Kriptografi Pada ATM

Auliya Unnisa Fitri S (13509067)

Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
13509067@std.stei.itb.ac.id

ABSTRAK

ATM merupakan singkatan dari Automated Teller Machine ataupun Anjungan Tunai Mandiri. ATM bukanlah satu hal yang asing dalam kehidupan masyarakat modern. ATM memudahkan nasabah suatu bank dalam berkegiatan perbankan di mana saja, tanpa harus mengantri di bank yang bersangkutan. Hanya dengan memasukkan *Personal Identification Number* (PIN) miliknya, datanya dapat dikenali oleh bank nasabah dan nasabah dapat mengakses akunnya dengan mudah. Karena kemudahan inilah, nasabah memerlukan perlindungan khusus terhadap data miliknya. Agar milik nasabah dapat terjaga dengan baik, diperlukan suatu sistem yang melindungi data nasabah. Hal ini dapat dilakukan melalui kriptografi. Pada makalah ini akan dijelaskan bagaimana sistem pengamanan itu bekerja dengan memanfaatkan kriptografi.

Kata kunci : ATM, DES, ECB, 3DES

1. PENDAHULUAN

Tak dapat dipungkiri lagi bahwa manusia selalu berusaha menemukan cara yang bisa mengefektifkan waktu yang digunakan dalam menjalankan suatu kegiatan dalam hidupnya. Apa yang bisa dimanfaatkan? Jawabannya tentulah teknologi. Teknologi telah merasuki dan memegang peranan penting dalam kehidupan manusia. Hal ini dapat dilihat dari maraknya penggunaan teknologi di berbagai aspek dalam kehidupan. Peminatnya terdiri dari berbagai kalangan umur mulai dari anak-anak hingga orang tua. Teknologi pun dapat ditemukan dimana saja mulai dari lingkungan tempat tinggal hingga tempat-tempat umum.

Salah satu kegiatan yang cukup membuang waktu tapi sering dilakukan adalah mengantre di bank untuk kegiatan perbankan. Apa yang teknologi berikan agar kegiatan seperti ini bisa menghemat waktu? Jawabannya Automated Teller Machine atau sering disebut Anjungan Tunai Mandiri (ATM). Ya, ATM adalah penemuan manusia dalam bidang teknologi yang membuat kegiatan perbankan berjalan dengan waktu seefektif dan seefisien mungkin.

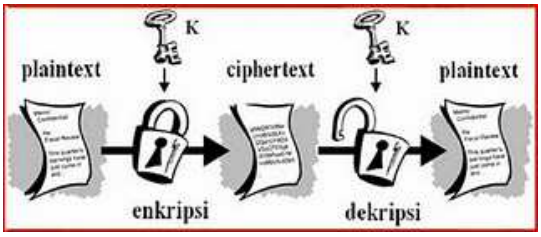
ATM adalah sebuah alat elektronik yang mengizinkan para nasabah bank untuk mengambil uang dan mengecek rekening tabungan mereka tanpa perlu dilayani oleh seorang *teller* manusia. ATM pertama mulai digunakan pada Desember 1972 di Inggris; IBM 2984 dirancang atas permintaan Lloyds Bank . Mesin 2984 CIT (Cash Penerbitan Terminal) adalah ATM yang pertama, fungsinya serupa dengan fungsi mesin hari ini. Saat ini ATM masih merupakan merek dagang terdaftar dari Lloyds TSB di Inggris[4].

Gambar 1. ATM Modern

ATM tak ubahnya sebuah mesin pemroses uang melalui kartu ATM. ATM dapat digunakan untuk memenuhi berbagai keperluan seperti penarikan uang secara tunai, pentransferan uang ke rekening lain, bahkan dapat digunakan untuk pembayaran tagihan. Pengguna hanya tinggal memasukkan kartu dan melakukan instruksi-instruksi yang diberikan.

Saat *customer* memasukkan kartu ATM, maka kartu ini dimasukkan ke dalam *card reader*. Kemudian *card reader* akan membaca data kartu ATM customer tersebut. Lalu data tersebut akan dikirim ke komputer Server Bank melewati *switching*. *Switching* adalah pengaturan/ pengontrol lalu lintas. Kartu ini akan divalidasi apakah benar terdaftar di Server Bank, apabila customer memasukkan kartu bank lainnya ke mesin ATM maka tentu saja akan gagal dan kartu tersebut akan keluar lagi. Bila Kartu tersebut ternyata benar milik Bank tersebut maka mesin akan meminta password atau yang biasa disebut PIN (*Personal Identification Number*). Kemudian PIN yang kita masukkan ini akan dikirim ke server lagi untuk dicocokkan lagi.

Dari sisi ATM ke server ada sebuah proses yang dinamakan enkripsi dan dekripsi, Saat data PIN tersebut dikirim maka akan dienkripsi. Enkripsi adalah pengonversian kedalam bahasa tertentu agar tidak bisa dibaca atau bahasa kasarnya di acak sehingga tidak bisa terbaca. Proses enkripsi menggunakan algoritma-algoritma tertentu. Server dapat membaca data itu karena di sisi server terjadi dekripsi dengan *key algoritma* tersebut agar dapat terbaca. Hal ini dilakukan sebagai keamanan agar tidak ada pihak lain yang tahu passwordnya, bahkan pihak server sendiri tidak mengetahui password tersebut. Jika diilustrasikan akan seperti gambar dibawah.



Gambar 2. Enkripsi dan Dekripsi

Dasar matematis yang mendasari proses enkripsi dan dekripsi adalah relasi antara dua himpunan yaitu yang berisi elemen teks terang /plaintext dan yang berisi elemen teks sandi/ciphertext. Enkripsi dan dekripsi merupakan fungsi transformasi antara himpunan-himpunan tersebut. Apabila elemen-elemen teks terang dinotasikan dengan Plaintext, elemen-elemen teks sandi dinotasikan dengan Chipertext, sedang untuk proses enkripsi dinotasikan dengan E, dekripsi dengan notasi D.

Enkripsi :

E(Plaintext) = Chipertext

Dekripsi :

D(Chipertext) = Plaintext

atau

D(E(Plaintext)) = Plaintext[2]

Metode enkripsi data yang digunakan pada ATM adalah dengan teknik *Data Encryption Standard* (*DES*); yang kemudian dikembangkan menjadi *Triple Data Encryption Standard (3DES)* guna meningkatkan keamanan data. Mode yang digunakan adalah *Electronic Code Book (ECB)*.

2. PERAN KRIPTOGRAFI

2.1. Algoritma Kunci Simetrik

Metode enkripsi dibagi menjadi algoritma kunci simetrik dan algoritma kunci asimetrik. DES merupakan salah satu contoh algoritma kunci simetrik. Pada algoritma kunci simetrik, pengirim dan penerima harus memiliki kunci yang digunakan bersama dan dijaga kerahasiaanya. Pengirim menggunkan kunci ini untuk enkripsi dan penerima menggunakan kunci yang sama untuk dekripsi.

Kelebihan :

- Kecepatan operasi lebih tinggi bila dibandingkan dengan algoritma asimetrik.
- Karena kecepatannya yang cukup tinggi, maka dapat digunakan pada sistem real-time

Kelemahan :

- Untuk tiap pengiriman pesan dengan pengguna yang berbeda dibutuhkan kunci yang berbeda juga, sehingga akan terjadi kesulitan dalam manajemen kunci tersebut.
- Permasalahan dalam pengiriman kunci itu sendiri yang disebut "key distribution problem".

Contoh algoritma : Data Encryption Standard (DES), blowfish, TwoFish, Rijndael, Camellia.

Cipher kunci simetrik dapat dibedakan dalam dua tipe, tergantung pada bagaimana cipher tersebut bekerja. Yang pertama pada blok simbol pada ukuran yang tetap (cipher blok), sedangkan yang kedua pada aliran simbol terus-menerus (stream cipher).

2.1.1. *Cipher* Aliran (*Stream Cipher*)

Algoritma kriptografi beroperasi pada plainteks/cipherteks dalam bentuk bit tunggal, yang dalam hal ini rangkaian bit dienkripsikan/didekripsikan bit per bit.

Adapun algoritma yang termasuk dalam stream cipher yang sering digunakan adalah algoritma A5/1 untuk jaringan GSM.

Algoritma A5 adalah algoritma stream cipher yang digunakan untuk mengenkripsi pesan dalam transmisi udara. Stream cipher ini diinisialisasi dengan setiap frame yang dikirim. Stream cipher ini diinisialisasikan dengan kunci sesi, Kc, dan jumlah frame yang akan dienkripsi. Kunci sesi yang sama digunakan sepanjang panggilan berlangsung, tetapi 22 bit nomor frame berubah selama proses berlangsung, kemudian membangkitkan keystream yang unik untuk setiap frame [FIR06].

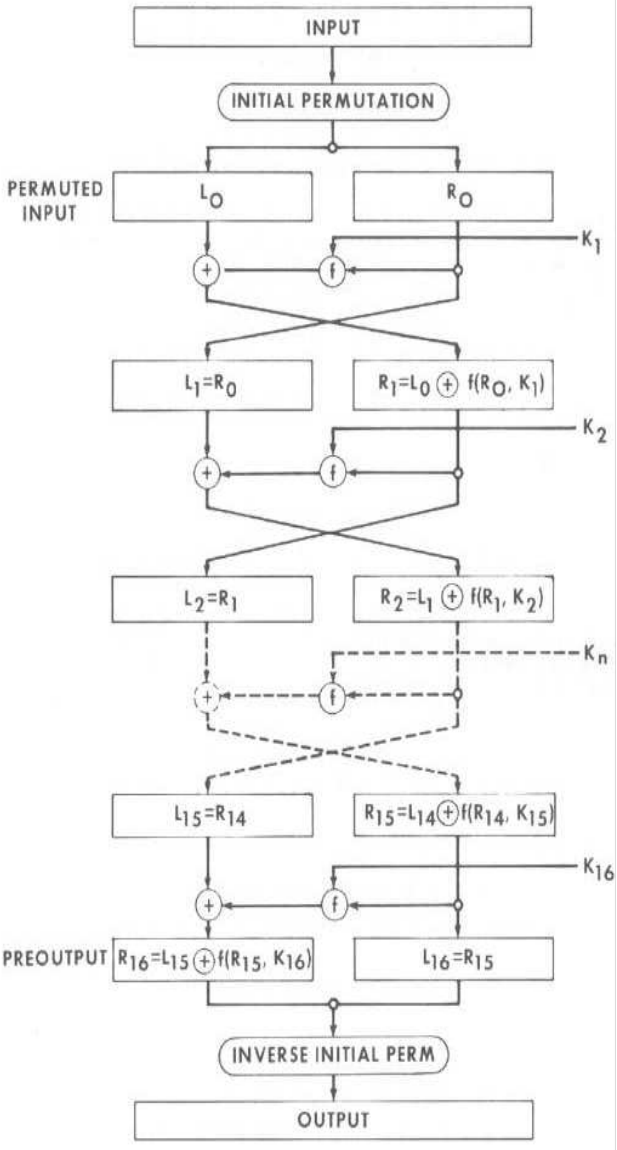
2.1.2. *Cipher* Blok (*Block Cipher*)

Pada *cipher* blok, plaintext dibagi menjadi beberapa blok dengan panjang tetap. Ketika melakukan enkripsi, *cipher* blok mungkin saja menerima input 128-bit plaintext dan mengeluarkan 128-bit keluaran ciphertext. Transformasi selengkapnya dikontrol menggunakan masukan kedua- yaitu kunci. Begitu pula halnya dengan dekripsi, algoritma untuk melakukan dekripsi akan menerima masukan 128-bit cipherteks dan kunci kemudian menghasilkan keluaran 128-bit plainteks aslinya.

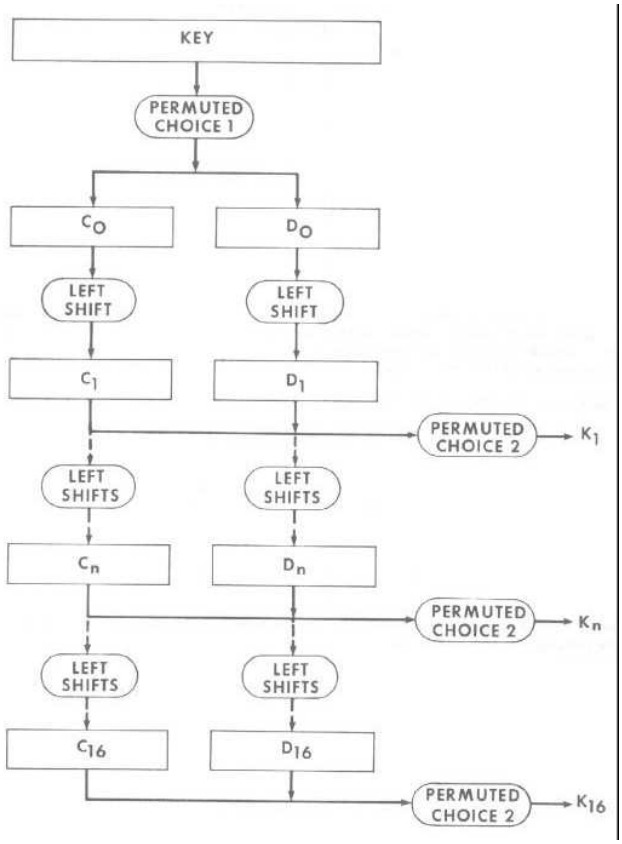
Untuk melakukan enkripsi terhadap pesan yang lebih panjang dari ukuran blok, pada cipher blok, digunakan mode-mode tertentu. Salah satunya adalah Electronic Code Book (ECB)[3].

2.2. Data Encryption Standard (DES)

Dalam bidang kriptografi, Data Encryption Standard (DES) adalah algoritma enkripsi sandi blok kunci simetrik dengan ukuran blok 64-bit dan ukuran kunci 56-bit[1]. Pada algoritma DES, setiap blok dienkripsi sebanyak 16 kali putaran dengan kunci internal yang berbeda-beda yang dibangkitkan dari kunci eksternal[8].

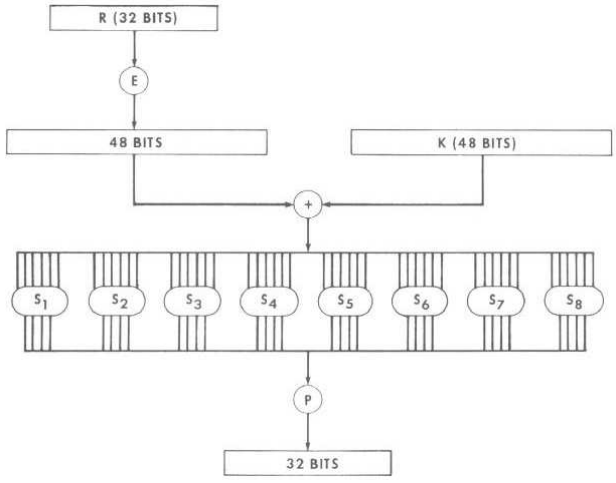


Gambar 3. Skema Algoritma DES



Gambar 4. Proses Pembangkitan Kunci-Kunci Internal DES

Permutasi awal (permuted choice 1) bertujuan mengacak plainteks sehingga urutan bit-bit di dalamnya berubah. Terhadap blok hasil permutasi awal tesebut dilakukan proses *enciphering* (enkripsi) dengan melakukan 16 putaran (*round*). Pada proses inilah digunakan kunci internal yang berbeda-beda untuk setiap putarannya. Permutasi terakhir dilakukan setelah 16 kali putaran terhadap gabungan blok kiri dan blok kanan. Sedangkan komputasinya dapat dijelaskan dengan suatu fungsi yang disebut fungsi Feistel yang diproses pada blok chiper[7].



Gambar 5. Fungsi Feistel

Walaupun DES memiliki panjang kunci 56 bit yang berarti akan terdapat 2^{56} atau 72.057.594.037.927.936 kemungkinan kunci, DES dinilai tidak aman lagi dipergunakan. Hal ini dibuktikan DES-cracker yang dibangun oleh Electronic Frontier Foundation (EFF), sebuah komunitas yang bergerak dalam dunia cyber. Dengan serangan brute force, hanya diperlukan kurang dari 2 hari untuk menemukan kuncinya. Untuk itulah dirancang Triple Data Encryption Standard (3DES), suatu system yang dinilai akan lebih kuat dari sekedar DES saja[5].

2.3. Triple Data Encryption Standard (3DES)

Sesuai namanya, 3DES merupakan pengembangan dari DES. Dengan menggunakan enkripsi standar DES, Triple-DES mengenkripsi data tiga kali dan menggunakan kunci yang berbeda untuk setidaknya satu dari tiga lewat memberikan ukuran kunci kumulatif 112-168 bit.

Enkripsi:

Chipertext = EK*3*(EK*2*(EK*1*(Plaintext)))

Dekripsi:

Plaintext = DK*3*(DK*2*(DK*1*(Chipertext)))[6]

Keterangan:
E = enkripsi
D = dekripsi
K*i* = kunci ke-*i*

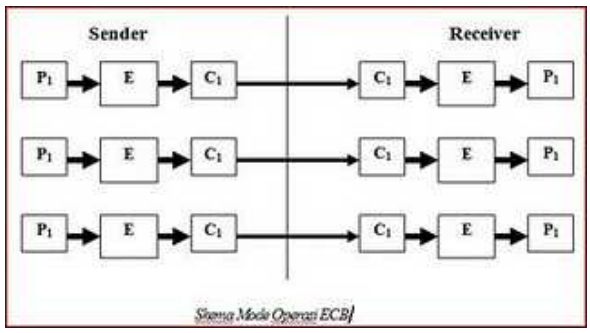
Gambar 6. Enkripsi 3DES

2.4. Electronic Code Book (ECB)

Pada mode operasi ECB sebuah blok input plaintext dipetakan secara statis ke sebuah blok output ciphertext. Sehingga tiap plaintext yang sama akan menghasilkan ciphertext yang selalu sama pula. Sifat- sifat dari mode operasi ECB :

- Sederhana dan efisien
- Memungkinkan implementasi paralel
- Tidak menyembunyikan pola plaintext
- Dimungkinkan terjadi adanya active attack[2].

Skema dari mode operasi ECB dapat digambarkan sebagai berikut :



Gambar 7. Skema Operasi ECB

3. IMPLEMENTASI PENGAMANAN PADA ATM

Seluruh kegiatan perbankan di ATM hanya dapat diakses dengan menggunakan PIN yang benar. PIN terdiri dari minimal 4 digit yang harus dijaga kerahasiaannya oleh pemilik kartu ATM, sebab orang lain yang mengetahui PIN dapat menggunakan kartu ATM yang dicuri atau hilang untuk melakukan penarikan uang. PIN digunakan untuk memverifikasi kartu yang dimasukkan oleh nasabah di ATM. Proses verifikasi dilakukan di komputer pusat (host) bank, oleh karena itu harus ada komunikasi dua arah antara ATM dan komputer host.

ATM mengirim PIN dan informasi tambahan pada kartu ke komputerhost, host melakukan verifikasi dengan cara membandingkan data dari PIN yang di-entry-kan oleh nasabah dengan data yang disimpan di dalam basisdata komputerhost, lalu mengirimkan pesan tanggapan ke ATM yang menyatakan apakah transaksi dapat dilanjutkan atau ditolak.

Selama transmisi dari ATM ke komputerhost, PIN harus dilindungi dari penyadapan oleh orang yang tidak berhak. Bentuk dengan engenkripsikan PIN. Di sisi bank, PIN yang disimpan di dalam basisdata juga dienkripsi. Algoritma enkripsi yang digunakan adalah DES dengan mode ECB.

Proses pembuatan nomor PIN tersebut menggunakan perhitungan sebagai berikut:

1. Ambil lima digit terakhir dari nomor rekening
2. Gabungkan kelima angka tersebut dengan 11 digit data validasi (data validasi diciptakan sendiri)
3. Keenambelas angka tersebut merupakan data yang menjadi data masukan untuk algoritma DES. Pada pemrosesan dengan algoritma DES digunakan kunci berukuran 16 digit yang kemudian disebut sebagai "kunci PIN".
4. Dari hasil pemrosesan dengan DES diambil 4 digit pertama kemudian diubah ke dalam bentuk desimal – penggunaan DES akan menghasilkan bilangan dengan satuan heksadesimal. Empat digit tersebut kemudian disebut sebagai "PIN alami".
5. Dari PIN alami tersebut kemudian ditambahkan dengan 4 digit yang disebut sebagai *offset* sehingga menghasilkan nomor PIN yang akan digunakan oleh nasabah.

Sebagai contoh:

- Misalkan nomor rekening nasabah adalah *4506602100091715*
- Lima digit terakhir adalah *91715*
- Data validasi adalah *88070123456*
- Masukan untuk algoritma DES adalah *8807012345691715*
- "Kunci PIN" untuk algoritma DES adalah *FEFEFEFEFEFEFEFE*
- Hasil dari algoritma DES adalah *A2CE126C69AEC82D*
- "PIN alami" (empat digit pertama) adalah *0224*
- Nilai *offset* adalah *6565*
- Nomor PIN nasabah adalah *6789*[9]

Segala data nasabah dapat disimpan pada kartu ATM. Kartu ATM saat ini masih berjenis *Magnetic Card Reader* atau kartu magnetik yang memiliki garis hitam di sisi belakang kartu yang memuat data tentang nomor pengguna kartu tersebut. Garis magnetik terletak 0,223 inci (5,56 mm) dari tepi kartu, dan 0,375 inci (9,52 mm) lebar. Pita magnetik berisi tiga trek, masing-masing 0,110 inci (2,79 mm) lebar. Trek satu dan tiga biasanya dicatat pada 210 bit per inci (8,27 bit per mm), sedangkan trek dua biasanya memiliki kepadatan rekaman 75 bit per inci (2,95 bit per mm). Setiap trek dapat berisi karakter alfanumerik 7-bit atau karakter numerik 5-bit.

Karena panjang PIN hanya 4 digit, maka peluang ditebak sangat besar. Seseorang yang memperoleh kartu ATM curian atau hilang dapat mencoba semua kemungkinan kode PIN yang mungkin, sebab hanya ada $10 \times 10 \times 10 \times 10 = 10.000$ kemungkinan kode PIN 4-digit. Untuk mengatasi masalah ini, maka kebanyakan ATM hanya membolehkan peng-entry-an PIN maksimum 3 kali, jika 3 kali tetap salah maka ATM akan 'menelan' kartu ATM. Selain itu, bank juga mulai mengembangkan sistem pengamanan mereka dengan mulai menerapkan system PIN 6 digit.

4. KESIMPULAN

Kriptografi sangat banyak diimplementasikan dalam kehidupan manusia yang semakin modern. Salah satunya pada kegiatan perbankan melalui ATM. Kunci kriptografi pada ATM terletak pada PIN si nasabah. Dari PIN inilah segala data sang nasabah di bank dapat diakses. Karena itu, PIN harus dirahasiakan demi keamanan nasabah. Di sinilah kriptografi berperan, yaitu dalam menjaga kerahasiaan PIN nasabah.

REFERENCES

[1] Rinaldi Munir, *Matematika Diskrit*. Bandung : Informatika, 2005, ch 5.

[2] "Enkripsi & Dekripsi" destiasalma.blogspot.com, Destia Salma, 11 Desember 2010

[3] "Enkripsi dan Dekripsi" apriladewikoto.com, Aprilia Dewi Koto, 11 Desember 2010

[4] "ATM" wikipedia.org, 11 Desember 2010

[5] "Data Encryption Standard (DES)" wikipedia.org, 11 Desember 2010

[6] "Triple DES" wikipedia.org, 11 Desember 2010

[7] Data Encryption Standard (DES) FIPS PUB 46-3

[8] Rinaldi Munir, "Data Encryption Standard," in IF5054 Kriptografi slide.

[9] Roni Sambiangga, "Sistem Keamanan ATM (*Automated Teller Machine* / Anjungan Tunai Mandiri)," Kriptografi., submitted for publication

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, 14 Desember 2010

ttd

Auliya Unnisa
NIM. 13509067