UJIAN AKHIR SEMESTER
KEAMANAN INFORMASI
KRIPTOGRAFI

Nama:

Dirga Rahman Kharisma Burhanudin 1310651122

Jurusan Teknik
Akademi Teknik Informatika
Jember 2015

KRIPTOGRAFI

Kriptografi adalah sebuah cara untuk melakukan komunikasi yang aman yang hanya dapat dipahami oleh penerima yang dimaksud saja, dengan cara dienkripsi yaitu kata sebenarnya kita ubah menjadi sebuah kode yang dapat dipahami oleh penerima yang dituju dengan mendekripsi informasi yang terenkripsi tersebut, sehingga pihak ketiga tidak akan dapat memahami informasi yang dienkripsi oleh pengirim.

TAHUKAH ANDA?

Enkripsi yang kuat menghancurkan pola.Jika satu bit perubahan plaintext, kemungkinan setiap sedikit menghasilkan ciphertext perubahan harus 50/50.Tanda-tanda nonrandomness dapat digunakan sebagai petunjuk untuk cryptanalyst sebuah, mengisyaratkan pada urutan yang mendasari plaintext asli atau kunci.

Jenis Kriptografi

Enkripsi Simetris

Enkripsi simetris menggunakan satu kunci untuk mengenkripsi dan mendekripsi.Jika Anda mengenkripsi file zip dan kemudian mendekripsi dengan kunci yang sama, Anda menggunakan enkripsi simetris.Enkripsi simetris juga disebut "kunci rahasia" enkripsi: kunci harus dirahasiakan dari pihak ketiga.Kekuatan termasuk kecepatan dan kekuatan kriptografi per bit dari kunci.Kelemahan utama adalah bahwa kunci harus aman bersama sebelum kedua pihak dapat berkomunikasi secara aman.Kunci simetris sering bersama melalui metode out-of-band, seperti melalui tatap muka diskusi.

Stream dan blok cipher

Enkripsi simetris mungkin memiliki aliran dan blok mode.Modus aliran berarti setiap bit secara independen dienkripsi dalam mode Blok cipher mengenkripsi blok data setiap putaran "aliran.": 56 bit untuk Data Encryption Standard (DES) dan 128, 192, atau 256 bit AES untuk, misalnya.Beberapa cipher blok dapat meniru stream cipher dengan menetapkan ukuran blok untuk 1 bit;mereka masih dianggap cipher blok.

Vektor inisialisasi dan chaining

Vektor inisialisasi digunakan dalam beberapa cipher simetrik untuk memastikan bahwa blok dienkripsi pertama data acak.Hal ini memastikan bahwa plainteks identik mengenkripsi untuk ciphertexts yang

berbeda.Juga, sebagai Bruce Schneier mencatat di Applied Cryptography, "Lebih buruk lagi, dua pesan yang dimulai sama akan mengenkripsi dengan cara yang sama untuk perbedaan pertama.Beberapa pesan memiliki header umum. Kop surat, atau 'Dari' line, atau apa pun "1 vektor Inisialisasi memecahkan masalah ini.Chaining (disebut umpan balik dalam mode aliran) biji blok dienkripsi sebelumnya ke blok berikutnya yang akan dienkripsi.Ini menghancurkan pola dalam ciphertext yang dihasilkan.Modus DES Elektronik Kode Buku (lihat di bawah) tidak menggunakan vektor inisialisasi atau chaining dan pola dapat terlihat jelas dalam ciphertext yang dihasilkan.

DES

DES adalah Data Encryption Standard, yang menggambarkan Algoritma Enkripsi Data (DEA).IBM dirancang DES, berdasarkan lama Lucifer simetris cipher mereka.Menggunakan ukuran blok 64-bit (yang berarti mengenkripsi 64 bit setiap putaran) dan kunci 56-bit.