Analisis Kelemahan DES dan Distribusi Kunci (PKI & TLS/SSL)

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

Dosen Pengampu : Kodrat Mahatma.

Universitas Teknologi Digital

Disusun oleh:

Fernanda Syah Putra 20123019

PROGRAM STUDI S1 INFORMATIKA

UNIVERSITAS TEKNOLOGI DIGITAL

2025

Pendahuluan

Kriptografi merupakan fondasi utama dalam menjaga kerahasiaan, integritas, dan keaslian data pada sistem informasi modern. Dua aspek penting dalam kriptografi adalah algoritma enkripsi dan mekanisme distribusi kunci. Data Encryption Standard (DES) merupakan salah satu algoritma kriptografi simetris paling awal yang digunakan secara luas, sementara Public Key Infrastructure (PKI) dan protokol TLS/SSL menjadi tulang punggung distribusi kunci dan keamanan komunikasi di internet.

Makalah ini membahas dua fokus utama: (1) analisis kelemahan DES berdasarkan studi literatur dan perkembangan komputasi, serta (2) analisis distribusi kunci modern melalui PKI dan TLS/SSL, termasuk kelebihan dan tantangannya.

1. Analisis Kelemahan DES

1.1 Gambaran Umum DES

DES adalah algoritma block cipher simetris yang dikembangkan oleh IBM dan diadopsi sebagai standar oleh NIST pada tahun 1977. DES menggunakan ukuran blok 64-bit dan panjang kunci efektif 56-bit, dengan struktur Feistel sebanyak 16 ronde.

Pada masanya, DES dirancang untuk efisiensi perangkat keras dan keamanan yang cukup terhadap ancaman yang ada. Namun, perkembangan teknologi komputasi membuat DES tidak lagi memadai untuk digunakan pada sistem modern.

1.2 Kelemahan Panjang Kunci

Kelemahan paling fundamental dari DES adalah panjang kuncinya yang hanya 56-bit. Dengan ruang kunci sebesar 2^56, serangan brute force menjadi sangat realistis.

Pada tahun 1998, Electronic Frontier Foundation (EFF) berhasil membangun mesin khusus bernama *DES Cracker* yang mampu memecahkan kunci DES dalam waktu kurang dari tiga hari. Saat ini, dengan GPU dan cloud computing, serangan brute force terhadap DES dapat dilakukan dalam hitungan jam atau menit.

1.3 Kerentanan terhadap Serangan Kriptanalisis

Selain brute force, DES juga rentan terhadap beberapa bentuk kriptanalisis:

- **Differential Cryptanalysis**: Menganalisis perbedaan input dan output untuk menebak kunci.
- **Linear Cryptanalysis**: Menggunakan pendekatan statistik untuk menemukan hubungan linear antara plaintext, ciphertext, dan kunci.

Meskipun DES relatif tahan terhadap differential cryptanalysis dibanding algoritma awal lainnya, tingkat keamanannya tetap tidak memadai untuk standar keamanan modern.

1.4 Ukuran Blok yang Terbatas

Ukuran blok DES yang hanya 64-bit meningkatkan risiko serangan *birthday attack* ketika volume data yang dienkripsi sangat besar. Hal ini memungkinkan penyerang menemukan pola atau collision pada ciphertext.

1.5 Status DES di Era Modern

Karena berbagai kelemahan tersebut, DES telah dinyatakan tidak aman dan tidak direkomendasikan lagi. Sebagai solusi sementara, dikembangkan Triple DES (3DES), namun kini 3DES juga mulai ditinggalkan dan digantikan oleh Advanced Encryption Standard (AES).

2. Distribusi Kunci: PKI dan TLS/SSL

2.1 Permasalahan Distribusi Kunci

Dalam kriptografi simetris seperti DES, tantangan utama bukan hanya algoritma enkripsi, tetapi juga bagaimana kunci rahasia dapat dibagikan secara aman. Distribusi kunci yang tidak aman akan membuat sistem kriptografi menjadi sia-sia.

2.2 Public Key Infrastructure (PKI)

PKI adalah kerangka kerja yang menggunakan kriptografi kunci publik untuk mengelola identitas digital dan distribusi kunci. PKI melibatkan:

- **Certificate Authority (CA)** sebagai pihak tepercaya
- **Digital Certificate** untuk mengikat identitas dengan kunci publik

- **Public & Private Key Pair**

Dengan PKI, kunci publik dapat didistribusikan secara terbuka tanpa mengorbankan keamanan, sementara kunci privat tetap dirahasiakan.

2.3 TLS/SSL sebagai Implementasi Distribusi Kunci

TLS/SSL adalah protokol keamanan yang menggunakan PKI untuk melakukan *handshake*, yaitu proses negosiasi kunci antara klien dan server. Pada tahap ini:

1. Server mengirim sertifikat digital.
2. Klien memverifikasi sertifikat melalui CA.
3. Kunci sesi simetris dibuat secara aman.

Setelah handshake selesai, komunikasi dienkripsi menggunakan algoritma simetris yang jauh lebih efisien seperti AES.

2.4 Kelebihan dan Keterbatasan PKI & TLS/SSL

Kelebihan:

- Distribusi kunci aman tanpa saluran rahasia
- Skalabilitas tinggi untuk internet
- Mendukung autentikasi dan integritas

Keterbatasan:

- Ketergantungan pada CA (single point of trust)
- Risiko kompromi sertifikat
- Kompleksitas implementasi

Kesimpulan

DES merupakan algoritma kriptografi yang memiliki nilai historis tinggi, namun tidak lagi layak digunakan karena kelemahan panjang kunci, ukuran blok, dan kerentanan terhadap serangan modern. Permasalahan distribusi kunci pada kriptografi simetris dijawab oleh PKI dan protokol TLS/SSL, yang menjadi fondasi keamanan komunikasi digital saat ini.

Pemahaman terhadap kelemahan DES dan mekanisme distribusi kunci modern penting agar perancang sistem dapat memilih algoritma dan protokol yang tepat sesuai standar keamanan terkini.

Daftar Pustaka

1. Paar, C., & Pelzl, J. (2010). *Understanding Cryptography*. Springer.
2. NIST. (1999). *Data Encryption Standard (DES)*.
3. EFF. (1998). *Cracking DES*.
4. Kahn Academy & Christof Paar YouTube Lectures.
5. Dierks, T., & Rescorla, E. (2008). *The Transport Layer Security (TLS) Protocol*. IETF.

Lampiran Implementasi Code:

Google Colab :https://colab.research.google.com/drive/19-1QPYd6MaTGMuBigvxsvusKvsRfoOOx?usp=sharing