

Nama : Fajar Surya Negara
NIM : 1310651159
Mata Kuliah : Keamanan Informasi
Kelas : TI-A

KRIPTOGRAFI

➤ Kriptografi

Kriptografi adalah menulis rahasia: komunikasi yang aman yang dapat dipahami oleh penerima yang dimaksud saja

➤ KONSEP KRIPTOGRAFI CORNERSTONE

Kriptologi adalah ilmu komunikasi untuk menyembunyikan pesan tersembunyi. Sebuah cipher adalah algoritma kriptografi. Sebuah plaintext adalah pesan terenkripsi. Enkripsi mengubah data asli ke kode tertentu. Dekripsi ternyata mengembalikan kode tersebut ke data yang asli (pesan asli)

➤ Kerahasiaan, integritas, otentikasi, dan nonrepudiation

Kriptografi dapat memberikan kerahasiaan.

Kriptografi dapat memberikan jaminan,

bahwa pengguna tertentu melakukan transaksi tertentu dan bahwa transaksi tidak tidak berubah dan pastinya aman.

➤ Pergantian dan permutasi

Substitusi kriptografi menggantikan satu karakter untuk lain

. Pergantian dan permutasi sering dikombinasikan.

➤ kekuatan kriptografi

Enkripsi yang baik adalah yang kuat untuk menyembunyikan pesan asli kedalam kode-kode dimana orang yang tidak di perkanankan sulit menerjemahkan pesan kriptografi tersebut.

➤ **Monoalphabetic dan cipher polyalphabetic**

Sebuah cipher monoalphabetic menggunakan satu huruf: huruf tertentu (seperti "E") diganti untuk lain (seperti "X"). Sebuah cipher polyalphabetic menggunakan beberapa huruf: "E" mungkin digantikan untuk "X" satu putaran dan kemudian "S" babak berikutnya. Cipher Monoalphabetic rentan terhadap analisis frekuensi. Polyalphabetic cipher berusaha untuk mengatasi masalah ini melalui penggunaan beberapa huruf

➤ **Jenis kriptografi**

- Enkripsi simetris

menggunakan satu kunci : mengenkripsi kunci yang sama dan mendekripsi.

jika Anda mengenkripsi dengan satu tombol. Salah satu kunci dapat dibuat publik (disebut kunci publik); asimetris enkripsi juga disebut enkripsi kunci publik . Siapa pun yang ingin untuk berkomunikasi dengan Anda mungkin cukup download kunci publik Anda diposting publik.

- Kriptografi asimetris

menggunakan dua kunci: jika Anda mengenkripsi dengan satu tombol, Anda mungkin mendekripsi dengan yang lain.

- Hashing adalah transformasi kriptografi satu arah menggunakan

algoritma (dan tidak ada tombol). Sebuah fungsi hash memberikan enkripsi menggunakan algoritma dan tidak ada tombol.

- Fungsi hash

terutama digunakan untuk menyediakan integritas. Fungsi hash yang lebih tua umum termasuk Secure Hash Algorithm 1 (SHA-1), yang menciptakan hash 160-bit dan Message Digest 5 (MD5), yang menciptakan hash 128-bit. Kelemahan telah ditemukan di kedua MD5 dan SHA-1.

➤ **SERANGAN KRIPTOGRAFI**

Serangan kriptografi digunakan oleh cryptanalysts untuk memulihkan plaintext tanpa kunci. tidak ketika berhadapan dengan tersangka menggunakan kriptografi : mereka mendapatkan surat perintah pencarian dan mencoba untuk memulihkan kunci.

- Brute force

Sebuah serangan brute-force menghasilkan seluruh keyspace, yang setiap kunci yang mungkin. Mengingat waktu yang cukup, plaintext akan pulih

- Known Plaintext

Known Plaintext bertujuan untuk mendapatkan kunci yang digunakan. Anda mungkin bertanya-tanya mengapa Anda perlu kunci jika Anda sudah memiliki plaintext: memulihkan kunci akan memungkinkan Anda untuk mendekripsi ciphertexts lainnya yang dienkripsi dengan kunci yang sama.

- Chosen plaintext and adaptive-chosen plaintext

Tujuannya adalah untuk mendapatkan kunci. Enkripsi tanpa mengetahui kunci dilakukan melalui "enkripsi oracle" atau perangkat yang mengenkripsi tanpa mengungkapkan kunci.

- Meet-in-the-middle attack

Sebuah serangan-bertemu-di-tengah mengenkripsi di satu sisi, mendekripsi di sisi lain, dan bertemu di tengah. Serangan yang paling umum adalah melawan "ganda DES," yang mengenkripsi dengan dua tombol di "mengenkripsi, mendekripsi" order. Serangan itu adalah plaintext diketahui Serangan: penyerang memiliki salinan dari plaintext pencocokan dan ciphertext dan berusaha untuk memulihkan dua kunci yang digunakan untuk mengenkripsi.

- Differential cryptanalysis

Kriptanalisis diferensial berusaha untuk menemukan "perbedaan" antara plaintext terkait yang dienkripsi. The plaintexts mungkin berbeda dengan beberapa bit. Hal ini biasanya diluncurkan sebagai serangan plaintext adaptif yang dipilih: penyerang memilih plaintext yang akan dienkripsi (tapi tidak tahu kunci) dan kemudian mengenkripsi plaintexts terkait.

- Linear cryptanalysis

Kriptanalisis linear adalah serangan plaintext diketahui mana cryptanalyst menemukan besar jumlah plaintext pasang / ciphertext dibuat dengan tombol yang sama. Pasangan yang dipelajari untuk memperoleh informasi tentang kunci yang digunakan untuk membuat mereka.

Kedua analisis diferensial dan linear dapat dikombinasikan sebagai linear diferensial

analisis.

- Side-channel attacks

Serangan side-channel menggunakan data fisik untuk memecahkan kriptografi, seperti pemantauan Siklus CPU atau konsumsi daya yang digunakan saat mengenkripsi atau mendekripsi.

➤ **IMPLEMENTING CRYPTOGRAPHY**

- Tanda tangan digital

digunakan untuk dokumen tanda kriptografi. Tanda tangan digital memberikan nonrepudiation, yang mencakup otentikasi identitas penandatanganan dan bukti integritas dokumen (membuktikan dokumen tidak berubah). Ini berarti pengirim tidak dapat menolak.

- 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.

- Certificate Authorities and Organizational Registration Authorities.



Sertifikat digital yang dikeluarkan oleh Otoritas Sertifikat (CA). Pendaftaran organisasi Pihak berwenang (Oras) mengotentikasi identitas pemegang sertifikat sebelum menerbitkan sertifikat kepada mereka. Sebuah organisasi dapat bertindak sebagai CA atau ORA (atau keduanya).

Dan masih banyak lagi implementing cryptography lainnya.







Tugas UAS ke 2

Bagaimana cara Menyembunyikan pesan txt di sebuah gambar ?
Bagaimana menampilkan pesan yang tersembunyi?

Disini saya menggunakan aplikasi **stegomagic**, aplikasi bertujuan untuk menyembunyikan sesuatu dan menampilkan sesuatu yang tersembunyi.

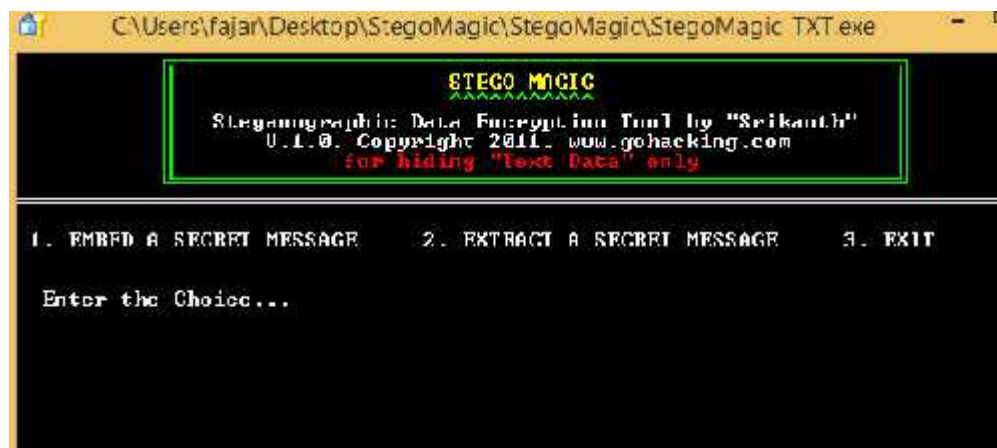
 StegoMagic_BIN	27/10/2011 22:00	Application	139 KB
 StegoMagic_TXT	27/10/2011 22:00	Application	139 KB

Langkah pertama untuk menyembunyikan *.txt di dalam gambar menggunakan stegomagic adalah dengan menempatkan dua file *.txt dan gambar pada satu folder pada stegomagic.exe

 jpg	30/06/2015 21:35	File folder	
 Instructions	28/10/2011 0:07	Text Document	2 KB
 joker	30/06/2015 21:36	PNG image	323 KB
 pesan	30/06/2015 21:30	Text Document	1 KB
 StegoMagic_BIN	27/10/2011 22:00	Application	139 KB
 StegoMagic_TXT	27/10/2011 22:00	Application	139 KB

Disini saya mempunyai file gambar joker.png dan text pesan.txt.

- Kemudian buka aplikasi Stegomagic_txt.exe



Menu 1 > untuk menyembunyikan pesan yang akan disembunyikan
2 > untuk menampilkan pesan yang disembunyikan

Pilih menu 1, kemudian ketik joker.png

```

                                STEGO MAGIC
                                ~~~~~
Steganographic Data Encryption Tool by "Srikanth"
0.1.0. Copyright 2011. www.gohacking.com
for hiding "Text Data" only

1. EMBED A SECRET MESSAGE      2. EXTRACT A SECRET MESSAGE      3. EXIT

Enter the Filename in Which You Want to Embed the Secret Message
joker.png

Enter the Filename Containing the Secret Message (*.txt)
pesan.txt
```

Kemudian ketik lagi pesan.txt dan tekan enter.

```

                                STEGO MAGIC
                                ~~~~~
Steganographic Data Encryption Tool by "Srikanth"
0.1.0. Copyright 2011. www.gohacking.com
for hiding "Text Data" only

1. EMBED A SECRET MESSAGE      2. EXTRACT A SECRET MESSAGE      3. EXIT

Enter the Filename in Which You Want to Embed the Secret Message
joker.png

Enter the Filename Containing the Secret Message (*.txt)
pesan.txt

Embedding Completed Successfully!

Your Secret Key for Decryption is 26

Press Any Key to Continue...
```

Setelah benar saya akan mendapatkan angka kunci deskripsi.

File Name	Date Modified	Type	Size
jpg	30/06/2015 21:35	File folder	
Instructions	28/10/2011 0:07	Text Document	2 KB
joker	30/06/2015 21:52	PNG image	323 KB
SecretKey	30/06/2015 21:52	Text Document	1 KB
StegoMagic_BIN	27/10/2011 22:00	Application	139 KB
StegoMagic_TXT	27/10/2011 22:00	Application	139 KB

Di folder stegomagic saya menghapus pesan.txt dimana isi file tersebut disembunyikan pada joker.png.

- untuk mengetahui pesan rahasia yang menggunakan stegomagic dengan cara buka kembali stegomagic_txt.exe kemudian pilih menu 2



Dan Tekan enter



Kemudian Masukkan kunci deskripsi yang di dapat tadi

```

                                STEGO MAGIC
                                ~~~~~
Steganographic Data Encryption Tool by "Srikant"
V.1.0. Copyright 2011. www.gohacking.com
for hiding "Text Data" only

1. EMBED A SECRET MESSAGE      2. EXTRACT A SECRET MESSAGE

Enter the Filename that You Want to Decrypt
joker.png

Enter the Secret Key for Decryption
26

Message Decryption Completed Successfully!

Output File is: MM_SecretMessage.txt

Press Any Key to Continue...

```

Dan di folder stegomagic akan mendapatkan MM_SecretMessage.txt dimana file tersebut memuat pesan rahasia yang telah disembunyikan



Mungkin hanya itu yang bisa jelaskan.Sekian dan Terimah Kasih