LAPORAN KRIPTOGRAFI TUGAS BESAR 3

Tugas Ini Dibuat Untuk Memenuhi Salah Satu Tugas Pada Mata Kuliah Kriptografi

Dosen Pengampu : Kodrat Mahatma S.T,.M.Kom.

Universitas Teknologi Digital

Oleh :

Mochammad Rival Sopyan

20123006

PROGRAM STUDI S1 INFORMATIKA

UNIVERSITAS TEKNOLOGI DIGITAL

TAHUN AJARAN 2025/2026

ANALISIS KELEMAHAN

DATA ENCRYPTION STANDARD (DES)

1. Pendahuluan

Data Encryption Standard (DES) adalah peristiwa penting dalam sejarah kriptografi kontemporer. IBM membuat algoritma ini pada awal tahun 1970-an. NIST, di Amerika Serikat, menetapkannya sebagai standar enkripsi. Pada saat itu, DES menjadi standar enkripsi blok pertama yang digunakan secara global oleh pemerintah dan perusahaan.

Namun, kemajuan pesat dalam teknologi komputer berdampak besar pada keamanan DES. Algoritma yang dulunya dianggap cukup aman tidak lagi mampu melindungi data dari ancaman saat ini. Tujuan dari esai ini adalah untuk menganalisis kekurangan dasar DES yang akhirnya menyebabkan algoritma ini ditinggalkan dan digantikan oleh standar enkripsi yang lebih baik.

2. Tujuan DES

DES adalah algoritma enkripsi simetris yang mengenkripsi data dalam blok berukuran tetap dengan menggunakan struktur Feistel yang terdiri dari enam belas putaran. Dalam setiap putaran, algoritma ini melakukan kombinasi proses permutasi dan substitusi pada data. Proses DES biasanya terdiri dari permutasi awal, pemrosesan data melalui sejumlah S-Boxes dan P-Boxes, dan permutasi akhir.

Tujuan dari proses ini adalah untuk menyamarkan hubungan antara teks asli dan teks terenkripsi, sehingga data tidak dapat dipahami tanpa kunci yang tepat. Untuk manajemen kunci, DES menggunakan kunci 64 bit, tetapi delapan bit digunakan untuk pemeriksaan kesalahan (bit paritas), sehingga panjang kunci efektif untuk enkripsi hanya 56 bit. Dari kunci ini, 16 subkunci dibuat untuk digunakan dalam setiap putaran enkripsi.

3. Analisis Kelemahan DES

3.1 Panjang Kunci Yang Terlalu Pendek

Salah satu kelemahan utama DES adalah panjang kuncinya yang hanya 56 bit. Saat diperkenalkan, ukuran kunci ini dianggap aman karena keterbatasan teknologi

komputasi saat itu, tetapi ini tidak lagi relevan di era komputasi saat ini. Seperti yang ditunjukkan oleh berbagai eksperimen masa lalu, seperti proyek DESCHALL dan mesin pemecah kunci DES milik Electronic Frontier Foundation (EFF), "Deep Crack", DES sangat rentan terhadap serangan pemecahan kunci, seperti yang ditunjukkan oleh penelitian tentang kemampuan hardware saat ini untuk menguji semua kunci DES yang mungkin.

3.2 Resiko Serangan Kriptanalis

Selain masalah panjang kunci, DES juga memiliki kelemahan dalam kriptanalisis. Kriptanalisis diferensial, serangan yang dikembangkan oleh Biham dan Shamir, adalah jenis serangan yang memanfaatkan perbedaan pola pada pasangan plaintext untuk mengekstraksi informasi tentang kunci. Selain itu, kriptanalisis linear yang diperkenalkan oleh Matsui mampu mengurangi kompleksitas pencarian kunci dengan menggunakan pendekatan matematis yang menghubungkan plaintext, ciphertext, dan kunci, meskipun DES dirancang agar cukup tahan terhadap kriptanalisis diferensial.

3.3 Kelemahan Struktur Internal

DES memiliki kelemahan struktural juga. Kunci lemah dan semi-lemah dapat menghasilkan pola subkunci yang identik atau berulang. Karena sifat enkripsi dan dekripsi menjadi saling berkaitan secara tidak wajar, kondisi ini membuat proses enkripsi menjadi kurang aman. Selain itu, DES memiliki sifat komplementasi, yang berarti bahwa hasil enkripsi plaintext dengan kunci tertentu memiliki hubungan matematis langsung dengan hasil enkripsi komplemennya. Sifat ini secara efektif mengurangi jumlah ruang kunci yang harus dicoba dalam serangan brute-force, menurunkan tingkat keamanan DES.

3.4 Dampak Ukuran Blok yang Terbatas

Ukuran blok data DES yang kecil dapat menyebabkan munculnya pola dalam data hasil enkripsi, terutama ketika data yang dienkripsi dalam jumlah besar. Pola

tersebut bisa dimanfaatkan oleh pihak yang tidak berwenang untuk menganalisis dan memecahkan data terenkripsi.

4. Penyelesaian Dan Transisi DES

Sebagai tanggapan terhadap kelemahan DES, Triple DES (3DES) dikembangkan dengan menerapkan proses enkripsi DES sebanyak tiga kali dengan kombinasi beberapa kunci. Teknik ini berhasil meningkatkan tingkat keamanan, tetapi 3DES masih dianggap sebagai solusi sementara karena kinerjanya yang agak lambat. Pada akhirnya, pada tahun 2001, NIST mengganti DES dengan Standar Enkripsi Tinggi (AES). AES memiliki panjang kunci yang lebih besar dan algoritma yang lebih tahan terhadap berbagai serangan kriptografi kontemporer.

5. Kesimpulan

DES adalah algoritma enkripsi yang memiliki nilai sejarah penting dan berkontribusi besar dalam perkembangan keamanan informasi. Meski begitu, beberapa kelemahan membuat DES tidak lagi cocok digunakan untuk melindungi data di era digital saat ini. Karena itu, sekarang DES lebih baik dipelajari sebagai bahan pembelajaran untuk memahami perkembangan ilmu kriptografi, bukan sebagai cara untuk melindungi data secara nyata.

Distribusi Kunci Dalam Kriptografi Modern (Pki & Tls/Sll)

1. Pendahuluan

Keamanan data dalam sistem kriptografi kontemporer ditentukan oleh kedua kekuatan algoritma enkripsi dan cara kunci kriptografi didistribusikan. Bagaimana dua orang yang tidak pernah berbicara sebelumnya dapat menyepakati sebuah kunci rahasia melalui jaringan yang tidak aman adalah masalah utama dalam distribusi kunci.

Tujuan dari esai ini adalah untuk mempelajari mekanisme distribusi kunci kontemporer dengan mengutamakan Infrastruktur Kunci Publik (PKI) dan Protokol Lapisan Transportasi Keamanan (TLS/SSL), yang merupakan komponen utama keamanan komunikasi internet saat ini.

2. Distribusi Public Key Infrasructure (PKI)

Public Key Infrasructure (PKI) merupakan sebuah sistem yang dirancang untuk mengelola kunci publik dan identitas digital. Sistem ini melibatkan beberapa komponen utama, seperti Certificate Authority (CA), Registration Authority (RA), repositori sertifikat, serta sertifikat digital.

Sertifikat digital, yang biasanya dibuat sesuai dengan standar X.509, digunakan untuk mengaitkan identitas seseorang atau kelompok dengan kunci publiknya. Dengan adanya tanda tangan digital dari CA, orang lain dapat memastikan bahwa kunci publik tersebut adalah yang asli dan memastikan bahwa komunikasi dilakukan dengan entitas yang sah.

3. Keamanan TLS/SSL

Transport Layer Security (TLS), yang merupakan pengembangan dari Secure Sockets Layer (SSL), adalah sebuah protokol keamanan yang bertugas melindungi komunikasi data di internet. TLS bekerja di antara lapisan aplikasi dan lapisan transport, sehingga mampu mengamankan berbagai jenis layanan, seperti layanan web, email, dan transfer data. Pada layanan web, penerapan TLS terlihat dari penggunaan protokol HTTPS. Proses kerja TLS terbagi menjadi dua tahap utama, yaitu handshake dan pertukaran data.

Pada tahap handshake, klien dan server saling melakukan autentikasi serta menyetujui berbagai parameter keamanan, seperti versi TLS, algoritma kriptografi, dan

kunci enkripsi. Selain itu, server juga mengirimkan sertifikat digital yang nantinya akan diverifikasi oleh klien menggunakan mekanisme Public Key Infrastructure (PKI) untuk memastikan bahwa identitas server tersebut benar-benar sah.

Setelah proses autentikasi selesai, klien dan server akan membuat kunci sesi yang bersifat rahasia. Kunci ini digunakan untuk mengenkripsi semua data yang ditukar selama komunikasi, sehingga data tetap aman meskipun ada upaya penyadapan. TLS menggunakan kombinasi kriptografi asimetris untuk melakukan autentikasi dan pertukaran kunci, serta kriptografi simetris untuk mengenkripsi data yang sebenarnya, sehingga mampu menawarkan tingkat keamanan yang tinggi dengan performa yang efisien.

4. Forward Secrecy dan Pentingnya Algoritma Modern

Salah satu konsep penting dalam TLS modern adalah Forward Secrecy. Konsep ini bertujuan untuk melindungi data komunikasi yang sudah terjadi dari risiko kebocoran kunci di masa depan. Jika tidak ada Forward Secrecy, kemungkinan kebocoran kunci privat server bisa membuat semua komunikasi sebelumnya terbongkar dan bisa dibaca oleh pihak yang tidak berwenang.

Dengan adanya Forward Secrecy, setiap sesi komunikasi menggunakan kunci yang berbeda dan hanya berlaku untuk waktu tertentu. TLS modern mencapai hal ini dengan mengandalkan algoritma pertukaran kunci seperti Diffie-Hellman Ephemeral (DHE) atau Elliptic Curve Diffie-Hellman Ephemeral (ECDHE). Pada metode ini, kunci sesi tidak tergantung langsung pada kunci privat server yang digunakan jangka panjang.

Oleh karena itu, meskipun kunci privat server pernah bocor di masa depan, penyerang tetap tidak bisa membuka data komunikasi yang terjadi sebelumnya. Hal ini menjadikan Forward Secrecy sebagai fitur penting dalam menjaga keamanan komunikasi digital secara berkelanjutan.

5. Kesimpulan

Distribusi penting untuk keamanan komunikasi modern. Public Key Infrastructure (PKI) bertanggung jawab untuk menyediakan cara untuk mempercayai dan memverifikasi identitas seseorang melalui sertifikat digital. Di sisi lain, TLS/SSL

menggunakan metode ini untuk menegosiasikan kunci sesi secara aman dan melindungi data saat sedang dikirim. Kombinasi antara keduanya, terutama dengan konsep Forward Secrecy, memastikan bahwa komunikasi tetap aman meskipun terjadi di jaringan umum. Oleh karena itu, mekanisme distribusi penting ini menjadi inti dari keamanan layanan digital yang digunakan saat ini.

DAFTAR PUSTAKA

Ariska, A., & Wahyuddin, W. (2022). Penerapan Kriptografi Menggunakan Algoritma Des (Data Encryption Standard). *Jurnal sintaks logika*, *2*(2), 9-19.

Rizqa, I., Safitri, A. N., & Harkespan, I. (2022). Kriptostegano Menggunakan Data Encryption Standard dan Least Significant Bit dalam Pengamanan Pesan Gambar. *Jurnal Masyarakat Informatika*, *13*(2), 111-120.

Sipayung, L. Y., & Purba, M. (2023). Data security analysis with triple DES cryptographic algorithm. *Journal of Intelligent Decision Support System (IDSS)*, *6*(4), 285-294.

Asaju, B. J. (2024). Addressing public key infrastructure (PKI) challenges in V2X networks: strategies for scalability, certificate management, and trusted authorities. *Journal of Science & Technology*, *5*(1), 69-86.

Aditya, M. F., Arfanda, W., Purnama, V. N., & Dara, C. (2023). STUDI ALGORITMA KRIPTOGTAFI KUNCI SIMETRIS PADA KEAMANAN DATA DENGAN METODE KOMPARASI. *JURNAL SITEBA*, *2*(1), 7-14.