (CSP) untuk mencegah injeksi skrip berbahaya.

## 5.4 Tantangan Keamanan Kriptografi Modern

Meskipun teknologi kriptografi terus berkembang, ancaman juga ikut berevolusi. Tantangan yang saat ini dihadapi antara lain:

1. Serangan Kuantum (Quantum Threat) algoritma kuantum seperti Shor’s Algorithm berpotensi memecahkan RSA dan ECC.

2. Kelemahan Implementasi (Implementation Flaw) kesalahan coding dapat membuka celah meskipun algoritma teorinya aman.
3. Manajemen Kunci yang Kompleks kesalahan dalam penyimpanan atau rotasi kunci dapat menyebabkan kebocoran data.

Sebagai solusi, para peneliti kini mengembangkan Post-Quantum Cryptography (PQC) yang tahan terhadap komputasi kuantum. Standar ini tengah disusun oleh NIST PQC Project, yang diharapkan menjadi masa depan keamanan kriptografi global.

## 5.5 Strategi Peningkatan Keamanan Kriptografi

Beberapa langkah strategis yang disarankan oleh ISO/IEC 27001:2022 dalam konteks peningkatan keamanan kriptografi meliputi:

- Audit Kriptografi Berkala: mengevaluasi efektivitas algoritma dan sertifikat yang digunakan.
- Pendidikan dan Pelatihan SDM: meningkatkan kesadaran keamanan dan kemampuan teknis staf TI.
- Automasi Manajemen Sertifikat: menggunakan sistem berbasis API untuk rotasi sertifikat otomatis.
- Integrasi Zero Trust Architecture (ZTA): memastikan setiap entitas diverifikasi sebelum mengakses sumber daya, meskipun berasal dari jaringan internal.

# BAB VI IMPLEMENTASI DAN STUDI KASUS LANJUT KRIPTOGRAFI MODERN

## 6.1 Implementasi Kriptografi di Dunia Nyata

Kriptografi telah menjadi pondasi utama dalam seluruh aktivitas digital modern. Setiap interaksi yang terjadi di dunia maya, baik berupa transaksi perbankan, komunikasi daring, maupun proses autentikasi, menggunakan sistem kriptografi di dalamnya. Dalam konteks keamanan informasi, kriptografi berperan penting untuk menjaga tiga aspek mendasar yaitu *Confidentiality*, *Integrity*, dan *Availability* (CIA Triad). Melalui algoritma matematis yang kompleks, kriptografi memastikan bahwa data hanya dapat dibaca oleh pihak yang berwenang, tidak diubah tanpa izin, dan tetap tersedia ketika dibutuhkan.

Di sektor perbankan digital, kriptografi simetris seperti AES (Advanced Encryption Standard) digunakan untuk melindungi data transaksi nasabah yang tersimpan dalam sistem, sementara algoritma asimetris seperti RSA dan Elliptic Curve Cryptography (ECC) digunakan dalam proses pertukaran kunci aman antara nasabah dan server bank. Selain itu, sistem pembayaran digital seperti QRIS dan e-wallet (contohnya DANA, OVO, dan GoPay) juga menerapkan protokol TLS/SSL guna menjamin keamanan komunikasi antara aplikasi pengguna dan server pusat.

Dalam bidang pemerintahan, kriptografi digunakan dalam sistem tanda tangan digital dan sertifikat elektronik untuk memastikan keaslian dokumen administrasi publik. Teknologi ini didasarkan pada konsep Public Key Infrastructure (PKI) yang memungkinkan identitas seseorang diverifikasi melalui sertifikat digital yang diterbitkan oleh otoritas terpercaya (*Certificate Authority*). Sementara dalam sektor kesehatan, sistem informasi rumah sakit (SIRH) memanfaatkan kriptografi untuk melindungi rekam medis elektronik pasien agar tidak disalahgunakan oleh pihak tidak bertanggung jawab.

Menurut ISO/IEC 27001:2022, penerapan kontrol kriptografi menjadi bagian dari kebijakan keamanan informasi organisasi. Standar ini menekankan bahwa setiap sistem yang mengelola data sensitif wajib memiliki mekanisme enkripsi, rotasi kunci, serta prosedur pencabutan kunci yang terdokumentasi dengan baik.

## 6.2 Penerapan Kriptografi dalam Infrastruktur dan Dunia Industri

Implementasi kriptografi dalam dunia industri dan infrastruktur kritikal bersifat sangat penting karena sistem-sistem ini seringkali menjadi target utama serangan siber. Dalam sistem Industrial Control System (ICS) dan Supervisory Control and Data Acquisition (SCADA) yang digunakan di pabrik, jaringan energi, maupun sistem transportasi, kriptografi digunakan untuk menjamin keaslian dan integritas komunikasi antar perangkat.

Sebagai contoh, dalam sistem kelistrikan nasional, komunikasi antara pusat kendali dan unit distribusi dilindungi dengan enkripsi AES 256-bit serta sertifikat digital berbasis PKI untuk memastikan bahwa hanya perangkat yang sah yang dapat mengirim dan menerima perintah. Hal ini mencegah serangan manipulasi sinyal (command injection) atau gangguan operasional akibat serangan dari luar jaringan.

Dalam konteks industri manufaktur, banyak perusahaan kini menerapkan sistem IoT Industrial (IIoT) yang memungkinkan mesin-mesin berkomunikasi secara otomatis. Penerapan kriptografi pada IIoT menggunakan algoritma ringan seperti ChaCha20 atau Lightweight AES (LAES) untuk menjaga performa perangkat dengan sumber daya terbatas.

Penelitian oleh Ross Anderson (2020) menunjukkan bahwa lebih dari 70% serangan pada sistem industri disebabkan oleh lemahnya implementasi keamanan pada level perangkat dan protokol komunikasi. Dengan demikian, penerapan kriptografi secara menyeluruh di setiap lapisan — mulai dari

sensor, jaringan, hingga server pusat merupakan kebutuhan mutlak bagi keberlangsungan operasional industri modern.

## 6.3 Studi Kasus: Implementasi TLS/SSL pada Layanan Cloud

Perusahaan penyedia layanan cloud seperti Google Cloud, Amazon Web Services (AWS), dan Microsoft Azure merupakan contoh nyata penerapan kriptografi berskala global. Mereka menggunakan TLS versi 1.3, yang menawarkan efisiensi lebih tinggi dengan proses *handshake* lebih cepat dan penghapusan algoritma rentan seperti RC4 dan SHA-1. TLS 1.3 juga mendukung fitur Perfect Forward Secrecy (PFS), yang menjamin bahwa data lama tidak dapat didekripsi bahkan jika kunci utama berhasil diretas.

Selain itu, layanan cloud besar menerapkan Certificate Transparency (CT) — sebuah sistem log publik yang memungkinkan masyarakat memverifikasi penerbitan sertifikat digital untuk mencegah penyalahgunaan atau penerbitan ilegal oleh otoritas sertifikat. Pendekatan ini memperkuat kepercayaan digital dan memastikan bahwa setiap komunikasi antara pengguna dan server cloud berlangsung dalam lingkungan terenkripsi yang tervalidasi.

# BAB VII TANTANGAN DAN PERKEMBANGAN TEKNOLOGI KRIPTOGRAFI

## 7.1 Tantangan dalam Penerapan Kriptografi

Meskipun teknologi kriptografi terus berkembang, terdapat beberapa tantangan serius dalam penerapannya di dunia nyata:

1. Ancaman Komputasi Kuantum: Komputer kuantum yang dikembangkan oleh perusahaan seperti IBM dan Google berpotensi mengancam sistem kriptografi tradisional. Dengan algoritma Shor, komputer kuantum dapat memecahkan kunci RSA atau ECC dalam waktu yang jauh lebih singkat dibanding komputer klasik. Hal ini membuat para peneliti mengembangkan algoritma baru yang tahan terhadap serangan kuantum.
2. Kesalahan Implementasi dan Manajemen Kunci: Banyak kebocoran data bukan disebabkan oleh lemahnya algoritma, melainkan kesalahan dalam implementasi dan penyimpanan kunci. Misalnya, penyimpanan kunci privat di lokasi tidak terenkripsi atau penggunaan kembali kunci lama yang telah kadaluarsa.
3. Masalah Kepercayaan terhadap Certificate Authority (CA): Ketika sebuah CA diretas atau menyalahgunakan kewenangannya, seluruh rantai kepercayaan digital dapat rusak. Contohnya, kasus kebocoran sertifikat pada Symantec (2017) menyebabkan Google dan Mozilla mencabut kepercayaan terhadap sertifikat yang diterbitkan CA tersebut.
4. Kurangnya Kesadaran dan Edukasi Pengguna: Pengguna akhir sering menjadi titik terlemah dalam rantai keamanan. Misalnya, menggunakan kata sandi yang lemah, tidak memperhatikan validitas sertifikat HTTPS, atau mengabaikan peringatan keamanan browser.

## 7.2 Arah Perkembangan Kriptografi Modern

Perkembangan teknologi kriptografi modern diarahkan untuk menghadapi ancaman baru serta meningkatkan efisiensi dan keandalan sistem. Beberapa tren utama yang berkembang saat ini adalah:

- Post-Quantum Cryptography (PQC): NIST sedang menstandarkan algoritma baru seperti CRYSTALS-Kyber untuk enkripsi dan Dilithium untuk tanda tangan digital yang tahan terhadap komputer kuantum.
- Zero Trust Architecture (ZTA): Model keamanan yang tidak lagi menganggap jaringan internal aman. Setiap permintaan akses, baik dari dalam maupun luar jaringan, harus diverifikasi melalui autentikasi dan enkripsi yang kuat.
- Blockchain Security: Blockchain mengandalkan fungsi hash dan tanda tangan digital untuk memastikan integritas data tanpa perlu otoritas pusat. Kriptografi menjadi inti dari sistem ini, mulai dari verifikasi transaksi hingga pembentukan blok baru.
- Homomorphic Encryption: Teknologi baru ini memungkinkan data diproses dalam keadaan terenkripsi tanpa perlu didekripsi terlebih dahulu, sangat berguna untuk keamanan cloud dan privasi data pengguna.

## 7.3 Peran Standar Internasional dalam Pengembangan Kriptografi

Lembaga seperti ISO, NIST, dan OWASP memiliki peran penting dalam pembentukan standar keamanan kriptografi global:

- ISO/IEC 27001:2022: Menetapkan pedoman sistem manajemen keamanan informasi (ISMS).
- NIST SP 800-53 Rev.5: Menyediakan daftar kontrol keamanan dan privasi bagi lembaga dan organisasi.

- OWASP Top 10 (2021): Mengidentifikasi sepuluh risiko utama keamanan aplikasi web yang sering dieksploitasi.

Standar-standar ini membantu organisasi untuk merancang sistem keamanan yang konsisten, dapat diaudit, dan memenuhi regulasi internasional.

# BAB VIII INOVASI DAN MASA DEPAN KRIPTOGRAFI DIGITAL

## 8.1 Evolusi Teknologi Kriptografi

Kriptografi modern terus berevolusi dari sistem manual menjadi algoritma matematis kompleks yang mendukung hampir seluruh teknologi informasi. Saat ini, inovasi seperti Attribute-Based Encryption (ABE) memungkinkan kontrol akses dinamis berdasarkan atribut pengguna, seperti jabatan atau lokasi. Selain itu, Quantum Key Distribution (QKD) juga sedang dikembangkan, yang menggunakan prinsip mekanika kuantum untuk mendistribusikan kunci dengan keamanan mutlak jika kunci disadap, sistem akan otomatis mendeteksi adanya gangguan.

## 8.2 Integrasi Kriptografi dan Kecerdasan Buatan (AI)

Integrasi antara kriptografi dan AI menjadi salah satu bidang penelitian paling aktif. AI dapat membantu mendeteksi pola serangan terhadap sistem kriptografi dengan menganalisis anomali data. Namun, di sisi lain, AI juga menimbulkan risiko baru karena dapat digunakan untuk meretas sistem dengan kecepatan dan kecerdasan adaptif yang tinggi. Oleh karena itu, muncul konsep AI-driven Encryption System, di mana algoritma enkripsi dapat menyesuaikan diri berdasarkan pola ancaman yang terdeteksi secara real-time.

## 8.3 Kriptografi pada Internet of Things (IoT) dan Edge Computing

Perangkat IoT menghadirkan tantangan besar dalam penerapan kriptografi karena keterbatasan sumber daya (daya, memori, dan prosesor). Untuk itu, dikembangkan algoritma ringan seperti Lightweight AES, ChaCha20-Poly1305, dan protokol DTLS (Datagram TLS) untuk komunikasi aman antarperangkat IoT. Dalam Edge Computing, data diproses lebih dekat ke sumbernya untuk mengurangi latensi. Penerapan enkripsi di level edge memastikan bahwa data tetap terlindungi bahkan sebelum mencapai pusat data utama (data center).

# DAFTAR PUSTAKA


ISO/IEC 27001:2022. *Information Security Management Systems — Requirements.* International Organization for Standardization (ISO), Geneva, 2022.

NIST Special Publication 800-53 Revision 5. *Security and Privacy Controls for Information Systems and Organizations.* National Institute of Standards and Technology (NIST), Gaithersburg, 2020.

NIST Cybersecurity Framework (CSF) 2.0. *Framework for Improving Critical Infrastructure Cybersecurity.* National Institute of Standards and Technology (NIST), February 26, 2024.

OWASP. *OWASP Top 10: The Ten Most Critical Web Application Security Risks.* Open Web Application Security Project (OWASP), 2021.

William Stallings. *Cryptography and Network Security: Principles and Practice.* 8th Edition. Pearson Education, 2022.

Ross Anderson. *Security Engineering: A Guide to Building Dependable Distributed Systems.* 3rd Edition. Wiley, 2020.

William Stallings & Lawrie Brown. *Computer Security: Principles and Practice.* 4th Edition. Pearson, 2017.

Bruce Schneier. *Applied Cryptography: Protocols, Algorithms, and Source Code in C.* 20th Anniversary Edition. Wiley, 2015.

Andrew S. Tanenbaum & David J. Wetherall. *Computer Networks.* 6th Edition. Pearson, 2021.

James F. Kurose & Keith W. Ross. *Computer Networking: A Top-Down Approach.* 8th Edition. Pearson, 2021.

NIST Online Documentation. *NIST Cybersecurity Framework Implementation Guides.* https://www.nist.gov/cyberframework pada 10 Oktober 2025.

OWASP Project Documentation. *OWASP Secure Coding Practices & Testing Guide.* https://owasp.org pada 10 Oktober 2025.

Medium Security Publications. *Top Cybersecurity and Cryptography Books 2023–2024.* Medium, 2024.