Penggunaan Kriptografi dalam Keamanan Suatu Jaringan Komputer

William Juniarta Hadiman - 13516026
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
13516026@std.stei.itb.ac.id

***Abstraksi*—Makalah ini akan membahas tentang suatu teknik yang berguna untuk mengamankan suatu pesan, yaitu Kriptografi, pada suatu jaringan komputer. Saat suatu komputer memiliki data-data pribadi, dan komputer tersebut terhubung ke dalam suatu jaringan, maka perlu sebuah sistem yang dapat mengamankan data-data di dalam komputer tersebut agar orang luar tidak dapat mengakses data tersebut sembarangan. Apalagi jaman sekarang penggunan komputer sudah semakin maju, sehingga para oknum kejahatan sudah lebih membidik sasarannya dengan menggunakan berbagai cara.**

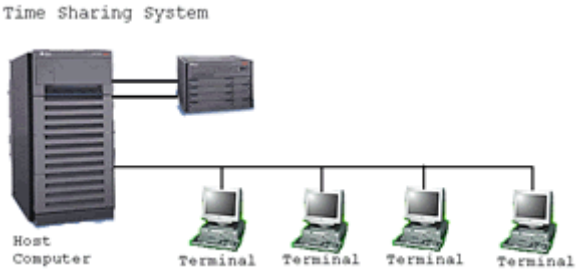
***Kata kunci*—kriptografi, keamanan komputer, sistem keamanan jaringan komputer, menjaga data suatu komputer**

I. PENDAHULUAN

Gambar 1. Berbagai jenis komputer sudah digunakan banyak orang bahkan sejak dini (sumber : https://kusumakencana.files.wordpress.com/2014/02/anak-main-hp.jpg)

Jaman sekarang tidak dapat dipungkiri bahwa suatu komputer adalah salah satu kebutuhan pokok dari masyarakat, mulai dari anak-anak yang membuat tugas sekolahnya, mahasiswa yang membuat tugas dan makalah dari universitasnya, maupun orang-orang yang sudah bekerjapun tetap harus menggunakan komputer sebagai tempat mengolah data-data yang diperlukan untuk perusahaannya.

Seiring berjalannya waktu, manusia mencoba mencari cara memanfaatkan suatu perangkat komputer dan menggunakan perangkat tersebut secara besamaan. Kemudian ada seorang peneliti di laboratorium di *Harvard University* mencobanya dan kemudian berhasil. Ini adalah suatu langkah awal suatu jaringan komputer.



Gambar 2. Bentuk Jaringan Pertama Kali (sumber : http://fadel05.tripod.com/network/jaringan.html)

Tetapi, ada suatu masalah yaitu ketika penggunaan jaringan ingin tetap dilakukan, namun diinginkan adanya pembatasan akses untuk beberapa hal. Maka, dibuatlah suatu enkripsi menggunakan kriptografi untuk membatasi akses agar hanya orang tertentu yang dapat mengakes data yang dibatasi tersebut.

II. DASAR TEORI

A. Apa itu kriptografi?

Kriptografi secara garis besar didefinisikan sebagai suatu ilmu yang mempelajari cara menjaga suatu pesan data tetap aman terkirim sehingga pihak ketiga tidak akan mengetahui isi dari pesan tersebut.

Ada banyak definisi kriptografi didefinisikan oleh beberapa ahli. Salah satunya Bruce Scheiner dalam bukunya "Applied Cryptography", menuliskan kriptografi adalah ilmu pengetahuan dan seni menjaga message tetap aman (secure). Kemudian ia juga menuliskan, secara umum kriptografi itu sendiri adalah ilmu dan seni untuk menjaga kerahasiaan suatu berita. Ia juga menuliskan ada pengertian lain, yaitu pengertian ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, sebagai contoh, keabsahan data, integritas data, serta autentikasi data (definisi oleh A. Menezes, P. van Oorshot, dan S. Vanstone. Dituliskan juga tidak semua aspek keamanan suatu jaringan komputer ditangani oleh kriptografi.

B. Mengapa Kriptografi digunakan untuk aspek keamanan suatu jaringan komputer?

Ada beberapa alasan kriptografi digunakan untuk mengamankan suatu data dalam jaringan, yaitu :

1. Rahasia

Semua sandi dari suatu kriptografi dapat menjaga isi informasi dari siapapun kecuali orang yang memiliki sandi tersebut untuk melihat informasi yang telah dikunci tersebut.

2. IntegritasData
   kriptografi berhubungan dengan penjagaan daripada perubahan data secara tidak sah oleh orang ketiga. Untuk menjaga integritas data, sistem harus bisa mendeteksi manipulasi data oleh orang pihak ketiga, seperti penysipan, penghapusan, dan pensubsitusian data lain kedalam data yang sebenarnya.

3. Autentikasi
   Berhubungan dengan identifikasi atau pengenalan. Dua pihak yang saling berkomunikasi harus saling memerkenalkan diri Hal ini untuk mengecek keaslian, isi datanya, waktu pengiriman, dll.

4. Non-repudasi
   Usaha mencegah terjadinya penyangkalan terhadap terciptanya suatu informasi.

C. *Istilah yang Digunakan Dalam Kriptgrafi*

Gambar 3. Proses Kriptografi (sumber : http://2we26u4fam7n16rz3a44uhbe1bq2.wpengine.netdna-cdn.com/wp-content/uploads/071114_1013_WindowsCryp2.jpg)

Berikut adalah beberapa istilah saat akan menggunakan kriptografi. Diantaranya :

- Plaintext (M) : Pesan yang ingin dikirimkan.
- Chipertext (C) : Pesan yang sudah ter-*encript* yang merupakan suatu hasil enkripsi
- Enkripsi (E) : Proses mengubah plaintext (M) menjadi chiptertext (C).
- Dekripsi (D) : Proses mengubah chipertext(C) menjadi plaintext(M).

D. Karakteristik kriptografi yang baik

Berikut adalah karakteristik dari suatu kriptosistem yang baik:

- Kemanan kriptogafi terletak pada kerahasiaan kunci bukan pada kerahasiaan algoritma kriptografinya.
- Memiliki ruang kunci yang besar.
- Menghasilkan chipertext yang terliat acak dalam seluruh tes statistik yang digunakan pada teknik kriptografi tersebut.
- Mampu menahan semua serangan yang telah dikenal sebelumnya.

E. Macam Kriptosistem

1. KriptosistemSimetrik
   Dalam bentuk ini, kunci pada proses enkripsi dan dekripsi pada prinsipnya identik, tetapi satua buah kunci dapat di turunkan dari kunci lainnya. Kunci tersebut harus dirahasiakan. Bentuk ini disebut juga sebagai *secret-key ciphersystem*. Contoh dari sistem ini adalah Data Encryption Standard (DES), Blowfish, dan IDEA.

2. Kriptosistem Asimetrik
   Dalam bentuk ini, digunakan 2 buah kunci yang pertama disebut kunci publik karena dapat dipublikasikan. Yang kedua disebut kunci privat, karena harus dirahasiakan. Contoh dari sistem ini adalah *RSA Scheme* dan *Merkle-Hellman Scheme.*

F. Kriptosistem pada Protokol

Ada beberapa protokol yang menggunakan kriptografi untuk mencegah *eavesdropping* ataupun *cheating.* Ada beberapa jenis penyerangan yang biasanya dilakukan untuk menyerang suatu protokol diantaranya :

1. Chipertext-only Attack
   Seorang penyerang yang meiliki chipertext dari sejumlah pesan yang seluruhnya telah dienkripsi menggunakan algoritma yang sama.

2. Known-plaintext attack
   Seorang penyerang tidak hanya memiliki akses terhadap chipertect suatu pesan, namun ia juga memiliki plaintext pesan tersebut.

3. Chosen-plain atack.
   Penyerang tidak hanya memiliki akses chipertext dan plaintext untuk beberapa pesan, tetapi juga dia dapat memilih plaintext yang dienkripsi.

4. Adaptive-chosen-plaintext attack.
   Bentuk khasus khusus dari Chosen-plaintext attack. Tidak hanya dapat memilih paintext yang dienkrips, ia juga dapat memodifikasi pilihan berdasarkan hasil enkripsi sebelumya.

5. Chosen-chipertext attack.
   Penyerang dapat memilih chipertext yang berbeda untuk didekripsi dan memiliki akses untuk plaintext yang didekrpsi.

6. Chosen-key attack.
   Penyerang memiliki pengetahuan tentang hubungan antasa kunci yang berbeda.

7. Rubber-hose cryptanalys.
   Penyerang akan mengancam, memeras, dll hingga mereka memberikan kuncinya.

F. Jenis Penyerangan pada jalur komunikasi

Ada beberapa jenis penyerangan yang berada pada jalur kommunikasi diantaranya adalah :

1. Sniffing.
   Penyerang merekam pembicaraan apa saja yang terjadi pada pesan yang tidak erenkripsi

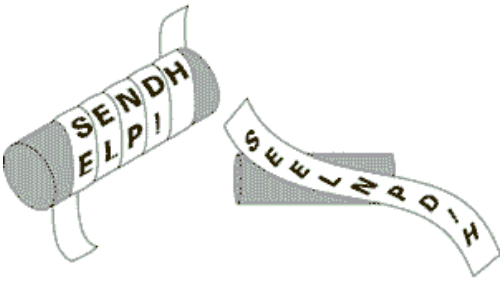
2. Replay attack.
   Jika seseorang merekam pesan-pesan *handshake*(persiapan komunikasi), ia dapat mengulang pesan tersebut dan digunakan untuk menipu salah satu pihak.

3. Spoofing.
   Membuat suatu prototype palsu. Dan orang yang ditipu akan dbuat percaya dengan prototype tersebut. Kemudian akhirnya penipu dapat mendapatkan data yang diinginkannya.

4. Man-in-the-middle
   Melakukan spoofing namun 2 arah.

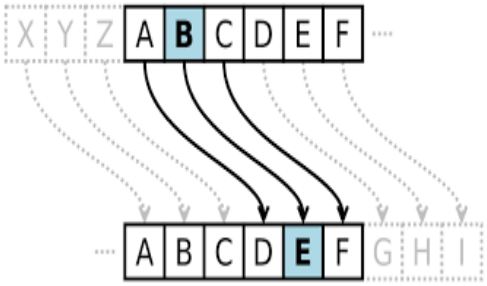
G. Metode Kriptografi

1. Metode Kuno
   - Pada tahun 475 S.M. bangsa sparta(bangsa jaman yunani kuno) menggunakan teknik kriptografi yang disebut scytale. Scytale ini digunakan untuk kepentingan berpetang. scytale ini terbuat dari tongkat dengan papyrus yang mengelilinginya secara spiral (seperti kertas panjang yang mengelilingi pensil). Kunci dari scytale ini adalah diameter tongkat harus sama antara mengirim dan penerima sehingga saat digulungkan kertas papyrus tersebut, penerima pesan dapat mengetahui apakah arti dari pesan tersebut.



Gambar 2. Bentuk Sytale (sumber : https://i2.wp.com/indiatechlaw.com/wp-content/uploads/2017/02/scytale-1.png?ssl=1)

   - Pada tahun 60 S.M. seorang kaisar terkenal Romawi yang bernama Julius Caesar menggunakan suatu teknik kriptografi yang sekarang disebut caesar chiper. Teknik yang diguakan adalah mensubtitusikan alfabet secara berurutan dengan ketiga yang mengikutinya. Misalkan alfabet "A" digantikan oleh "D", kemudian "B" digantikan oleh "E", dst



Gambar 3. Caesar Chiper (sumber : http://www.geeksforgeeks.org/wp-content/uploads/Caesar-Cipher-3.png)

2. Teknik Dasar Kriptografi
   - Subtitusi
     Teknik subtitusi mengubah pesan yang ingin di encript dengan membandingkannya dengan tabel subtitusi. Tabel subtitusi dapat dibuat sendiri sesuka hati asalkan penerima memiliki tabel yang sama sehingga bisa kembalkan kembali ke bentuk asal dari bentuk chipertextnya.
   - Blocking
     Teknik ini membagi plaintext menjadi beberapa block dan kemudian dienkripsikan secara independen.

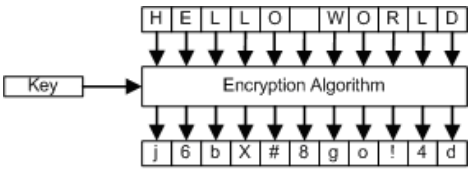
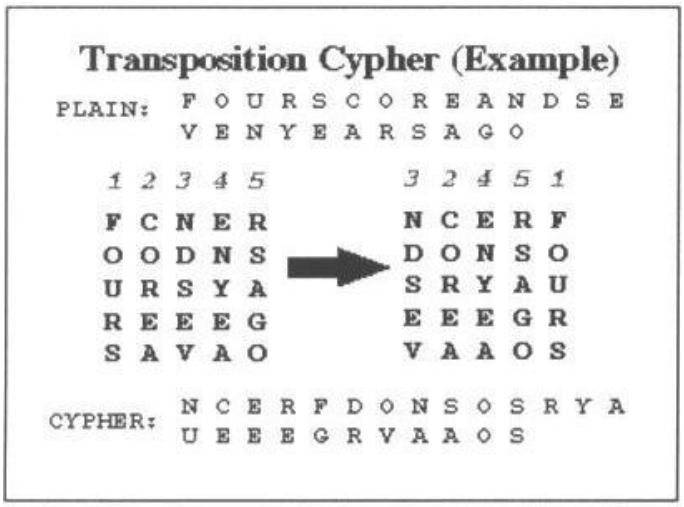


Diagram 2. Block Cipher

Gambar 4.. Block Chiper (sumber : https://www.codeproject.com/KB/security/crypto/crypto3.gif)



Gambar 5. Permutation Chiper (sumber : http://bestcodes.weebly.com/uploads/2/0/1/9/20195317/_2920461_orig.jpg)

- Permutasi
  Teknik ini emiliki kemiripan dengan teknik subtitusi, perbedaannya hanya pada letak pengacakannya. pada subtitusi, kita mengubah nilai dari hal yang kita acak tersebut. namun pada permutasi, kita mengubah urutan daripada pesan yang kita akan sampaikan.

H. APLIKASI ENKRIPSI

1. Jasa telekomunikasi

Gambar 5. Telekomunikasi (sumber : http://2.bp.blogspot.com/--Fni5gGMqUE/UZI0EERpjxI/AAAAAAAAAmc/tUgZXrfh5XA/s1600/Cover.jpg)

   - Enkripsi untuk mengamankan pesan suata, gambar, dll yang akan dikirimkan ke lawan bicaranya.
   - Enkripsi pada transfer data untuk keperluan manajemen jaringa
   - Transfer data online billing
   - Enkripsi menjaga copyright dari informasi yang diberikan.

2. Militer dan Pemerintahan
   - Enkripsi dalam mengirimkan pesan pemeriintahan
   - Menyimpan data rahasia militer dan pemerintahhan yang tidak boleh diketahui sama sekali oleh orang luar.

3. Data Perbankan
   - informasi personal dalam bank tidak boleh disebarkan ke orang lan
   - pengaksesan uang pada mesin ATM
   - informasi transfer uang antar bank

4. Data Konfidensial perusahaan
   - Rencana strategis, formula-formula produk, basis data pelanggan/karyawan dan basis data operasional
   - pusat penyimpanan data perusahaan
   - melindungi data dari pembacaan maupun perubahan yang tak sah.

5. Pengamanan electronic mail
   - Mengamankan pada saat ditransisikan maupun dalam media penyimpanan
   - mengamankan email diantaranya PEM(Privacy Enhanced Mail) dan PGP(Pretty Good Privacy), dengan keduanya berbasis DES dan RSA.

6. Kartu Plastik

Gambar 6. Enkripsi pada SIM CARD (sumber : http://images.wisegeek.com/sim-card-yellow.jpg)

   - Enkripsi pada SIM Card, kartu telepon umum, kartu langganan TV kalel, kartu kontrol akses ruangan dan komputer, kartu kredit, dll.

III. ANALISIS PERSOALAN

Untuk keamanan komputer ketika online, maka kriptografi haruslah bekerja dan memberikan rasa aman kepada pengguna jaringan. Maka ada beberapa solusi yang ditawarkan yaitu enkripsi modern, diantaranya :

1. Data Encryption Standard (DES)
   - digunakan sebagai standar di USA Government
   - didukung ANSI dan IETF
   - untuk metode secret key, ia cukup populer
   - terdiri dari : 40 bit, 56 bit, dan 3x56 bit (triple DES)

2. Advanced Encryption Standard (AES)
   - Launching tahun 2001
   - Menggantikan DES
   - menggunakan variable length block chiper
   - panjang kata : 128 bit, 192 bit, 256 bit
   - dapat digunakan untuk smart card

3. Digital ertificate Server (DCS)
   - untuk vervikasi digital signature
   - untuk mengautentikasi pengguna
   - menggunakan 2 maca key yaitu public dan private
   - contoh : Netscape Certificate Server

4. IP Security (IPSe)
    - mengenkripsi public / priate key
    - perancangnya CISCO System
    - menggnakan DES 40 bit
    - menggunakan autentikasi
    - built-in pada produk CISCO
    - cocok untuk Virtual Private Network(VPN) dan Remote Network Access

5. Kerberos
    - Solusi untuk autentikasi pengguna
    - dapat menangani multiple system atau multiple platform
    - open source

6. Point to point tunneling protocol (PPTP), Layer Two Tunneling Protool (L2TP)
    - dirancang oleh microsoft
    - autentication berdasarkan PPP (point to point protocol)
    - enkripsi berdasarkan algoritma Microsoft (tidak open source)
    - terintegrasi dengan NOS Microsoft(NT,2000,XP).

7. Remote Access Dial in User Service (RADIUS)
    - multiple remote access device
    - menggunakan 1 database untuk autentikasi
    - didukung oleh 3com, CISCO, dan Ascend
    - tidak menggunakan enkripsi

8. RSA Encryption
    - Dirancang oleh Rivest, Shamir, Adleman tahun 1977
    - standar secara fakta dalam enkripsi publik atau private
    - didukung oleh Microsoft, apple, novell, sun, dan lotus
    - mendukung proses autentikasi
    - multi platform

9. Secure Hash Algorithm (SHA)
    - dirancang oleh National Institute of Standard and Technology(NIST) USA
    - bagian dari standar DSS (Decision Support System) USA dan bekerja sama dengan DES untuk digital signature
    - SHA-1 menyediakan 160-bit message digest
    - Versi : SHA-256, SHA 384, SHA-512
    - Berintegrasi dengan AES

10. MD5
    - dirancang oleh Prof. Robert Rivest (RSA,MIT) pada thaun 1991
    - menghasilkan 128 bit digest
    - cepat tapi kurang aman

11. Secure shell(SSH)
    - digunakan untuk client side autentikasi antara 2 sistem
    - mendukng UNIX, windows, OS/2
    - melindungi telnet dan ftp (file transfer protocol)

12. Secure Socket Layer (SSL)
    - dirancang Netscape
    - menyediakan enkripsi RSA pada layer session dari model OSI.
    - bebas terhadap service yang ada
    - melindungi sistem secure web e-commerce
    - metode publik atau private key dan dapat melakukan autentiasi
    - terintegrasi dalam produk browser dan web server Netscape.

13. Security Token
    - aplikasi penyimpanan password dan data user di smart card

14. Simple Key Management for Internet Protocol
    - seperti SSL bekerja pada leve session model OSI
    - menghasilkan key yang static, mudah bobol.

IV. KESIMPULAN

Ada banyak kriptografi modern yang dipakai dalam pengamanan jaman sekarang, namun tidak semua pengamanan efektif dalam menangani setiap kasus. Sehingga kita harus memilih teknik enkripsi yang paling optimal untuk mengatasi kasus yang diperlukan.

REFERENCES

[1] http://fadel05.tripod.com/network/jaringan.html# Diakses pada tanggal 3 Desember 2017 pukul 12.24

[2] http://ditonugroh08.blogspot.co.id/2012/09/keamanan-jaringan-komputer-menggunakan.html Diakses pada taggal 3 Desember 2017 pukul 12.15

[3] http://muhammad-ikhsan74.blogspot.co.id/2012/05/pengertian-kriptografi.html Diakses pada tanggal 3 Desember 2017 pukul 12.30

[4] http://asalkena.blogspot.co.id/2012/11/pengertian-dan-contoh.html Diakses pada tanggal pada tanggal 3 Desember 2017 pukul 12. 35

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 3 Desember 2017

William Juniarta Hadiman - 13516026