Implementasi Kriptografi dalam Sistem Keamanan Anjungan Tunai Mandiri

Ferdy Efendi[1] dan Nanindya Pramesti Dewanti[2]
[1,2]*Jurusan Informatika, Fakultas KOMPUTER, Universitas Amikom Yogyakarta*
Jl. Ring Road Utara, Condong Catur, Sleman, Yogyakarta
E-mail : Ferdyefendi10@gmail.com[1], Naninprmst6@gmail.com[2]

Abstract—In the current modern era, the Automated Teller Machine, or often called as an ATM, deals with online transactions which are certainly very vulnerable to security. So to prevent it a barrier is needed and one of the fields in computer science is used, it is Cryptography. The creation of a security system at the Automated Teller Machine uses one of the DES (Data Encryption Standard) cryptographic algorithms, with using the Personal Identification Number (PIN) method. Where to use cards with magnetic ribbons that save the card numbers, PIN, and security data for accessing Automated Teller Machine. On the bank side when making a PIN owned by a bank customer, it is done with encrypting the DES algorithm, which is saved on the magnetic tape contained in the ATM card. When a transaction occurs, the ATM will be connected to a banking network to communicate with the bank's computer server.

Abstrak—Tujuan penulisan karya tulis ini untuk memaparkan implementasi kriptografi dalam sistem keamanan Anjungan Tunai Mandiri. Di era modern saat ini, Anjungan Tunai Mandiri atau yang sering disingkat menjadi ATM ini bergelut dalam transaksi online yang tentu sangat rawan keamanannya. Dalam hal ini berarti terdapat banyak jalur untuk dapat menerobos sistem keamanannya, maka untuk mencegahnya diperlukan suatu tembok penghalang dan dipakailah salah satu bidang dalam ilmu komputer yaitu Kriptografi. Pembuatan Sistem keamanan pada Anjungan Tunai Mandiri ini menggunakan salah satu algoritma kriptografi DES (*Data Encryption Standart*), dengan menggunakan metode *Personal identification number* (PIN). Dimana mennggunakan kartu dengan pita magnetic yang menyimpan nomor kartu, PIN, dan data keamanann untuk pengaksesan ATM. Pada sisi bank saat pembuatan PIN milik nasabah bank, dilakukan dengan enkripsi algoritma DES tadi, yang disimpan pada pita magnetik yang terdapat dalam kartu ATM. Saat terjadi transaksi, ATM akan terhubung dengan jaringan perbankan untuk berkomunikasi dengan komputer server bank. Sehingga data PIN yang ada dalam kartu ATM akan dicocokkan dengan yang ada dalam server bank. Jika cocok, maka server akan memperbolehkan transaksi berlangsung.

Kata Kunci— ATM, Metode PIN, DES, Sistem Keamanan.

I. PENDAHULUAN

A. Latar Belakang

Dalam sebuah bank rasa nyaman pelanggan atau nasabah adalah no 1, tidak terkecuali masalah kerahasian dan keamanan saat melakukan sebuah pertukaran data. Dimana kerahasian dan keamanan saat melakuakn pertukaran data adalah hal yang sangat penting dalam komunikasi data, karena disitu terdapat privasi individu setiap orang. Salah satu caranya adalah dengan menggunakan enkripsi, yang didasarkan dari algoritma kriptografi.

Enkripsi sendiri adalah suatu pengubahan suatu data berisi karakter menjadi data karakter yang tidak dapat dikenali atau dibaca. Algoritma enkripsi yang biasanya digunakan DES, Triple DES, IDEA, dan Blowfish. Pada karya tulis ini akan membahas system keamanan Anjungan Tunai Mandiri (ATM). Para pengguna ATM biasanya tidak memikirkan seberapa sulit algoritma yang digunakan dalam pengimplementasiannya, yang mereka pikirkan adalah bagaimana keamanan data mereka. Sistem keamanannya sendiri memerlukan kartu yang terdapat pita magnetic didalamnya, yang berisi informasi pengguna dan PIN, dalam penggunakan pin adalah dengan metode enkripsi DES (Data Encryption Standart).

Untuk menyisipkan gambar, tempatkan kursor pada titik yang dituju kemudian pilih di antara: *Insert* | *Picture* | *From File* atau kopi gambar ke *clipboard* lalu pilih *Edit* | *Paste Special* | *Picture* (dengan “float over text” tidak dicentang).

B. Rumusan Masalah

1. Apa itu kriptografi?.
2. Bagaimana sistem keamanan di ATM?.
3. Apa saja serangan pada keamanan sistem keamanan ATM?

C. Tujuan Penulisan

1. Pembaca dapat memahami dan mengenal kriptografi.
2. Pembaca dapat mengetahui bagaimana sistem dan cara kerja keamanan di ATM.
3. Pembaca dapat mengetahi macam – macam serangan pada sistem keamanan di ATM.

II. METODE PENELITIAN

Dalam menjamin kemanan pada ATM digunakanlah metode enkripsi data berbasis kriptografi dengan Teknik DES (*Data Encryption Standard*). Teknik DES sendiri adalah sebuah standart algoritma enkripsi didasarkan pada algoritma simetri. Dan algoritma kriptografi simetri digunakan pada pemrosesan terhadap bit dalam bentuk *block cipher*, dimana DES sendiri beroperasi menggunakan blok 64-bit*plaintext* dan menggunakan kunciblok eksternal (*Eksternal Key*) 64-bit juga, serta menggunakan 56-bit kunci block internal (*Internal Key*).Adapun sebutan lain, *plain text* untuk pesan asli dan *chipertext* untuk pesan yang telah diubah.

DES memiliki skema umum sebagai berikut:

1. Blok *plaintext*dipermutasi dengan matrik permutasi awal (*Initial Permutation*/IP).
2. Hasil tadi kemudian di proses enciphering dengan melakukan 16 kaH (putaran),dimana setiap putaran memiliki *internal key* yang berbeda-beda.
3. Hasil encipheiring tersebut akan di perutasi lagi dengan matrik permutasi balikan (*invers initial permutation*) dan akan menjadi blok eksternal.

Di dalam proses enciphering sendiri, blok plaintext akan terbagi menjadi 2 bagian, yaitu L (kiri) dan R (kanan), yang mana akan menjadi 32 bit panjangnya, didasarkan dari model jaringan Feistel. Dimana di dalam jaringan Feistel ini digunakan *internal key* terhadap fungsi transformasinya.Selanjutnya, *internal key* tadi setelah dibangkitkan akan digunakan sebagai fungsi f dalam algoritma DES.

$\mathbf{L_i = R_{i-1}}$
$\mathbf{R_i = L_{i-1} + f(R_{i-1}, K_i)}$
Keterangan:
L = blok kiri (*left*)
R = blok kanan (*right*)
I = jumlah putaran
K_i = *key* pada putaran ke-i

Secara garis besar proses *enciphering* adalah proses pada model jaringan Feistel, yang memiliki rumus:

Satu putaran DES adalah perumpaan dari model jaringan Feistel sendiri, dimana jika (L,6, R,6) adalah keluaran putarab terakhir (ke-16), maka (R,6, L,s) termasuk *pra chipertext* dari *enciphering* itu sendiri. Dimana*chipertext* diperoleh dari permutasi awal balikan IP-1 terhadap blok *pre chipertext.* Berikut adalah skema 1 putaran DES:

Sedangkan proses pembangkitan kunci dilakukan dengan *external key* sebelumnya,dilakukan dengan permutasi dan pergeseran bit ke kiri. Seperti skema berikut:

Misalkan kita mempunyai *external key* yang terdiri dari 64-bit kita sebut saja Z, dimana *external key* ini digunakan untuk masukan untuk permutasi dengan matriks permutasi kompresi PC-1 berikut :

6	17	11	42	31	48	28	38	13	45	25	53	18	9
32	12	40	2	16	7	43	24	20	52	3	33	39	26
22	30	56	47	41	19	1	50	44	27	46	54	4	35
5	36	15	29	49	21	37	34	8	51	23	14	55	10

Dalam permutasi ini, tiap bit ke-8 diabaikan, dan hasil permutasinya adalah 56 bit, sehingga panjang kunci DESnya adalah 56 bit. Dan dibagi menjadi dua, yang masing – masing mendapat 28 bit kiri dan kanan, dan disimpan dalam DO dan CO yang berisi:

CO : 6, 17, 11, 42, 31, 48, 28, 38, 13, 45, 25, 53, 18, 9
32, 12, 40, 2, 16, 7, 43, 24, 20, 52, 3, 33, 39, 26

DO : 22, 30, 56, 47, 41, 19, 1, 50, 44, 27, 46, 27, 46,
54, 4, 35
5, 36, 15, 29, 49, 21, 37, 34, 8, 51, 23, 14, 55, 10

Yang selanjutnya, kedua bagian itu (CO dan DO) akan digeser ke kiri (*left shift*) sesuai bit tiap putaran.

III. HASIL DAN PEMBAHASAN

A. Pengertian kriptografi

Sebelumnya kriptografi sendiri adalah salah satu algoritma kemananan data informasi yang dimana berkerja menjadikan pesan menjadi kode yang rumit dan susah dipahami untuk mencegah pencurian pesan, dan ketika pesan tersebut dibutuhkan oleh pemilik atau yang berhak menerima maka kode tersebut akan kembali ke bentuk semula atau istilah lainnya adalah enkripsi sedangkan pengembalian kode ke pesan disebut dekripsi. Algoritma kriptografi sendiri dibagi menjadi 3 jenis, yaitu:

(a) Algoritma Simetris

Dimana algoritma ini tidak ada pengubahan kunci dalam proses enkripsi maupun dekripsi dalam artian kuncinya masi sama, sehingga banyak pihak yang mulai meragukan keamanan algoritma jenis ini. Contoh algoritmanya adalah *Data Encryption Standart*(DES), *International Data Encryption Algorithm*(IDEA), Twofish, dll.

(b) Algoritma Asimetris

Algoritma ini bisa disebut kebalikan dari algoritma simetris, yang mana penggunaan kunci

berbeda pada proses enkripsi maupun deskripsi. Contohnya *Digital Signature Algorithm*(DSA), Rivest-Shamir-Adleman(RSA), Diffie-Hellman, dll.

(c) Fungsi Hash

Termasuk dalam fungsi matematika dimana mengambl suatu input Panjang dan mengubahnya ke dalam bentuk biner yang mana panjangnya tetap. Contoh umumnya dalam *Massage Digest 5*(MD5).

B. Keamanan ATM

Sesuai topik, kita akan membahas sistem keamanan di ATM. Sistem keamanan di ATM sendiri menggunakan implementasi dari kriptografi dengan metode *Data Encryption Standart*(DES). Seperti yang kita ketahui ATM sendiri umunya menggunakan PIN sebagai basic keamanannya yang menggunakan 4 digit angka, yang mana dalam penggunaan PIN tersebut menggunakan algoritma kriptografi simetris dengan metode DES. Berikut adalah prosesnya :

1. Sistem mengambil 5 digit terakhir dari nomor rekening.
2. Sistem akan menggabungkan kelima angka tersebut dengan 11 digit dari data valisasi yang diciptakan sendiri.
3. Maka total akan terdiri dari 16 angka yang kita sebut saja 16 bit, yang akan menjadi kunci PIN untuk dimasukkan dalam algoritma DES.
4. Hasil pemrosesan sebelumnya oleh DES akan diambil 4 digit pertama, yang kemudian diubah ke bentuk decimal, dan akan diubah lagi ke dalam bentuk heksadesimal oleh DES. Yang kemudian 4 digit tersebut disebut "PIN alami".
5. Kemudian dari PIN alami tersebut ditambah dengan 4 digit baru yang disebut *offset* dan kemudian mengahasilkan PIN yang siap digunakan oleh nasabah.

Contoh :
Nasabah A ingin membuat sebuah ATM, dia telah memiliki rekening dengan nomor 4506602100091715. Proses yang akan terjadi adalah sebagai berikut :

1. Dari nomor rekening 4506602100091715 akan diambil 5 digit terakhir, yaitu 91715.
2. Lima digit tadi akan digabung dengan 11 dikit data validasi 88070123456 maka akan menjadi 8807012345691715 yang terdiri dari 16 digit.
3. Telah tersedia dari algoritma DES "Kunci PIN" yaitu FEFEFEFEFEFEFEFE yang sama-sama terdiri dari 16 digit. Dan akan diproses diubah bentuknya oleh metode DES sampai ke A2CE126C69AEC82D, dan akan diambil 4 digit pertama untuk di proses lagi oleh algoritma DES untuk dapat "PIN Alami" yaitu 0224.
4. Dan "PIN Alami" tersebut ditambahkan dengan *offset*nya 6565.
5. 0224 + 6565 = "6789" yang mana itu adalah nomor PIN nasabah.

Dan nomor tersebut akan disimpat ke dalam pita magnetik yang terdapat pada kartu ATM, Bersama dengan data penting lainnya semacam nomor rekening, nomor kartu, dll.

C. Ancaman pada Sistem Keamanan ATM

Seperti sebuah kata dalam sebuah film "*No System is Safe*" yang dikutip dari film Who Am I (2014), mungkin bisa menjadi judul yang tepat untuk topik ini. Bahwasannya setiap sistem itu tidaklah sempurna, kita cuma bisa membuatnya menjadi sulit ditembus dan mencegah agar tidak terjadi, tetapi bukan berarti tidak bisa di tembus. Begitu juga pada sistem keamanan ATM ini, yang tidak akan bisa menjamin 100% akan aman.

Berbagai bentuk kecurangan ataupun kejahatan pada sistem keamanan ATM ini juga tidaklah sedikit, mulai dari kasus fisik seperti pencurian, perampokan, pencopetan, untuk memaksa korban sampai pada penggunaan teknologi mulai dari yang sederhana sampai yang canggih untuk mengetahuinomer rekening maupun PIN ATM korban.

Berikut ini ada beberapa jenis ancaman dalam bentuk teknologi terhadap sistem keamanan ATM :

1) Mengambil uang nasabah

Yang dimaksud disini bukan cara fisik seperti penodongan, pencurian, pemaksaan, dll, tetapi lebih menggunakan teknologi untuk mengakalinya. Dimana pelaku membuat sejenis duplikasi dari tempat keluarnya uang di ATM, dan digunakan untuk menyimpan uang milik nasabah. Sehingga yang terjadi uang tidak akan keluar tetapi akan masuk ke alat duplikatnya tempat menyimpan uang, dan nasabah akan tidak curiga karena mengira bahwa uang yang ada di ATM itu telah habis dan pergi begitu saja. Setelah itu pelaku akan mengambil uang itu, pada tengah malam.

2) Menggunakan alat untuk mengambil kartu nasabah

Disini pelaku memprioritaskan untuk mengambil kartu milik korban, yang dimana pelaku membuat sejenis alat" yang bisa mengakali seolah olah kartu milik korban tertelan oleh mesin ATM, sehingga ATM yang telah dimasukkan akan tertahan di dalam mesin ATM.

Pelaku biasanya menggunakan semacam strip tipis atau sejenis plastik film (*Lebanese Loop Method*) yang

berguna menghalangi slot di mesin ATM, tetapi orang Indonesia menggunakan alat yang lebih sederhana yaitu menggunakan batang korek api untuk menyumbat kartu ATM, sebenranarnya penggunaan plastik film lebih efektif karena plastic film memiliki ketahanan dan tidak mudah terkoyak disamping itu juga lebih tipis, sehingga korban tidak menyadari bahwa ada plastic film di mulut mesin tersebut. Selanjutnya setelah pelaku berhasil menghalangi kartu tersebut untuk keluar, pelaku membutuhkan nomor PIN agar pelaku bisa leluasa mengambil uang milik korban.

Ada beberapa metode kejahatan untuk mendapatkan nomor PIN korban, yaitu :

a) Modus menolong

Setelah kartu ATM milik korban tertelan mesin ATM, maka korban akan panik dan bingung, disitulah peran saat pelaku untuk masuk dan menwarkan bantuan dan memberi solusi kepada korban, yang bahkan meminta nomor PIN korban. Dan korban yang sudah panik akan menurut saja kepada pelaku yang berpura-pura menolong korban.

b) Memempelkan stiker *Call Center* palsu

Di modus kejahatan ini, setelah korban bingung dan panik karena ATMnya tertelan, korban biasanya akan langsung menghubungi Call Center yang nomornya dipasang di mesin ATM, korban yang dalam keadaan panik dan tidak tau bahwa nomor tersebut telah di sabotase, akan menelfon nomor tersebut yang tersambung ke pelaku, disitulah pelaku beraksi untuk mendapatkan nomor PIN korban.

c) Memasang kamera

Pelaku kejahatan memasang kamera perekam kecil untuk merekam korban saat memasukkan PIN ATMnya, tempat pelaku biasanya memasang kamera diatas keypad dimana korban tidak akan menyadari baahwa ada kamera disitu, karena sejatinya bagian di atas keypad mesin ATM dipasang untuk menutupi nasabah saat memasukkan nomor PIN.

d) Memasangkeypad palsu

Metode ini berja dimana pelaku memasang keypad palsu tepat diatas keypad asli, sehingga korban tidak sadar bahwa saat memasukkan PIN secara tidak langsung juga akan menekan di keypad palsu. Didalam keypad palsu tersebut saat ditekan akan langsung terekam dan langsung dikirimkan ke server pelaku.

3) Metode Skimmer

Salah satu metode yang paling terkenal dan paling canggih dalam segi teknologi untuk mendapatkan informasi mengenai kartu ATM, seperti yang diketahui bahwa kartu ATM memuat informasi penting seperti nomor rekening, nomor PIN, dll. Metode ini bekerja dengan menempelkan alat yang bernama skimmer di letakkan di mulut mesin ATM, yang berguna untuk medapatkan semua informasi yang berada di kartu ATM korban dengan menscandata yang ada di pita magnetiknya. Setelah pelaku mendapatkan data tersebut, pelaku akan menduplikasi kartu ATM milik korban dengan memasukkan data informasi yang didapat tadi ke kartu ATM korban. Sehingga korban tidak akan menyadari karena kartu yang asli masih dipakai selayaknya, dan korban akan bisa terus menggunakan uang yang ada pada kartu ATM tersebut.

IV. KESIMPULAN

Dari semua apa yang dibahas diatas, mengenai implementasi kriptografi dalam sistem keamanan Anjungan Tuna Mandiri didapatkan bahwa sistem keamanan Anjungan tunai mandiri (ATM) masih menggunakan implementasi dari kriptografi dengan metode *Data Encryption Standart*(DES) yang mana didasarkan pada lagoritma simeti yang kuncinya tidak berubah saat proses enkripsi maupun dekripsi. Selain itu dengan perkembangan teknologi enkripsi, perkembangan kejahatan pun juga semakin berkembang khususnya pada sistem keamanan ATM, yang memiliki berbagai jenis ancaman yang dapat merugikan nasabah.

DAFTAR PUSTAKA

[1] http://ilmu-kriptografi.blogspot.com/2009/05/algoritma-des-data-encryption-standart.html
[2] http://nakita.grid.id/read/0230240/hati-hati-ini-4-modus-kejahatan-di-atm-yang-paling-sering-terjadi?page=all
[3] https://www.indo-blogger.com/2016/11/metode-mebobol-atm-yang-biasa-dilakukan-penjahat.html
[4] http://yolandaaprinusa.blogspot.com/2017/01/permutasi-des.html
[5] https://www.komentarmu.com/contoh-abstrak/