Nama : Wildan Akmala

NIM : 1310651044

Kelas : C

UAS Take Home Sistem Keamanan Informasi

Tugas 1

Resume Tentang Cryptography

PENGERTIAN Dari cryptography

Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data .Tetapi tidak semua aspek keamanan informasi dapat diselesaikan dengan kriptografi.
Kriptografi dapat pula diartikan sebagai ilmu atau seni untuk menjaga keamanan pesan.

Ada tiga jenis utama dari enkripsi yang modern:

- Simetris, menggunakan satu kunci: mengenkripsi kunci yang sama dan mendekripsi bisa disebut juga “KUNCI RAHASIA”
  Kelemahan : untuk tiap pengiriman pesan dengan pengguna yang berbeda dibutuhkan kunci yang berbeda juga
- Asimetris, menggunakan dua kunci: jika Anda mengenkripsi dengan satu tombol, Anda mungkin mendekripsi dengan yang lain. Disebut juga “KUNCI PUBLIK”.
  Kelemahan : kecepatan lebih rendah bila di bangdingkan dengan simetris, untuk tingkat keamanan sama, kunci yang digunakan lebih panjang dibandingkan dengan simetris.
- Hashing adalah transformasi kriptografi satu arah menggunakn algoritma dan MD5.
  MD5 adalah algoritma Message Digest 5, diciptakan oleh Ronald Rivest. Ini adalah yang paling
  banyak digunakan dari keluarga MD algoritma hash. MD5 menciptakan nilai hash 128-bit berdasarkan pada setiap panjang input. MD5 telah cukup populer selama bertahun-tahun, namun kelemahan
  telah ditemukan di mana tabrakan dapat ditemukan dalam jumlah yang praktis
  waktu. MD6 adalah versi terbaru dari keluarga MD algoritma hash, pertama kali diterbitkan pada tahun 2008.

Plaintext, yaitu pesan yang dapat dibaca
Ciphertext, yaitu pesan acak yang tidka dapat dibaca
Key, yaitu kunci untuk melakukan teknik kriptografi
Algorithm, yaitu metode untuk melakukan enkrispi dan dekripsi.

SERANGAN CRYPTOGRAPHY
Selain ada pihak yang ingin menjaga agar pesan tetap aman , dan juga ada yang ingin mengetahui pesan rahasia tersebut. Ada beberapa macam penyerangan , yaitu :

- Chipertext attack , penyerangan hanya mendapatkan pesan yang sudah tersandikan saja.

- Know Plaintext attack, selain mendapatkan sandi , juga mendapatkan pesan asli . bisa disebut dengan cleartext attack.
- Choosen plaintext attack, sama dengan know plainttext attack, namun penyerang bahkan dapat memilih penggalan mana dari pesan asli yang akan disandikan.

Beberapa contoh nyata dari kriptografi

- Digital signatures(tanda tangan digital)

Contoh
Roy ingin mengirim e-mail secara digital menandatangani kontrak dengan Rick. Roy menulis e-mail, yang adalah plaintext. Dia kemudian menggunakan fungsi SHA-1 hash untuk menghasilkan nilai hash dari plaintext. Dia kemudian menciptakan tanda tangan digital dengan mengenkripsi hash dengan RSA nya kunci pribadi

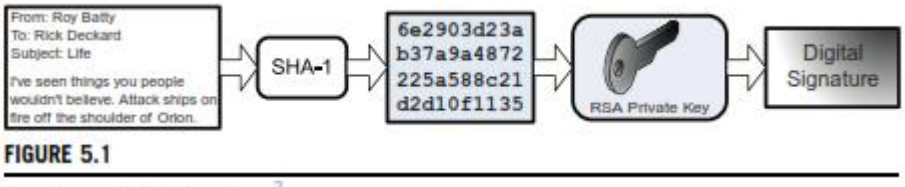


FIGURE 5.1

Gambar diatas menunjukkan proses ini. Roy kemudian menempel tanda tangan untuk nya e-mail plaintext dan hit kirim.
Rick menerima e-mail Roy dan menghasilkan SHA-1 hash nilai sendiri dari plaintext e-mail. Rick kemudian mendekripsi tanda tangan digital dengan RSA kunci publik Roy, memulihkan SHA-1 hash Roy dihasilkan. Rick kemudian membandingkan nya SHA-1 hash dengan Roy.

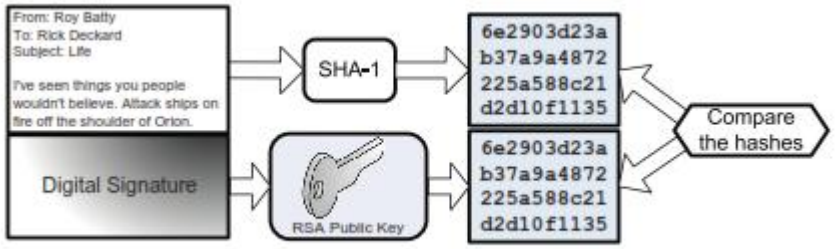


FIGURE 5.2

Gambar diatas menunjukkan proses.
Jika kedua hash cocok, Rick tahu beberapa hal:
1. Roy harus mengirim e-mail (hanya Roy tahu kunci pribadinya). Ini mengotentikasi Roy sebagai pengirim.
2. e-mail tidak berubah. Ini membuktikan integritas e-mail.
Jika hash cocok, Roy tidak bisa kemudian menyangkal telah menandatangani e-mail. Ini adalah nonrepudiation.
Jika hash tidak cocok, Rick yang tahu baik Roy tidak mengirimkannya atau integritas e-mail ini dilanggar.

- Public Key Infrastructure

Public Key Infrastructure (PKI) memanfaatkan semua tiga bentuk enkripsi untuk memberikan
dan mengelola sertifikat digital. Sebuah sertifikat digital adalah kunci publik ditandatangani dengan

tanda tangan digital. Sertifikat digital mungkin berdasarkan server atau client berbasis. Jika
dua digunakan bersama-sama, mereka menyediakan saling otentikasi dan enkripsi. standar
format sertifikat digital X.509.

- SSL and TLS

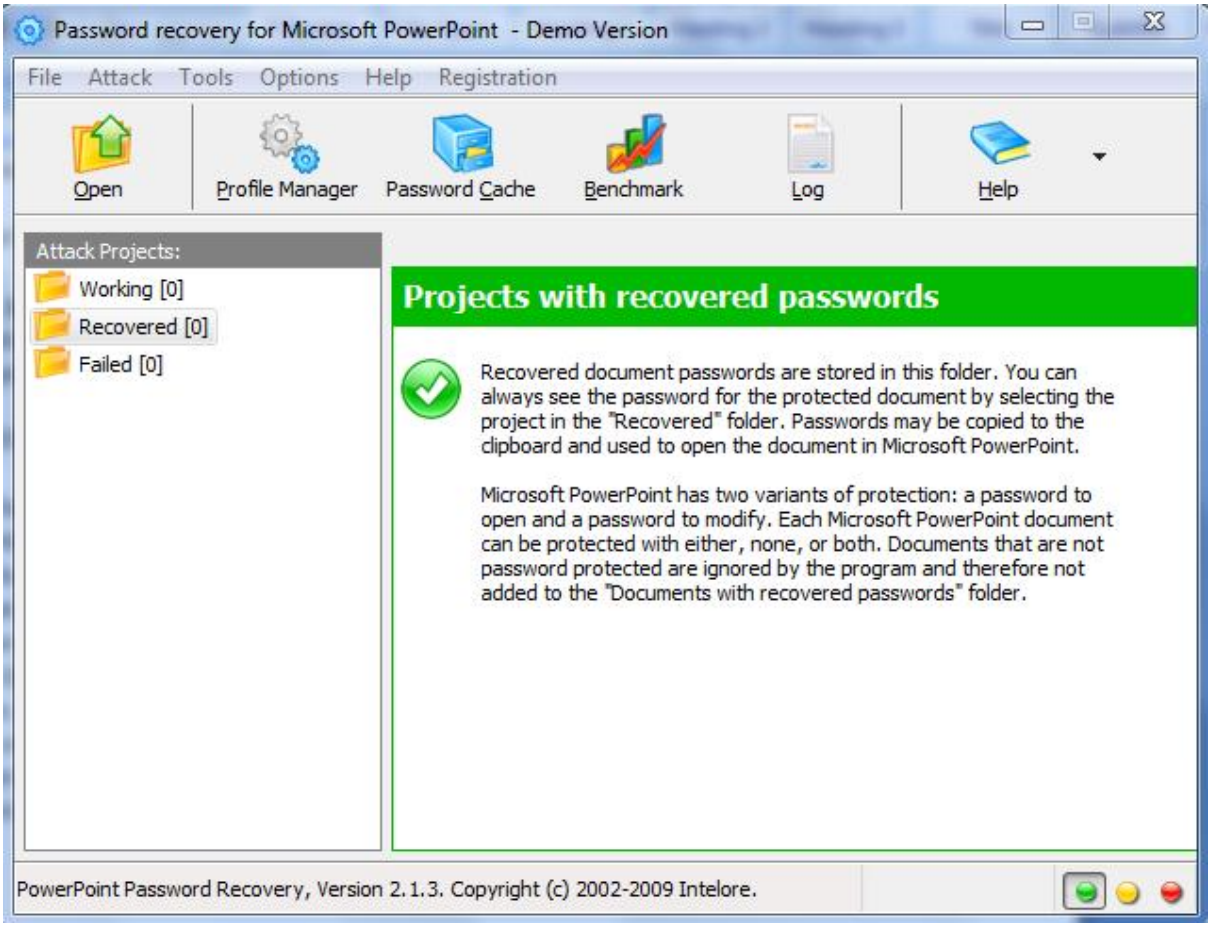
Secure Socket Layer (SSL) membawa kekuatan PKI ke Web. mengotentikasi SSL
dan menyediakan kerahasiaan untuk lalu lintas web. Transport Layer Security (TLS) adalah
penerus SSL. Mereka umumnya digunakan sebagai bagian dari HTTPS (Hypertext Transfer
Protocol Secure).
SSL dikembangkan untuk browser Web Netscape pada 1990-an. SSL 2.0 adalah
pertama kali dirilis versi; SSL 3.0 tetap sejumlah masalah keamanan dengan versi 2. TLS
didasarkan pada SSL 3.0. TLS sangat mirip dengan versi yang, dengan beberapa keamanan

perbaikan. Meskipun biasanya digunakan untuk HTTPS untuk mengamankan lalu lintas
Web, TLS mungkin
digunakan untuk aplikasi lain seperti Internet chatting dan e-mail server-server atau
akses klien.

Tugas 2

Cara menggunakan softwere power point password recovery.

1. Pertama kita buka softwere dan akan muncul seperti berikut



2.