KRIPTOGRAFI PADA KEJAHATAN PEMBOBOLAN ATM DI INDONESIA

M. Pasca Nugraha (13507033)

Sekolah Teknik Elektro dan Informatika
Program Studi Teknik Informatika
Institut Teknologi Bandung
Jalan Ganesha 10 Bandung
e-mail: if17033@students.if.itb.ac.id, mpascanug@yahoo.co.id

ABSTRAK

Pada zaman sekarang ini, dimana budaya antri sudah hampir ditinggalkan karena ketidak-efektifannya, transaksi melalui ATM menjadi sebuah kebutuhan bagi banyak orang. ATM menyediakan akses yang cepat dan mudah dari seorang nasabah bank ke *account* yang dia punya. Namun di balik kemudahan tersebut, sebuah teknologi juga menawarkan terjadinya kejahatan baru.

Akhir-akhir ini masyarakat Indonesia, khususnya di sejumlah kota besar, dikejutkan dengan maraknya kejahatan pembobolan ATM. Modus pembobolan ini ditengarai cukup lihai dengan menggunakan berbagai macam cara, dimana beberapa diantaranya termasuk serangan terhadap kriptogtafi.

Dalam makalah ini pertama-tama akan dibahas mengenai cara kerja mesin ATM, terutama hubungannya dengan kriptografi, dalam hal ini adalah proses enkripsi terhadap nomor pin masukkan pengguna. Setelah itu akan dibahas mengenai kejahatan pembobolan ATM beserta metode-metodenya, dikaitkan dengan kriptografi. Kemudian penulis akan sedikit membahas tentang sistem keamanan pada ATM disertai dengan solusi yang ditawarkan untuk mengatasi masalah pembobolan ATM di atas.

Kata kunci: pembobolan ATM, serangan terhadap kriptografi.

1. PENDAHULUAN

ATM (Automatic Teller Machine atau Automated Teller Machine, yang di Indonesia juga kadang merupakan singkatan bagi Anjungan Tunai Mandiri) adalah sebuah alat elektronik yang mengijinkan nasabah bank untuk mengambil uang dan mengecek rekening tabungan mereka tanpa perlu dilayani oleh seorang "teller" manusia. Banyak ATM juga mengijinkan penyimpanan uang atau cek, transfer uang atau bahkan membeli perangko.

Konsep ATM pertama kali lahir pada tahun 1968. Mesin ini ditemukan oleh Don Wetzel, Vice President of Product Planning pada perusahaan Docutel, bersama dengan rekan-rekannya yaitu Tom Barnes, Kepala Mekanik dan George Chastian, seorang insinyur listrik.

Pada perkembangannya, demi menjaga keamanan nasabah, ATM ini tidak terlepas dari kriptografi, terutama pada saat transmisi nomor PIN dari mesin ATM ke pusat data bank. Oleh karena itu pada bab ini akan dijelaskan terlebih dahulu metode-metode kriptografi terkait dan dihubungkan dengan mekanisme kerja ATM secara singkat.

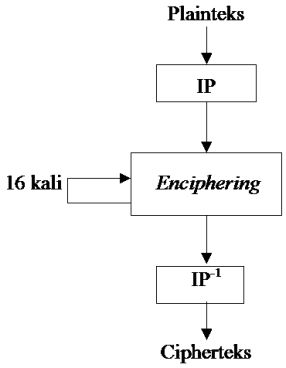
1.1 Metode

Seperti telah disebutkan sebelumnya bahwa algoritma yang digunakan dalam meng-enkripsi nomor PIN yang di-entry pengguna sebelum ditransmisikan ke komputer host adalah algoritma DES dengan mode ECB. Berikut akan dijelaskan secara singkat algoritma DES dan mode ECB yang dimaksud.

1.1.1 Algoritma DES

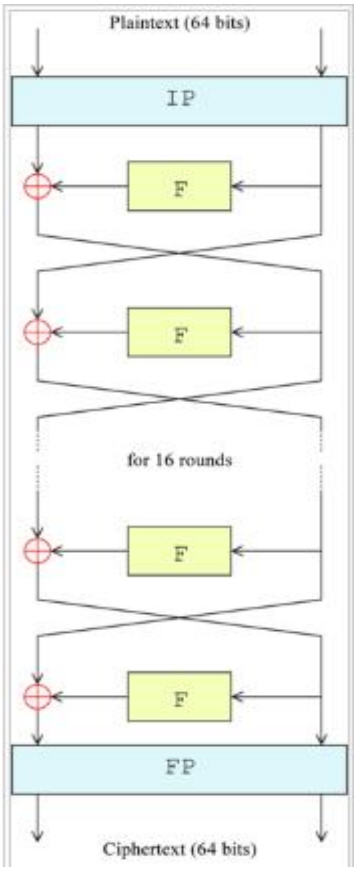
Algoritma DES atau Data Encryption Standard adalah sebuah block cipher yang merupakan kriptografi kunci simetri dan menggunakan algoritma DEA (Data Encryption Algorithm). DES beroperasi pada ukuran blok 64 bit, dengan panjang kunci sama dengan ukuran blok, aitu 64 bit juga, tetapi hanya terpakai 56 bit (8 bit lainnya tidak terpakai).

Pada algoritma DES, setiap blok dienkripsi sebanyak 16 kali putaran dengan kunci internal yang berbeda-beda yang dibangkitkan dari kunci eksternal. Selain itu juga dilakukan permutasi awal dan inversi permutasi awal (kadang disebut permutasi akhir). Skema global DES dapat dilihat pada skema di bawah ini :



Gambar 1. Skema global DES

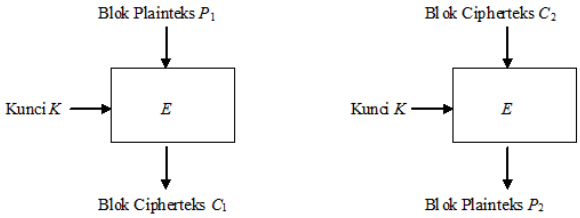
Sedangkan diagram algoritma DES secara lengkap dapat dilihat pada gambar berikut ini:



Gambar 2. Algoritma DES

1.1.2 Mode ECB

ECB atau *Electronic Code Book* merusapakan salah satu mode operasi cipher block. Setiap blok plainteks P_i dienkripsi secara individual dan independen menjadi blok cipherteks C_i . Skema sederhananya adalah sebagai berikut :



Gambar 3. Skema ECB

Keuntungan mode ECB adalah pemrosesannya yang berlangsung linear sehingga kesalahan pada satu atau lebih bit pada suatu blok tidak mempengaruhi blok yang lain. Namun, kelemahannya, pada mode ECB, blok plainteks yang sama selalu dienkripsi menjadi blok cipherteks yang sama. Oleh karena itu, berdasarkan statistik, mode ni mudah diserang.

1.1.3 Serangan Terhadap Kriptografi

Pada bab berikutnya akan membahas mengenai pembobolan ATM yang merupakan serangan terhadap kriptografi. Oleh karena itu pada bab ini akan dibahas sedikit mengenai teori serangan terhadap kriptografi.

Serangan terhadap kriptografi dapat dibagi berdasarkan keterlibatan penyerang dalam komunikasi, berdasarkan teknik yang digunakan untuk menemukan kunci, dan berdasarkan ketersediaan data.

Berdasarkan ketersediaan data, serangan dapat dibagi paling tidak menjadi 3 macam :

1. Ciphertext-only attack, dimana penyerang hanya mengetahui ciphertext untuk dianalisis.
2. Known-plaintext attack, dimana penyerang memiliki pasangan plaintext dan ciphertext yang berpadanan.
3. Chosen plaintext-attack, dimana penyerang dapat memilih plaintext tertentu untuk dienkripsikan dan mengetahui ciphertextnya.

dan masih ada beberapa macam lagi, namun pada umumnya dapat diwakili oleh 3 pembagian di atas.

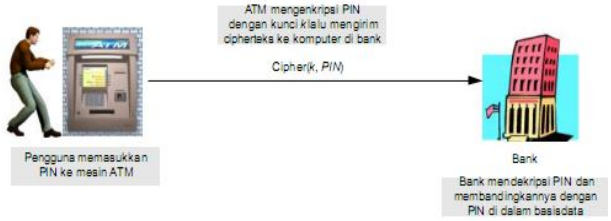
1.2 Kriptografi pada ATM

Suatu transaksi lewat ATM membutuhkan sebuah kartu ATM dan sebuah kode PIN yang berasosiasi dengan kartu tersebut. Kode PIN pada umumnya terdiri atas 4 angka

(tergantung bank bersangkutan) yang harus terjamin kerahasiaannya oleh pemegang kartu.

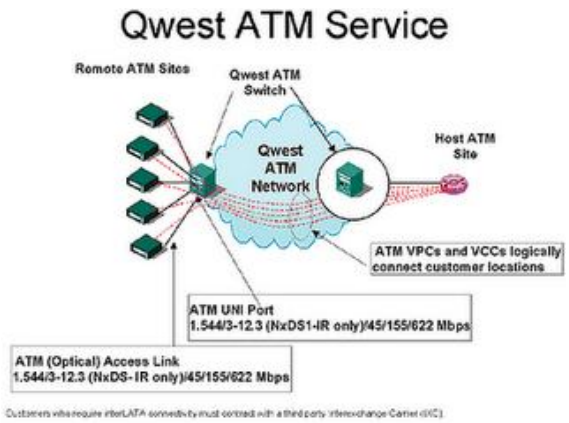
Ketika pengguna ATM memasukkan kartu ATM ke dalam mesin, kemudian mengetikkan nomor PIN, maka asosiasi kartu dan PIN tersebut akan diverifikasi oleh komputer pusat (*host*) bank dengan cara membandingkannya dengan basis data pusat. Setelah itu *host* memberikan feedback, apakah PIN tersebut legal atau tidak untuk menentukan apakah transaksi bisa dilanjutkan atau dihentikan.

Untuk melindungi PIN pengguna dari penyadapan, maka nomor PIN yang diketikkan oleh pengguna dienkripsi terlebih dahulu sebelum ditransmisikan ke komputer *host* di bank pusat, sehingga yang dikirimkan berupa pesan terenkripsi (ciphertext). Algoritma enkripsi yang digunakan adalah DES dengan mode ECB, yang telah dijelaskan pada subbab sebelumnya. Setelah ditransmisikan, komputer *host* kemudian mendekripsi ciphertext tadi menjadi nomor PIN semula, kemudian baru membandingkannya dengan basis data yang ada pada komputer *host*. Proses enkripsi-dekripsi pada transaksi di ATM dapat dilihat pada gambar di bawah ini.



Gambar 4. Mekanisme enkripsi-dekripsi pada ATM

Sedangkan makanisme jaringan yang menghubungkan ATM dengan host pusat seperti yang disebutkan sedikit di atas dapat digambarkan sebagai berikut :



Gambar 5. Jaringan layanan ATM

2. PEMBAHASAN

Hasil penyelidikan terhadap pelaku pembobolan ATM yang berhasil ditangkap menyebutkan bahwa terdapat beberapa cara yang biasa dilakukan oleh pembobol ATM di Indonesia.

Modus pertama, pelaku mencuri data digital kartu ATM nasabah dengan *skimmer* yang terpasang di mesin ATM. Kemudian untuk mencuri nomor PIN nasabah, pelaku menggunakan bantuan kamera pengintai yang terpasang di dalam ruang ATM atau dengan mengintip langsung ketika nasabah mengetik nomor PIN. Pelaku kemudian menyalin data ke kartu palsu dan selanjutnya menguras tabungan nasabah.

Modus kedua, pelaku memasang suatu alat di dalam mesin ATM untuk menjepit kartu ketika nasabah memasukkan kartu. Pelaku juga memasang stiker palsu di *body* mesin. Di stiker tertulis nomor *hotline* palsu yang dapat dihubungi jika mengalami gangguan. Setelah kartu tertahan di dalam mesin, korban kemudian menghubungi nomor *hotline* tersebut dan diterima oleh petugas bank gadungan. Petugas palsu tersebut lalu berpura-pura meminta identitas nasabah, seperti nama, alamat, tanggal lahir. Kemudian pada akhirnya dia meminta nomor PIN. Lalu petugas menyuruh korban untuk pergi dan mengambil kartunya di kemudian hari. Setelah korban pergi, pelaku kemudian mendatangi mesin ATM dan mengambil kartu korban lalu menguras isi dari tabungannya.

Modus ketiga hampir sama dengan modus kedua. Namun pada modus ketiga, pelaku tidak menggunakan stiker, tetapi pelaku sendiri yang menghampiri korban dan menyarankan kepada korban untuk menghubungi *call center* 14000. Namun ketika dihubungi, yang menerima panggilan adalah operator palsu.. Selanjutnya sama dengan modus ketiga.

Modus keempat, pelaku mencuri data digital kartu ATM beserta nomor PIN lalu menjualnya kepada pelaku lain seharga Rp 1 juta per data.

Modus kelima, pelaku menyadap transmisi antara mesin ATM dengan komputer *host* di bank pusat, kemudian berusaha mendekripsi nomor PIN yang telah terenkripsi dengan pendekatan *known plaintext attack* atau bahkan dengan *chosen plaintext attack*.

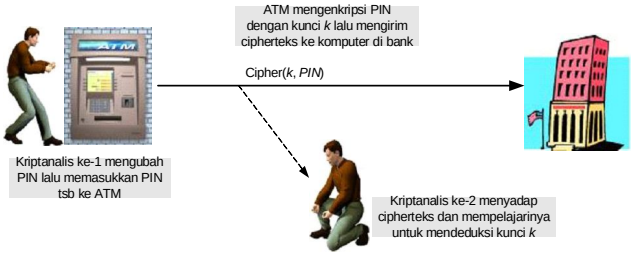
Modus pertama hingga modus keempat merupakan masalah teknis yang tidak terlalu berkaitan dengan masalah kriptografi. Sedangkan modus kelima termasuk salah satu serangan terhadap kriptografi dimana terdapat kriptanalis yang berusaha memecahkan ciphertext yang telah dibuat.

Aksi yang dilakukan oleh pembobol ATM pada modus kelima diatas kurang lebih dapat digambarkan sebagai berikut :

Pertama-tama, kriptanalis ke-1 masuk ke dalam bilik ATM lalu meng-*entry*-kan beberapa alternatif nomor

PIN, baik itu secara acak maupun ditentukan sedemikian sehingga mengarah kepada ditemukannya kunci serta algoritma yang sesuai. Nomor PIN tersebut akan ditransmisikan melalui jaringan dari mesin ATM ke komputer host di pusat data bank. Pada saat yang sama, kriptanalis ke-2 melakukan penyadapan terhadap jaringan tersebut untuk mendapatkan nomor PIN yang telah dienkripsi oleh sistem. Setelah itu para kriptanalis mempelajari padanan antara plaintext dan ciphertext yang telah didapat tadi untuk kemudian melakukan deduksi kunci k.

Proses penyadapan yang dilakukan kriptanalis di atas dapat digambarkan seperti di bawah ini :



Gambar 6. Ilustrasi penyadapan yang dilakukan kriptanalis

Setelah mengetahui kunci k, maka kriptanalis dapat mengetahui nomor PIN masukan pengguna dengan cara melakukan dekripsi terhadap ciphertext dari nomor kunci yang di-*entry*-kan pengguna. Ciphertext itu sendiri didapatkan dari penyadapan kembali.

Dari sini, maka kejahatan pembobolan ATM dapat dilakukan. Kartu ATM nya sendiri dapat diperoleh baik dengan melakukan salah satu modus kejahatan yang disebutkan di atas ataupun dengan pemalsuan kartu.

3. ALTERNATIF SOLUSI

Serangan terhadap kriptografi yang dilakukan oleh para kriptoanalis di atas merupakan serangan terhadap sistem keamanan bank. Oleh karena itu solusi yang dapat ditawarkan adalah dengan memperkuat sistem keamanan dari bank itu sendiri. Algoritma enkripsi yang lebih rumit dan kompleks akan mempersulit para kriptanalis pembobol ATM untuk menemukan kuncinya.

Selain itu, semakin panjang nomor PIN juga semakin aman. Beberapa bank telah menyediakan nomor PIN yang lebih dari 4 angka. Hal ini dapat mempersulit kriptanalis memecahkan kunci.

4. KESIMPULAN DAN SARAN

Pembobolan ATM yang terjadi beberapa waktu ke belakang dilakukan dengan berbagai macam modus/cara, salah satunya adalah dengan melakukan serangan terhadap kriptografi. Kriptanalis menyadap transmisi dari mesin ATM ke *host* bank pusat, kemudian melakukan *chosen plaintext attack* terhadap nomor PIN yang dimasukkan pengguna.

Beberapa solusi yang dapat dilakukan adalah dengan menambah kerumitan algoritma enkripsi nomor PIN, sehingga sulit dipecahkan kuncinya. Selain itu, pemanjangan digit nomor PIN juga dapat mempersulit kriptanalis melakukan pemecahan.

Pada intinya, keamanan juga harus diperhatikan oleh pengguna sendiri. Sedapat mungkin berhati-hati dalam melakukan transaksi di ATM. Dengan demikian dapat menekan angka kejahatan seminimal mungkin.

REFERENSI

[1] Munir, Rinaldi, Slide kuliah IF3058 Kriptografi, Program Studi Teknik Informatika STEI ITB, 2010

[2] Stalling, William, “Cryptography and Network Security”, 4th ed., Prentice Hall

[3] http://id.wikipedia.org/wiki/ATM
diakses pada tanggal 24 Maret 2010

[4] http://one.indoskripsi.com/node/7638
diakses pada tanggal 24 Maret 2010

[5] http://en.wikipedia.org/wiki/Data_Encryption_Standard
diakses pada tanggal 25 Maret 2010