UAS KEAMANAN INFORMASI

RESUME TENTANG

“CRYPTOGRAPHY”

Oleh :

MUHAMMAD ALI MUKARROM

1310652023

TEKNIK INFORMATIKA

UNIVERSITAS MUHAMMADIYAH JEMBER

Kriptografi disebut juga persandian yaitu secara singkat dapat berarti seni melindungi data dan informasi dari pihak-pihak yang tidak dikehendaki baik saat ditransmisikan maupun saat disimpan. Ilmu persandiannya disebut **KRIPTOLOGI** yaitu ilmu yang mempelajari tentang bagaimana tehnik melindungi data dan informasi tersebut beserta seluruh ikutannya.

Jenis kriptografi :
Ada tiga jenis utama dari enkripsi yang modern

- **Enkripsi simetris** menggunakan satu kunci untuk mengenkripsi dan mendekripsi
- **Kriptografi asimetris** menggunakan dua kunci : mengenkripsi dengan satu kunci , dapat mendekripsi dengan yang lain .Atau disebut juga kunci public.
- **Hashing** adalah transformasi kriptografi satu arah menggunakan algoritma dan tidak ada kunci

Serangan pada Kriptografi / serangan pada Enkripsi

Tujuan dari penyerang dalam semua kasus adalah untuk dapat mendekrip sebuah ciphertext baru tanpa informasi tambahan. Yang menjadi idaman bagi penyerang adalah untuk mengekstrak kunci rahasia.

- **Known-key attack.** Pada serangan ini penyerang mendapatkan beberapa kunci yang telah digunakan sebelumnya kemudian menggunakan informasi ini untuk menentukan kunci baru.

- **Tanda tangan digital** digunakan untuk dokumen tanda kriptografi. Tanda tangan digital yang mencakup otentikasi identitas penandatangan, dan membuktikan dokumen tidak berubah. Maksudnya pengirim tidak dapat menyangkal atau menolak menandatangani dokumen.

- **Infrastruktur Kunci Publik** dibuat untuk dapat mengelola dokumen digital yang ditandatangani secara digital. Infrastruktur Kunci Publik memanfaat 3 bentuk enkrpsi.

Escrow Account

Pihak ketiga yang memegang salinan public atau sepasang kunci pribadi yang sering dibagi menjadi 2 bagian atau lebih.

KESIMPULAN

Kriptografi merupakan salah satu dari media komunikasi dan informasi kuno yang masih dimanfaatkan hingga saat ini. Kriptografi disebut juga persandian yaitu secara singkat dapat berarti seni melindungi data dan informasi dari pihak-pihak yang tidak dikehendaki baik saat ditransmisikan maupun saat disimpan. Sedangkan ilmu persandiannya disebut kriptologi yaitu ilmu yang mempelajari tentang bagaimana tehnik melindungi data dan informasi tersebut beserta seluruh ikutannya.Pengguna diberikan ID dan password untuk mengakses sistem yang ada. Password dienkripsi untuk mencegah terjadinya akses illegal terhadap sistem misalnya pencurian data-data penting oleh mereka yang tidak berhak. Demikian juga enkripsi pada file-file penting dapat dilakukan (misalnya file yang berisi data keuangan). Metode enkripsi yang digunakan dapat berbentuk enkripsi kunci simetris, misalnya menggunakan algoritma DES, RSA, dll. Untuk mendapatkan algoritma enkripisi ini tidak dibutuhkan biaya karena telah dipublikasikan secara umum. Oleh karena itu, dapat disimpulkan bahwa kriptografi masih merupakan sistem yang efektif dalam hal keamanan dan proteksi serta dapat digunakan secara luas di berbagai bidang usaha dan teknologi.