MODUL 8

KRIPTOGRAFI DAN TEKNIK PENYAMARAN INFORMASI

8.1 Tujuan Praktikum

1. Mengetahui dan memahami konsep kriptografi dan teknik penyamaran informasi
2. Mengetahui dan memahami tujuan penyamaran informasi
3. Mengetahui dan memahami macam-macam teknik kriptografi dan teknik penyamaran informasi
4. Mengethaui dan memahami implementasi dari kriptografi dan teknik penyamaran informasi lain dalam keamanan jaringan

8.2 Alat dan Bahan

1. VirtualBox
2. OS Kali Linux
3. Steghide
4. Laptop
5. Mouse

8.3 Dasar Teori

8.3.1 Pengertian Kriptografi

Kata kriptografi atau cryptography diketahui berasal dari bahasa Yunani, kripto dan graphia. Dimana kripto memiliki arti menyembunyikan, sementar graphia berarti tulisan. Sehingga bisa dijabarkan kriptografi merupakan ilmu yang mempelajari teknik-teknik matematika yang berkaitan dengan aspek keamanan informasi.

8.3.2 Sejarah Kriptografi

Kriptografi menurut catatan sejarah telah eksis sejak masa kejayaan Yunani atau kurang lebih sekitar tahun 400 Sebelum Masehi. Alat yang

digunakan untuk membuat pesan tersembunyi di Yunani pada waktu itu disebut *Scytale*. *Scytale* berbentuk batangan silinder dengan kombinasi 18 huruf.

Pada masa Romawi, di bawah kekuasaan Julius Caesar, penggunaan kriptografi semakin intens karena pertimbangan stabilitas negara. Meski teknik yang digunakan tak serumit Yunani, namun untuk memahami pesan kriptografi dari masa Romawi terbilang cukup sulit untuk dikerjakan.

8.3.3 Tujuan Kriptografi

Tujuan Kriptografi digunakan diantaranya:

1. Kerahasiaan

   Hal ini berkaitan dengan layanan yang berfungsi menjaga isi informasi. Kerahasiaan diberlakukan kepada siapa saja. Tentunya selain kepada Anda yang mempunyai kunci rahasia atau otoritas untuk membuka informasi terkait menggunakan kata sandi yang tepat.

2. Integritas Data

   Tujuan kedua berkaitan dengan penjagaan perubahan data yang tidak sah. Misalnya dari upaya tidak bertanggung jawab para *hacker*. Dibutuhkan suatu sistem yang dapat mendeteksi manipulasi data yang dilakukan pihak lain seperlu menjaga integritas data. Adapun manipulasi yang dimaksud bisa berupa penyisipan, penghabusan, hingga pensubsitusian data lain ke dalam data asli.

3. Autentikasi

   Autentikasi dalam kriptografi berkaitan dengan pengenalan atau identifikasi, baik yang berlangsung untuk kesatuan sistem atau hanya informasi itu sendiri. Dalam hal ini dua belah pihak yang saling berkomunikasi wajib memperkenalan diri. Adapun info diri yang diberikan via kanal mesti diautentikasi kebenarannya. Yakni mencakup isi data, waktu pengiriman, dan lain sebagainya.

4. Non Repudiasi

   Tujuan keempat adalah non repudiasi atau yang populer juga disebut anti penyangkalan. Merupakan suatu upaya seperlu mencegah adanya penyangkalan akan pengiriman informasi oleh pihak yang mengirim. Penyangkalan bahwa pesan berasal dari pihak yang ditunjuk.

8.3.4 Teknik-Teknik Kriptografi

Algoritma kriptografi dibedakan menjadi beberapa teknik yaitu:

1. Simetris

   Kriptografi simetris adalah salah satu algoritma kriptografi kunci simetris dan kripto polyalphabetic. Kriptografi jenis ini populer juga disebut dengan hill cipher atau kode hill. Jenis kriptografi ini diciptakan oleh Lester S. Hil sekitar tahun 1929 yang mana dibuat dengan tujuan bisa mewujudkan cipher yang tidak mudah dipecahkan meski menggunakan teknik analisis frekuensi.

2. Asimetris

   Jenis kriptografi berikutnya kriptografi asimetris yang memanfaatkan 2 jenis kunci. Algoritma kunci publik ini menggunakan kunci publik dan juga kunci rahasia. Kedua jenis kunci tersebut memiliki fungsi berbeda seperti kunci publik untuk mengenkripsi pesan. Kunci publik bersifat global yang tidak dirahasiakan sehingga bisa dilihat oleh siapa saja. Sementara kunci rahasia termasuk kunci yang dirahasiakan yang hanya bisa dilihat oleh orang tertentu saja.

3. Hybrid

   Kriptografi hybrid adalah jenis kriptografi yang dibuat seperlu mengatasi adanya trade off antara kecepatan dan kenyamanan. Dimana diketahui semakin aman, sejatinya semakin tidak nyaman. Sebaliknya semakin nyaman, maka sebenarnya sistem semakin tidak aman.

Selain kriptografi simetris, asimetris, dan hybrid terdapat pula teknik kriptografi lain yang digunakan dalam keamanan jaringan, yaitu:

1. *Encoding*

   Encoding adalah proses mengubah data menjadi format lain dengan menggunakan aturan tertentu, tetapi tidak ada upaya untuk mengamankan data. Ini lebih merupakan teknik representasi ulang data daripada metode keamanan sejati.

   Encoding adalah proses yang dapat diulang dan *reversibel*, artinya data yang diubah dapat dikembalikan ke bentuk aslinya tanpa memerlukan kunci khusus.

Contoh *encoding* termasuk Base64 encoding, URL encoding, dan HTML *encoding*. Ini sering digunakan untuk mengubah data biner menjadi format teks yang dapat ditransmisikan melalui protokol teks.

2. *Encryption* (Enkripsi)

   Encryption adalah proses mengubah data menjadi bentuk yang tidak dapat dibaca atau sulit dipahami, yang disebut *ciphertext*, dengan menggunakan algoritma enkripsi dan kunci enkripsi tertentu.

   Tujuan enkripsi adalah melindungi kerahasiaan data dan mencegah akses yang tidak sah. Hanya pihak yang memiliki kunci enkripsi yang benar yang dapat mendekripsi dan mengembalikan data ke bentuk aslinya.

   Enkripsi dapat menggunakan kunci simetris (kunci yang sama digunakan untuk enkripsi dan dekripsi) atau kunci asimetris (pasangan kunci publik dan pribadi) tergantung pada algoritma yang digunakan.

   Contoh algoritma enkripsi termasuk AES, RSA, dan DES.

3. Dekripsi

   Dekripsi adalah kebalikan dari enkripsi. Ini adalah proses mengubah data yang telah dienkripsi kembali ke dalam format asli atau terbaca. Proses dekripsi memerlukan penggunaan kunci dekripsi yang sesuai yang cocok dengan kunci enkripsi yang digunakan saat proses enkripsi.

   Dekripsi dilakukan oleh penerima atau pemegang kunci dekripsi yang sah untuk mengakses data yang telah dienkripsi. Proses ini mengembalikan data ke bentuk semula sehingga dapat dibaca dan dimengerti.

4. *Hashing* (Pengacakan)

   Hashing adalah proses mengonversi data (*plaintext*) menjadi nilai *hash* yang tetap panjang dan unik menggunakan fungsi *hash*.

   Hash digunakan untuk menguji integritas data dan memverifikasi tanda tangan digital. Nilai *hash* yang dihasilkan akan berbeda jika ada perubahan pada data input.

   Proses *hashing* bersifat satu arah (*one-way*), artinya tidak dapat mengembalikan nilai hash ke bentuk *plaintext* aslinya.

Contoh fungsi hash termasuk SHA-256, MD5, dan SHA-1. Penggunaan yang tepat dari fungsi *hash* sangat penting untuk keamanan dan integritas data.

8.3.5 Steganografi

Teknik penyamaran informasi dalam keamanan jaringan sering disebut "Steganografi." Steganografi adalah suatu metode atau teknik yang digunakan untuk menyembunyikan informasi dalam data atau media lain secara tidak terlihat atau tidak terdeteksi oleh mata manusia atau alat deteksi biasa. Dalam konteks keamanan jaringan, steganografi dapat digunakan untuk menyembunyikan data sensitif dalam file gambar, audio, atau bahkan teks biasa tanpa menarik perhatian yang tidak sah. Dengan menggunakan steganografi, pengguna dapat menyisipkan pesan rahasia ke dalam gambar, audio, atau bahkan video, dan kemudian mengirimkannya melalui jaringan tanpa membuatnya terlihat bagi pihak yang tidak berhak. Penerima yang sah kemudian dapat mengungkap pesan tersebut dengan menggunakan kunci atau alat dekripsi yang sesuai. Steganografi adalah salah satu alat yang digunakan dalam upaya untuk menjaga kerahasiaan dan keamanan komunikasi dalam dunia digital dan sering digunakan bersamaan dengan enkripsi untuk melindungi informasi yang dikirimkan melalui jaringan.

8.3.6 Teknik-Teknik Steganografi

Ada beberapa teknik penyamaran informasi atau steganografi yang digunakan untuk menyembunyikan data dalam media atau komunikasi yang berbeda. Berikut beberapa teknik penyamaran informasi yang umum digunakan:

- Steganografi Gambar: Teknik ini melibatkan penyisipan data dalam file gambar. Data rahasia dapat disembunyikan dalam piksel-piksel gambar atau bahkan dalam struktur metadata gambar. Teknik ini mencakup metode seperti LSB (*Least Significant Bit*) steganografi, di mana data disisipkan pada bit paling tidak signifikan dalam gambar.
- Steganografi Audio: Dalam steganografi audio, data rahasia disisipkan dalam file audio, seperti mp3 atau WAV, dengan mengubah amplitudo atau

frekuensi suara. Ini dapat dilakukan dengan mengganti sampel suara yang kurang signifikan.

- Steganografi Video: Serupa dengan steganografi gambar, teknik ini digunakan untuk menyembunyikan data dalam file video. Data dapat disisipkan dalam bingkai video atau struktur metadata.
- Steganografi Teks: Dalam steganografi teks, data rahasia disisipkan dalam teks biasa dengan cara mengubah tampilan atau format teks, seperti menggunakan spasi ekstra, penggantian karakter, atau metode lainnya.
- Steganografi File: Teknik ini melibatkan menyisipkan data rahasia dalam file lain, seperti dokumen PDF, file Word, atau file lainnya. Data rahasia dapat disisipkan dalam metadata file atau sebagai tambahan dalam konten file.
- Steganografi Jaringan: Ini melibatkan penyisipan data rahasia dalam lalu lintas jaringan. Teknik ini digunakan dalam komunikasi melalui jaringan untuk menyembunyikan pesan dari pihak yang tidak berhak.
- Steganografi Pesan Tersembunyi: Dalam teknik ini, pesan tersembunyi disisipkan dalam pesan yang tampaknya tidak mencurigakan. Misalnya, mengganti kata-kata tertentu dalam teks dengan sinonimnya yang memiliki makna yang sama.
- Steganografi File Sistem: Data rahasia dapat disembunyikan dalam struktur file sistem, seperti file sistem operasi atau file konfigurasi.
- Steganografi dalam Email atau Dokumen Web: Teknik ini melibatkan penyisipan data rahasia dalam email atau dokumen web, seringkali dengan menggunakan font atau warna teks yang hampir tidak terlihat.
- Steganografi dalam *QR Code*: *QR code* dapat digunakan untuk menyembunyikan data tambahan dalam gambar kode QR tanpa mengganggu fungsi utamanya.

8.3.7 Steghide

Steghide adalah salah satu *tool* yang berfungsi untuk belajar Steganografi menggunakan *command line* di terminal Linux. Steghide merupakan program Steganografi yang menyembunyikan bit-bit suatu file data di beberapa bit paling tidak signifikan dari file lain sedemikian rupa sehingga keberadaan file data tersebut tidak dapat dilihat dan tidak dapat dibuktikan. Steghide dirancang secara portable dan dapat dikonfigurasi serta memiliki fitur penyembunyian data dalam file bmp, jpeg, wav dan file au, enkripsi *blowfish*, MD5 hashing untuk paraphrase ke *blowfish key*, dan distribusi bit tersembunyi secara *pseudo-random* dalam sebuah data kontainer. Setghide juga sangat berguna dalam investigasi digital forensik.