RESUME

KRIPTOGRAFI

Penyusun :

Juwita Dwi Wayudi

1110651149

KELAS : D

JURUSAN TEKNIK INFORMATIKA UNIVERSITAS MUHAMMADIAH JEMBER TAHUN AJARAN 2014 -2015

DEFINISI KRIPTOGRAFI

- **Kriptografi didefinisikan** sebagai ilmu dan pelajaran untuk tulisan rahasia dengan pertimbangan bahwa komunikasi dan data dapat dikodekan untuk mencegah dari mata-mata atau orang lain yang ingin mengetahui isinya, dengan menggunakan kode-kode dan aturan-aturan tertentu dan metode lainnya sehingga hanya orang yang berhak yang dapat mengetahui isi pesan sebenarnya.
  Dalam menjaga kerahasiaan data, *kriptografi* mentransformasikan data jelas (plaintext) ke dalam bentuk data sandi (ciphertext) yang tidak dapat dikenali. Ciphertext inilah yang kemudian dikirimkan oleh pengirim (sender) kepada penerima (receiver). Setelah sampai di penerima, ciphertext tersebut ditranformasikan kembali ke dalam bentuk plaintext agar dapat dikenali.

TUJUAN DASAR KRIPTOGRAFI

- Kerahasiaan, adalah layanan yang digunakan untuk menjaga isi dari informasi dari siapapun kecuali yang memiliki otoritas atau kunci rahasia untuk membuka/mengupas informasi yang telah disandi.
- Integritas data, adalah berhubungan dengan penjagaan dari perubahan data secara tidak sah. Untuk menjaga integritas data, sistem harus memiliki kemampuan untuk mendeteksi manipulasi data oleh pihak-pihak yang tidak berhak, antara lain penyisipan, penghapusan, dan pensubsitusian data lain kedalam data yang sebenarnya.
- Autentikasi, adalah berhubungan dengan identifikasi/pengenalan, baik secara kesatuan sistem maupun informasi itu sendiri. Dua pihak yang saling berkomunikasi harus saling memperkenalkan diri. Informasi yang dikirimkan melalui kanal harus diautentikasi keaslian, isi datanya, waktu pengiriman, dan lain-lain.
- Non-repudiasi., atau nirpenyangkalan adalah usaha untuk mencegah terjadinya penyangkalan terhadap pengiriman/terciptanya suatu informasi oleh yang mengirimkan/membuat.

SUBTITUSI DAN PERMUTASI KRIPTOGRAFI

- merupakan sistem kriptografi simetris bertipe block cipher yang bersifat iteratif, terdiri dari proses substitusi, permutasi, dan penjadwalan kunci. Salah satu algoritma kriptografi yang berbasis pada SPN adalah AES (Advanced Encryption Standard). Berbeda dengan DES (Data Encryption Standard) yang berbasis pada jaringan Feistel. Pada tahun 2001, NIST (National Institute of Standards and Technology) menetapkan AES sebagai standar enkripsi untuk menggantikan DES yang telah digunakan sebagai standar enkripsi sejak tahun 1973.

KEKUATAN KRIPTOGRAFI

- Kekuatan dari algoritma kriptografi umumnya bergantung kepada kuncinya, oleh sebab itu kunci yang lemah tidak boleh digunakan. Panjang kunci yang digunakan juga menentukan kekuatan dari dari algoritma kriptografi contoh kunci yang panjangnya 128bit lebih sukar dipecahkan jika dibandingkan dengan kunci 56bit dengan algoritma yang sama.

MONOALFABETIK DAN POLIALFABETIK CHIPER

- Monoalfabetik chiper Pada prinsipnya, setiap huruf digantikan dengan huruf yang berada tiga (3) posisi dalam urutan alfabet. Sebagai contoh huruf “a” digantikan dengan huruf “D” dan seterusnya.
- Polialfabetik chipper pada Penyandi Polialfabetik adalah Playfair. Playfair ini menggunakan tabel 5×5. Semua alfabet kecuali J diletakkan ke dalam tabel. Huruf J dianggap sama dengan huruf I, sebab huruf J mempunyai frekuensi kemunculan yang paling kecil.

EXCLUSIVE OR

- Dalam Mendukung Kriptografi, nilai biner yang, dalam sebuah operasi eksklusif-OR dengan nilai biner yang diberikan dari panjang yang sama, menghasilkan nilai biner dari semua orang.
 (2) Nilai yang dapat ditambahkan ke nomor yang sama nilai yang diberikan.

JENIS-JENIS KRIPTOGRAFI

- Algoritma kriptografi berdasarkan jenis kunci yang digunakan dapat dibedakan menjadi dua jenis yaitu :
    - Algoritma *simetris*
- Dimana kunci yang digunakan untuk proses enkripsi dan dekripsi adalah kunci yang sama
    - Algoritma *asimetris*
- Dimana kunci yang digunakan untuk proses enkripsi dan dekripsi menggunakan kunci yang berbeda.

ENKRIPSI SIMETRIS

- adalah algoritma yang menggunakan kunci untuk proses enkripsi sama dengan kunci untuk proses dekripsi. Algoritma kriptografi simetris dibagi menjadi 2 kategori yaitu algoritma aliran (*Stream Ciphers*) dan algoritma blok (*Block Ciphers*). Pada algoritma aliran, proses penyandiannya berorientasi pada satu bit atau satu byte data. Sedang pada algoritma blok, proses penyandiannya berorientasi pada sekumpulan bit atau byte data (per blok).

ENKRIPSI ASIMETRIS

- Kunci asimetris adalah pasangan kunci-kunci kriptografi yang salah satunya dipergunakan untuk proses enkripsi dan yang satu lagi untuk dekripsi. Semua orang yang mendapatkan kunci publik dapat menggunakannya untuk mengenkripsikan suatu pesan, sedangkan hanya satu orang saja yang memiliki rahasia tertentu – dalam hal ini kunci privat – untuk melakukan pembongkaran terhadap sandi yang dikirim untuknya.

FUNGSI HASH

- Fungsi Hash merupakan sebuah algoritma yang mengubah text atau message menjadi sederetan karakter acak yang memiliki jumlah karakter yang sama. Hash juga termasuk salah satu bentuk teknik kriptografi dan dikategorikan sebagai kriptografi tanpa key (*unkeyed cryptosystem*). Selain itu hash memiliki nama lain yang juga dikenal luas yaitu "*one-way functio*n".

SERANGAN TERHADAP KRIPTOGRAFI

- Serangan terhadap kriptografi pada dasarnya adalah memecahkan (membongkar keamanan) algoritma kriptografi, yang selanjutnya digunakan untuk usaha mengupas data tersandi tanpa mengetahui/menggunakan kunci. Kegiatan ini (memecahkan algoritma kriptografi) adalah bagian dari kriptanalisis, yaitu ilmu/seni memecahkan data tersandi. Kripanalisis dan kriptografi merupakan sebuah cabang ilmu pengetahuan yang disebut kriptologi.