Kriptografi dan Sistem Keamanan Bank

Raihan Maulana Warman 13514076[1]
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
raihanwarman@s.itb.ac.id

Abstrak- *Pada makalah ini akan dibahas mengenai penerapan ilmu dan teknik kriptografi dalam sistem perbankan. Seperti yang kita ketahui bahwa seiring berkembangnya zaman, maka kebutuhan dan aktifitas pun juga terus meningkat. Oleh karena itu dibutuhkan juga sistem pengelolaan uang yang baik. Bank yang mengemban tugas untuk menjaga dan memfasilitasi segala proses yang berkaitan dengan uang harus memiliki sistem yang efisien untuk keperluan tersebut. Bank juga membutuhkan sistem keaman yang baik untuk memproteksi segala bentuk kegiatan bank dari kejahatan-kejahatan yang ditakutkan akan merugikan banyak pihak. Oleh karena itu bank mulai mengembangkan suatu sistem keamana berbasis cyber untuk memproteksi segala bentuk kejatahatan yang berasal dari dunia cyber. Maka dikembangkanlah suatu Teknik Kriptografi yang dikhususkan untuk sistem keamanan bank.*

***Keywords*—Algoritma, Bank, Keamanan, Kriptografi.**

I. PENDAHULUAN

Dewasa ini, Zaman sudah semakin berkembang sehingga manusia diharuskan untuk melaksanakan segala sesuatunya dengan lebih cepat dan lebih baik. Hal ini diharuskan karena kegiatan manusia yang sangat banyak dan beragam sehingga dibutuhkan kerja yang cepat dan efisien agar semua perkejaan dan kewajiban kita dapat terlaksana. Untuk mengimbangi kebutuhan manusia yang sangat banyak dan beragam itu, maka dikembangkanlah teknologi yang diharapkan dapat memudahkan kita dalam melaksanakan aktivitas sehari-hari. Dampak dari teknologi ini pun juga semakin terasa seiirng perkembangannya yang sangat pesat. Banyak penemuan-penemuan baru yang muncul setiap tahunnya.

Salah satu contoh pemanfaatan teknologi yang paling banyak dimanfaatkan oleh manusia adalah sistem pembayaran yang dilaksanakan secara online. Kemudahan dalam pembayaran secara online ini menyebabkan sirkulasi uang yang terjadi sangatlah cepat oleh karena itu, Bank selaku badan penegelola keungan yang resmi harus menciptakan sistem yang baik, aman dan efisien untuk memfasilitasi, mengawasi dan memproteksi perputaran uang yang sangat cepat ini agar tidak terjadi kejahatan-kejahatan yang dapat merugikan banyak pihak.

Agar kejahatan-kejahatan tersebut dapat dihindarkan, maka bank juga harus memiliki sistem keamanan yang sangat baik sehingga para penjahat baik itu penjahat cyber atau bukan tidak bisa mengganggu aktivitas dari bank itu sendiri. Khusus untuk proteksi terhadap kejahatan cyber, bank mengimplementasikan ilmu-ilmu yang dipelajari dalam bidang kriptografi. Karena ilmu kriptografi adalah ilmu yang mempelajari matematika yang bertujuan untuk menjaga aspek-aspek keamanan informasi seperti kerahasiaan data, keabsahan data, autentikikasi data dan integritas data (Menezes, 1996).

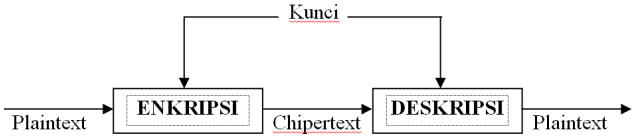
II. DESKRIPSI KRIPTOGRAFI

2.1 Pengertian Kriptografi

Kriptografi terdiri dari kata *Kriptos* dan *Graphia*. Kriptos berarti sesuatu yang dirahasiakan, sedangkan Graphia berarti tulisan. Oleh karena itu Kriptografi secara bahasa berarti tulisan yang dirahasiakan.

Sedangkan secara umum, kriptografi berarti adalah ilmu dan seni untuk menjaga kerahasiaan suatu berita. Menurut A. Menezes dalam bukunya yang berjudul Handbook of Applied Chryptography menyebutka bahwa kriptografi adalah teknik matematika yang berhubungan dengan aspek keamanan seperti kerahasiaan data, keabsahan data, integritas data dan keabsahan data.

Dalam menjaga kerahasiaan data, kriptografi mentransformasikan data jelas (data yang dapat dimengerti semua orang) yang disebut juga dengan *Plainteks* menjadi data yang telah disandikan yang disebut dengan *Chiperteks*. Proses mengubah data Plainteks ke Chiperteks disebut dengan *Enkripsi* sedangkan proses mengubah data Chiperteks ke bentuk Plainteks disebut dengan *Dekripsi*.



Gambar disadur dari 1.bp.blogspot.com

2.2 Sejarah Kriptografi

Kriptografi ternyata sudah ada sejak zaman dahulu kala. Pada awalnya, tujuan dari kriptografi ini hanyalah untuk merahasiakan pesan-pesan penting. Yaitu proses merngubah suatu pesan dari bentuk yang dapat dibaca dan diketahui semua orang menjadi bentuk yang hanya diketahui segelintir orang. Kriptografi yang paling sering digunakan dulu disebut dengan *Sandi Transposisi,* yaitu tekni enkripsi pesan dengan cara mengatur aturan huruf pada pesan. Huruf di subtitusi dengan huruf lain yang berjarak beberapa huruf sesuai dengan aturan aplhabet. Contohnya yaitu kalimat “Fly at Once” di enkripsikan menjadi “gmz bu podf”. Teknik Enkripsi ini dulu sering digunakan seorang Kaisar Romawi bernama Julius Caesar untuk ber komunikasi dengan jenderal-jenderak nya secara rahasia. Sedangkan di Yunani Kuno, mulai berkembang juga ilmu kriptografi yang disebut dengan *Steganografi* yang berarti menyembunyikan kehadiran pesan sehingga pesan

tersebut hanya dapat dilihat oleh orang tertentu. Steganografi inilah yang menginspirasi penggunaan tinta tak tampak, mikrodot, dan tanda air digital untuk menyembunyikan Informasi pada dunia modern.

Enkripsi diatas tergolong mudah dipecahkan jika seseorang sudah mengetahui pola dari kriptografi tersebut. Oleh karena itu pada Abad ke-9 soerang ilmuwan dan ahli matematika dan Arab yang bernama Al-Kindi mengembangkan teknik enkripsi baru menggunakan teknik analisis frekuensi. Muncul juga istilah *Kriptanalisis* yang juga menggunakan teknik analisis frekuensi untuk memecahkan pesan yang telah di enkripsi.

2.2 Tujuan Kriptografi

Menurut Kurniawan J. dalam bukunya yang berjudul *Keamanan Internet dan Jaringan Komunikasi* Kriptografi memiliki empat tujuan dasar yaitu :

- Kerahasiaan Data, adalah layanan yang digunakan untuk menjaga isi dari informasi dari siapapun kecuali yang memiliki otoritas atau yang memiliki kunci untuk mengakses informasi tersebut.
- Integritas Data, bertujuan untuk menjaga agar data tidak dapat diubah oleh sembarang orang atau data diubah secara tidak sah. Oleh karena itu sistem harus memiliki kemampuan untuk mendeteksi tindakan manipulasi data oleh pihak-pihak nakal. Contoh dari manipulasi data adalah Penyisipan, Subtitusi data, panghapusan data.
- Autentikasi, yang bertujuan untuk mengautentikasi setiap proses yang terjadi. Setiap proses seperti waktu pengiriman, identitas user bahkan keabsahan informasi juga harus si autentikasi terlebih dahulu.
- Non-Repudiasi, yaitu usaha untuk mencegah terjadinya penyangkalan terhadap proses pengiriman atau terciptanya suatu informasi yang berasal dari user.

III. KRIPTOGRAFI FINANSIAL

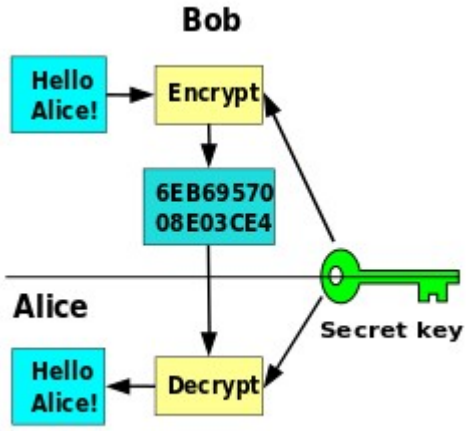
Untuk meingkatkan sistem keamanan dari suatu bank, maka dikembangkan Ilmu Kriptografi dengan algoritma yang memang dirancang khusus untuk keamanan bank. Kriptografi tersebut dinamakan kriptografi finansial.

Pada dasarnya, Kriptografi Finansial banyak menggunakan Teknik kriptografi Simetri dan Asimetri

3.1 Teknik Kriptografi Simetri

Hingga tahun 1976, hanya ada satu jenis teknik kriptografi yang diketahui orang. Yaitu teknik kriptografi Simetri. Teknik Krptografi Simetri merupakan metode enskripsi dimana kedua belah pihak baik itu pengirim dan penerima memiliki kunci untuk meng-enkripsi dan men-dekripsi pesan yang dikirim. Oleh karena penerima dan pengirim pesan berbagi kunci yang sama, maka kedua belah pihak itu harus saling mempercayai untuk berbagi kunci enkripsi-dekripsi yang sama.

Sedangkan untuk enkripsi tingkat tinggi, seperti pengiriman e-mail. Chiper kunci simetris diimplementasikan secara chiper blok maupun chiper steam.



Gambar disadur dari

Sedangkan Algoritma yang dipakai untuk teknik Kriptografi Simetri ini adalah

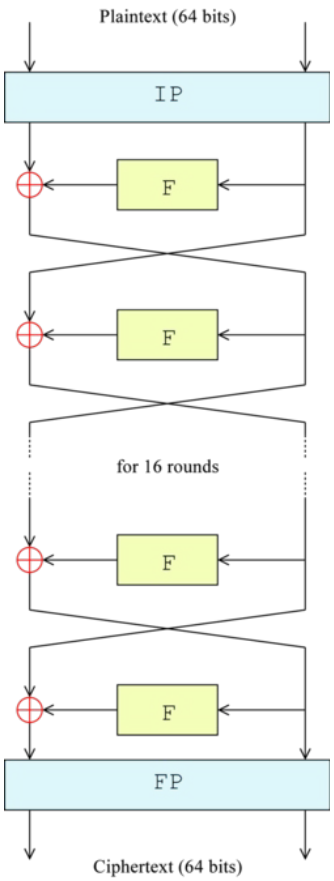
3.1.1 Data Encyption Standard (DES)

Data Encryption Standard adalah desain chiper blok yang dijadikan bahan rujukan sebagai standar kriptografi. Algoritma Data Encryption Standard merupakan algoritma enkripsi pertama yang dikembangkan. Pencetusan ide untuk membuat Data Encryption Standard ini pada awalnya disebabkan karena Amerika Serikat membutuhkan sistem keamanan komputer dan juga karena kebutuhan pemerintah Amerika Serikat untuk meng-enkripsi informasi-informasi yang bersifat rahasia. Hal ini dikarenakan Amerika Serikat berada pada masa dimana peran dari badan intelejen di Amerika Serikat sangat dibutuhkan karena sedang terjadi perang dingin dengan rusia sehingga informasi yang berlalu lalang menjadi sangat sensitif.

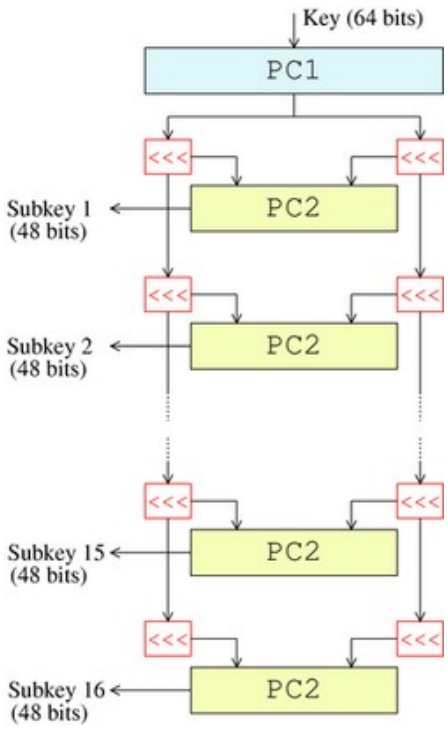
Oleh karena itu, tim IBM yang berangotakan Feistel, Walter Tuchman, Don Coppersmith, Alan Konheim, Carl Meyer, Mike Matyas, Roy Adler, Edna Grossman, Bill Notz, Lynn Smith, dan Bryant Tuckerman memberikan proposal untuk pembuatan Data Encryption Standard. Proposal tersebut diberikan pada tahun 1973.

Data Encryption Standard adalah algoritma yang memiliki serangkaian proses yang panjang untuk mengubah bitstring plainteks menjadi bitstring chiperteks dengan panjang yang sama. Untuk Data Encryption Standard sendiri, ukuran blok yang digunakan adalah 64 bit. Data Encryption Standard juga memiliki kunci untuk menyesuaikan proses transformasi plainteks ke chiperteks sehingga proses transformasi tersebut hanya dapat dilakukan oleh orang-orang yang memiliki kunci tersebut. Kunci juga memiliki panjang 64 bit. 8 bit digunakan untuk mengecek paritas, setelah dicek, 8 bit tersebut tidak digunakan lagi. Sisa bit yang sebanyak 56 digunakan untuk mendekripsi plainteks menjadi chiperteks.

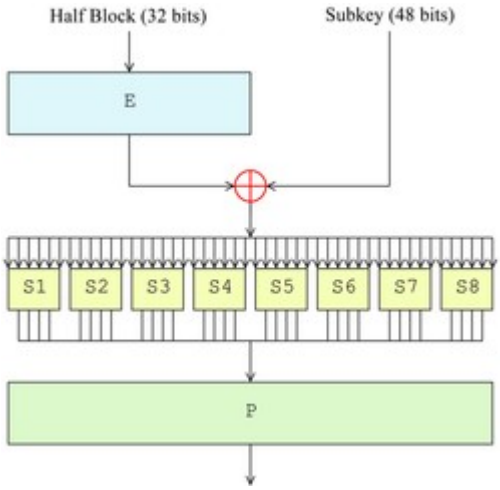
Berikut adalah gambar beberapa mode yang digunaka pada Data Encryption Standard



Fungsi Feisesl



sruktur Feistel DES



Kunci Jadwal DES

Seluru gambar disadur dari
https://bangunariyanto.wordpress.com/2010/03/09/data-encryption-standard/

Tapi Algoritma Data Encryption Standard ini tidak lagi dianggap aman karena ukuran kuncinya yang dianggap terlalu pendek. Kerentanan dari Data Encryption Standard terbukti setelah tim yang terdiri dari ahli keamanan komputer dan suatu komunitas mampu untuk memecahkan kunci Data Encryption Standard dalam waktu 22 jam.

3.1.2 Advanced Encryption Standard (AES)

Oleh karena Data Encryption Standard dianggap tidak aman lagi karena kuncinya dapat diretas dengan mudah. Pemerintah Amerika Serikat mengembangkan algoritma baru yang bertujuan untuk melampaui Algoritma Data Encryption Standard.

Oleh karena itu diajukan beberapa syarat yang nantinya akan dijadikan standard untuk Advanced Encryption Standard. Syarat tersebut yaitu :

- Algoritma harus berbasis algoritma chiper block.
- Seluruh rancangan algoritma harus transparan.
- panjang kunci terdiri dari 128 bit, 192 bit, 256 bit.
- Ukuran blok yang dienkripsi yaitu 128 bit.
- Algoritma harus bisa diimplementasikan secara hardware dan software.

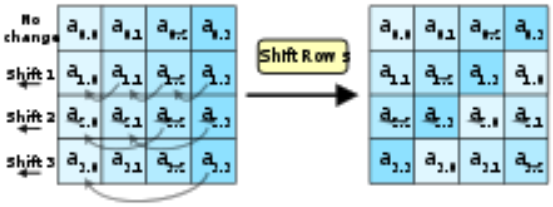
Setelah melalui serangkaian proses seleksi yang panjang dan rumit. Maka terpilihlah Algoritma rijndael yang ditemukan oleh Vincent Rijmen dan Joan Daemen yang berasal dari Belgia sebagai Advanced Encryption Standard. Peneetapan Algorimt Rijndael menjai Advanced Encryption Standard ini dilakukan pada bulan November tahun 2001.

Algoritma Rijndael memiliki banyak keunggulan dibandingkan dengan Data Encryption Standard. Hal ini dapat kita lihat pada banyak kunci dan panjang kunci yang digunakan. Pada Advanced Encryption Standard memiliki kunci dengan panjang 128 bit, 192 bit, dan 256 bit. Oleh karena ukuran kunci yang panjang tersebut, maka diharapkan

Advanced Encryption Standars tahan terhadap serangan Brute Force.

Pada proses transfomasi pesan pada Advanced Encryption Standard, memiliki 10, 12, dan 14 putaran sesuai dengan ukuran kunci yang digunakan. Setiap putaran memiliki proses sebagai berikut :

- Pergantian Byte seperti halnya DES.
- peralihan, yaitu pertukaran baris.
- campur jalur, yaitu peralihan kiri dan XOR bit-bit.
- Penambahan Subkunci, yaitu XOR bagian kunci dengan Keputusan Kitaran.



3.1.3 Kelebihan dan Kekurangan

Pada Data Encryption Standard, ditemukan beberapa kelebihan dan kekurangan. Kelebihannya adalah sebagai berikut :

- Kecepatan Operasi lebih tinggi dibanding teknik kriptografi asimetris
- Karena kecepatannya yang tinggi, maka Data Encryption Standard dapat digunakan pada sistem Real-Time.

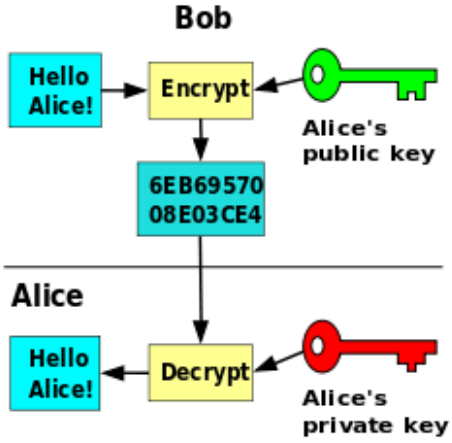
Kekurangan dari Data Encryption Standard adalah sebagai berikut:

- Terdapat permasalahan dalam pengiriman kunci yang disebut sebagai *"Key Distribution Problem"*.
- *Terjadi kesulitan manajemen kunci karena untuk setiap pesan yang berbeda, maka dibutuhkan kunci yang berbeda pula.*

3.2 Teknik Kriptografi Asimetris

Teknik Kriptografi Asimetris disebut juga teknik krptografi kunci publik. Disebut sebagai teknik kriptografi kunci publik dikarenak Teknik Kriptografi ini menggunakan satu kunci yang dapat diakses semua orang yang digunakan untuk mengenkripsikan pesan dari plainteks manjadi chiperteks. Kunci yang secara umum digunakan untuk melakukan proses enkripsi tersebut dinamakan *Public Key*. Sedangkan untuk prose dekripsi pesan chiperteks menjadi plainteks, dibutuhkan kunci yang disebut dengan *Private Key*.

Berikut adalah gambaran dari pemanfaatan Teknik Kriptografi Asimetris. Bob mengirimkan pesan kepada Alice yang berisi string "Hello Alice!". Pesan yang dikirimkan BOB ini kemudian dienkripsi menggunkan kunci publik milik Bob. Lalu pesan yang berbentuk chiperteks dikirm ke Alice. Seteleh Alice menerima chiperteks tersebut, Alice mendekripsi pesan tersebut dengan menggunaka private key milik Alice.



Gambar disadur dari https://id.wikipedia.org/wiki/Kriptografi

Algoritma yang tepat untuk digunakan sebagai teknik Kriptografi Asimetris adalah algoritma sebagai berikut :

3.2.1 Algoritma RSA (Rivest-Shamir-Adleman)

Algoritma ini diciptakan pada tahun 1977 oleh Ron Rivest, Adi Shamir , dan Len Adleman dari Massachusetts Institute of Technology. Algoritma ini kemudian dipatenkan oleh Massachusetts Institute of Technology yang berlaku hingga 21 September 2000.

Algoritma ini menggunakan banyak operasi aritmatika untuk penentuan pasangan public key dan private key nya. Algoritma ini juga dapat digunakan untuk mengecek kebsahan dari pesan tersebut. Metode ini dinamakan dengan *Padding Scheme.*

Algoritma RSA memiliki tiga proses utama, yaitu :

1. Proses Pembuatan Kunci

pada proses ini Algoritma menghasilkan Private Key dan Public Key. Pembuatan dari Private Key dan Public Key adalah sebagai berikut :

- Cari dua bilangan prima yang disimpan kedalam variabel *p* dan *q*. nilai p harus lebih besar dari q.
- Hitung n = p*q (Untuk digunakan sebagai pencarian nilai private key)
- Hitung pq = (p-1) * (q-1).(Untuk digunakan sebagai pencarian nilai private key)
- Pilih nilai e untuk public key dengan syarat (1< e < pq) dan (gcd(e,pq)=1). Gcd adalah *Greates Commont Divisor.*
- Pilih nilai d, dengan syarat nilai d memenuhi: (d*e) mod pq = 1

2. Proses Enkripsi

Mengubah pesan plainteks menjadi chiperteks dengan cara mengubah karakter yang ada pada pesan menjadi kode ASCII lalu menggunakan perhitungan yang melibatkan nilai n, public key dan kode ASCII

3. Proses Dekripsi

Mengubah pesan chiperteks menjadi plainteks dengan metode yang tidak berbeda jauh dengan proses enkripsi,

perbedaan nya hanyalah pada variabel yang digunakan untuk perhitungan menggunakan private key bukannya public key.

3.2.2 Kelebihan dan Kekurangan

Advanced Encryption Standard juga memliki beberapa kelebihan dan kekurangan. Kelebihannya adalah sebagai berikut:

- Masalah kemanan pada distribusi kunci lebih baik dibandingkan dengan Data Encryption Standard.
- Masalah manajemen kunci yang lebih baik karena jumlah kunci menjadi lebih sedikit.

Sedangkan kekurangan dari Advanced Encryption Standard adalah sebagai berikut :

- Kecepatan Pemrosesan enkripsi dan dekripsi yang lebih lambat dibandingkan dengan algoritma Data Encryption Standard.

Untuk tingkat kemanan yang sama, kunci yang digunakan lebih panjang dibandingkan dengan Data Encryption Standard.

IV. IMPLEMENTASI KRIPTOGRAFI PADA BANK

4.1 Mesin ATM

ATM adalah kepanjangan dari mesin Anjungan Tunan Mandiri. Biasanya digunakan oleh nasabah bank untuk melakukan transaksi perbankan. Kegunaan utama dari ATM adalah untuk menarik uang secara tunai. Namun pada saat ini, mesin ATM juga digunakan untuk kegiatan mentransfer uang ke rekening lain, pembayaran untuk berbagai jenis jasa yang tersedia, dll. Agar Mesin ATM dapat digunakan, maka dibutuhkan suatu kartu elektronik yang dinamakan kartu ATM. Kartu ATM diproteksi oleh password sebanyak 4 digit, Agar kartu ATM dapat digunakan, harus dimasukkan password yang benar, jika password yang dimasukkan sealah sebanyak 3 kali, maka mesin ATM akan otomatis menelan kartu ATM tersebut.

Setelah password dimasukkan, maka akan terjadi proses verifikasi password yang dilakukan di komputer pusat yang disebut dengan *Host*. Selama transmisi dari ATM ke komputer pusat, terjadi proses yang bertujuan untuk memproteksi keberlangsungan dari transmisi ATM ke komputer pusat, Proses tersebut adalah proses enkripsi. Proses enkripsi bertujua untuk melindungi Password yang kita gunakan dari penyadapan.

Gambar disadur dari http://cheesterzone.blogspot.co.id/2011/10/contoh-aplikasi-dan-pembahasan.html

Algoritma yang digunakan untuk proses enkirpsi ini adalah Algoritma Data Encryption Standard yang sudah dibahas tadi. Data Encryption Standard bekerja unuk pesan dengan panjang 64 bit sedangkan panjang password pada kartu ATM hanya 32 bit, oleh karena itu pada kartu ATM ditambahkan dengan *Padding Bits*. Padding bits ini memiliki panjang 32 bit sehingga panjang kartu ATM yang digunakan menjadi 64 bit.

4,2 Internet Banking

Internet Banking adalah suatu layanan yang disediakan oleh bank dalam rangka untuk memudahkan nasabah dari bank tersebut untuk melakukan aktivitas yang berkaitan dengan pengelolaan uang dari nasabah tersebut. Contoh dari aktivitas pengelolaan uang tersebut adalah aktivitas transfer, pembayaran tagihan, transfer uang, pembayaran tagihan, informasi rekening, pemindahbukuan, pengecekan saldo, dll. Layanan internet banking ini bisa digunakan dengan menggunakan layanan internet.

Agar aktivitas dari internet banking ini dapat aman dari kejahatan-kejahatan cyber, pihak bank harus memiliki sistem keamanan yang baik untuk memproteksi layanan Internet Banking ini. Oleh karena itu pihak bank menggunakan suatu metode enkripsi untuk melindungi informasi-informasi yang digunakan saat layanan internet banking digunakan. Metode ini disebut dengan metode enkripsi SSL.

4.2.1 SSL

SSL merupakan kepanjangan dari Secure Sockets Layer yang merupakan sebuah protokol yang digunakan untuk menjaga pengiriman data melalui web server. SSL dikembangkan pada tahun 1994 oleh Netscape Communication. SSL diciptakan dikarenakan kekhawatiran beberapa pihak yang merasa keamanan data dan informasi saat kita menggunakan layanan internet sangatlah rentan sehingga bisa disadap dengan mudah oleh pihak-pihak tertentu.

SSL sampai sekarang ini dijadikan sebagai standar keamanan untuk proteksi data pada layanan internet. Saat pengguna mengakses suatu website, SSL membuat koneksi yang sudah di-enkripsi antara server dari website yang dikunjungi tersebut dengan pengunjung dari website tersebut. Karena koneksinya sudah di-enkripsi, maka proses tukar-menukar informasi yang terjadi antara website dan pengunjung menjadi aman sehingga informasi tidak mudah disadap.

Protokol SSL mengotentikasi server kepada pengunjung dengan menggunakan kriptografi kunci asimetris. Algoritma yang digunakan untuk kriptografi kunci asimetris ini adalah algoritma RSA. Sedangkan untuk kunci rahasianya, SSL menggunakan algoritma IDEA, DES, dan Triple DES. Algoritma fungsi hash yang digunakan adalah MD5. Sedangkan untuk verifikasi kunci publik, sertifikat yang digunakan adalah yang memiliki standar X.509.

Pada SSL dikenal istilah Client dan Server. Client adalah sistem yang menginisiasi komunikasi, sedangkan server adalah sistem yang merespon request dari client. Client bertugas untuk mengajukan opsi SSL yang akan digunakan pada saat pertukaran informasi, sedangkan server menentukan opsi mana yang akan digunakan.

Ada beberapa tahapan proses pada SSL, yaitu :

Tahapan Otentikasi Server :

1. Client mengirimkan pesan Client Hello untuk mengajukan opsi SSL.
2. Server memberi respon dengan memilih opsi SSL melalui ServerHello.
3. Server mengirimkan sertifikat kunci publik pada pesan Certificate.
4. Server mengakhiri bagian negoisasi dengan pesan ServerHelloDone.
5. Client mengirimkan informasi session key yang dienkripsi dengan kunci publik server melalui pesan ClientKeyExchange.
6. Client mengirimkan pesan ChangeCipherSpec untuk mengaktifkan opsi yang dinegosiasikan untuk semua pesan yang akan dikirimkan.
7. Client mengirimkan pesan Finished sehingga memungkinkan server mengecek opsi baru yang diaktifkan.
8. Server mengirimkan pesan ChangeCipherSpec untuk mengaktifkan opsi yang dinegosiasikan untuk semua pesan yang akan dikirimkan.
9. Server mengirimkan pesan Finished sehingga memungkinkan client mengecek opsi baru yang diaktifkan.

Tahapan Pemisahan Otentikasi Server dan Enkripsi :

1. Client mengirimkan pesan ClientHello untuk mengajukan opsi SSL.
2. Server memberi respon dengan memilih opsi SSL melalui ServerHello.
3. Server mengirimkan sertifikat kunci publik pada pesan Certifikat.
4. Server mengirimkan kunci publik yang harus digunakan oleh client untuk mengenkripsi kunci simetrik pada ServerKeyExchange, kunci ini terdapat pada sertifikat server.
5. Server mengakhiri bagian negoisasi dengan pesan ServerHelloDone.
6. Client mengirimkan informasi session key pada pesan ClientKeyExchange (dienkripsi dengan kunci publik yang disediakan oleh server).
7. Client mengirimkan pesan ChangeCipherSpec untuk mengaktifkan opsi yang dinegoisasi untuk semua pesan yang akan dikirimkan.
8. Client mengirimkan pesan Finished sehingga memungkinkan server mengecek opsi baru yang diaktifkan.
9. Server mengirimkan pesan ChangeCipherSpec untuk mengaktifkan opsi yang dinegosiasikan untuk semua pesan yang akan dikirimkan.
10. Server mengirimkan pesan Finished yang memungkinkan client mengecek opsi baru yang diaktifkan.

Tahapan Otentikasi Client :

1. Client mengirimkan pesan ClientHello untuk mengajukan opsi SSL.
2. Server memberi respon dengan memilih opsi SSL melalui ServerHello.
3. Server mengirimkan sertifikat kunci publik pada pesan Certificate.
4. Server mengirimkan pesan Certificate Request untuk menunjukan bahwa server ingin mengotentikasi client.
5. Server mengakhiri bagian negosiasi dengan pesan ServerHelloDone.
6. Client mengirimkan sertifikat kunci publik pada pesan Certificate.
7. Client mengirimkan informasi session key pada pesan ClientKeyExchange (dienkripsi dengan kunci publik server).
8. Client mengirimkan pesan CertificateVerify yang menandai informasi penting tentang sesi menggunakan kunci privat client, server menggunakan kunci publik dari sertifikat client untuk memverifikasi identitas client.
9. Client mengirimkan pesan ChangeCipherSpec untuk mengaktifkan opsi yang dinegosiasikan untuk semua pesan yang akan dikirimkan.
10. Client mengirimkan pesan Finished sehingga memungkinkan server mengecek opsi baru yang diaktifkan.
11. Server mengirimkan pesan ChangeCipherSpec untuk mengaktifkan opsi yang dinegosiasikan untuk semua pesan yang akan dikirimkan.
12. Server mengirimkan pesan Finished yang memungkinkan client mengecek opsi baru yang diaktifkan.

Tahapan untuk melanjutkan sesi :

1. Client mengirimkan pesan ClientHello yang menetapkan ID sesi sebelumnya.
2. Server memberi respon dengan ServerHello untuk menyetujui ID sesi.
3. Server mengirimkan pesan ChangeCipherSpec untuk mengaktifkan kembali opsi pengamanan sesi untuk pesan yang akan dikirim.
4. Server mengirimkan pesan Finished yang memungkinkan client mengecek opsi baru yang diaktifkan kembali.
5. Client mengirimkan pesan ChangeCipherSpec untuk mengaktifkan kembali opsi yang dinegoisasi untuk semua pesan yang akan dikirimkan.
6. Client mengirimkan pesan Finished yang memungkinkan server mengecek opsi baru yang diaktifkan kembali.

SSL juga memiliki beberapa kelebihan dan kekurangan, berikut adalah kelebihan dari SSL:

- Enkripsi susah untuk dipecahkan
- Biaya pemakaian SSL yang tergolong murah
- User Friendly
- Proses membutuhkan alokasi memori yang sedikit
- Memiliki jaminan sertifikat

Sedangkan kekurangan dari SSL adalah :

- Lemah terhadap serangan Buffer Overflow, Man in the Middle Attack, Denial of Services, Cross Scripting Attack.
- Client sering tidak awas akan sertifikat palsu sehingga bisa dijadikan celah untuk menyadap informasi.

V. KESIMPULAN

Kesimpulan yang didapat pada makalah ini adalah sebagai berikut :

- Ilmu Kriptografi semakin berkembang seiring dengan pesatnya kemajuan teknologi
- Banyak pihak yang mulai membutuhkan ilmu Kriptografi ini agar informasi yang bersifat sensitif dapat dirahasiakan dan dijaga kemananannya
- Teknik Kriptografi terbagi menjadi dua, yaitu Teknik Kriptografi Simetri dan Teknik Kriptografi Asimetri.
- Algoritma yang digunakan untuk Teknik Kriptografi Simetri adalah Data Encryption Standard dan Advanced Encryption Standard, dll
- Algoritma yang digunakan untuk Teknik Kriptografi Asimetri adalah RSA
- Mesin Anjungan Tunai Mandiri menggunakan algoritma Data Encryption Standard untuk proses enkripsi data
- Fasilitas Internet Banking menggunakan protokol SSL untuk mengamankan informasi yang dikirim dan diterima
- SSL menggunakan algoritma DES, 3DES untuk private key dan menggunakan algoritma RSA untuk public key

REFERENSI

[1] http://octarapribadi.blogspot.co.id/2012/10/contoh-enkripsi-dengan-algoritma-des.html
[2] http://riskahomina.blogspot.co.id/2011/10/tugas-kriptografi_30.html
[3] kur2003.if.itb.ac.id/file/DES.doc
[4] B. Smith, “An approach to graphs of linear forms (Unpublished work style),” unpublished.
[5] https://bangunariyanto.wordpress.com/2010/03/09/data-encryption-standard/
[6] https://id.wikipedia.org/wiki/RSA
[7] http://cheesterzone.blogspot.co.id/2011/10/contoh-aplikasi-dan-pembahasan.html
[8] http://autotekno.sindonews.com/read/972998/133/cegah-kejahatan-internet-banking-dengan-enkripsi-1425627147
[9] http://blog.kunchunx.com/index.php/tag/enkripsi-ssl-128-bit/
[10] https://dimas347.wordpress.com/2011/02/14/security-socket-layer-ssl/
[11] http://www.jaringan-komputer.cv-sysneta.com/apa-itu-secure-socket-layer-ssl
[12] ttp://azxmy.blogspot.co.id/2012/05/pengertian-serta-cara-kerja-ssl-rsa-pgp.html
[13] http://thuekx.kolu.web.id/ssl-secure-socket-layer/
[14] http://blog.sslmurah.com/tutorial/ssl-faq/ukuran-kunci-bit-pada-sistem-enkripsi-data-sertifikat-digital-ssl/
[15] https://id.wikipedia.org/wiki/E-banking
[16] http://www.sulaidihasibuan.com/2015/09/pengertian-internet-banking.html
[17] http://www.temukanpengertian.com/2015/07/pengertian-internet-banking.html

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, 8 Desember 2015

ttd

Raihan Maulana Warman dan 13514076