Kriptografi pada Sistem ATM

13517090 Vania Velda[1]
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
[1]13517090@std.stei.itb.ac.id

Abstrak—Kegiatan perbankan saat ini tidak dapat terlepas dari kegiatan sehari hari masyarakat. Saat ini, kegiatan perbankan telah berkembang dapat dilakukan dari via Internet. Dalam melakukan transaksi, perbankan perlu memiliki sistem keamanan yang tinggi baik pada lokasi bank maupun pada saat transaksi demi kenyamanan dan keamanan para nasabah. Salah satu masalah utama yang harus dipikirkan adalah keamanan dalam melakukan transaksi serta proteksi terhadap data nasabah. Karenanya, saat ini transaksi perbankan secara online maupun melalui ATM telah menerapkan sistem kriptografi untuk meningkatkan keamanan transaksi.

***Keywords*—ATM,keamanan,kriptografi,perbankan,transaksi.**

I. PENDAHULUAN

Perbankan merupakan salah satu industri tertua dimana sejarah mencatat kemunculan sistem perbankan pertama kali pada 2000BC saat para pedagang memberikan pinjaman beras untuk petani dan pedagang melakukan pernjualan antar kota pada daerah Assyria dan Babylonia. Perkembangan sistem perbankan yang awalnya merupakan suatu sistem barter sederhana terus berkembang dan menjadi suatu model internet *banking* yang kita ketahui saat ini.

Tahun 2001 merupakan tahun yang memberikan dampak terbesar pada industri perbankan dikarenakan adanya krisis ekonomi global. Pada 10 tahun belakang, bank terus mengumpulkan data mengenai nasabah, *channel* ,situasi finansial dan resiko. Dengan bantuan dari perkembangan teknologi, data yang dikumpulkan data dianalisis dan diatur secara efektif. Selain itu, perkembangan yang paling dirasakan pada beberapa tahun belakang adalah adanya kemunculan transaksi *cashless* menggunakan e-banking maupun kartu ketika melakukan transaksi.

Saat ini, E-banking telah sangat berkembang dimana sistem E-banking memungkinkan transaksi dapat dilakukan melalui internet. Keamanan dan privacy menjadi fitur dasar yang harus dipenuhi pada sistem e-banking. Salah satu untuk meningkatkan keamanan dan menjaga privacy adalah dengan melakukan enkripsi informasi data. Selain itu, keamanan dapat didapatkan dalam bentuk password, tanda tangan digital , kode pin dan sebagainya.

Ketika melakukan transsaksi, selain dari pembayaran tunai, menggunakan kartu elektronik pada tahun belakang meningkat. Pihak bank memberikan berbagai promosi dan berbagai penawaran menarik apabila nasabah membuat kartu kredit maupun melakukan transaksi menggunakan kartu kredit atau kartu debit. Berkat promosi yang dilakukan, penggunaan kartu dalam transaksi meningkat sehingga sistem perbankan terus menerus meningkatkan keamanan ketika melakukan transaksi menggunakan kartu.

Adanya kebutuhan melakukan enkripsi menjadikan kriptografi berperan penting dalam sistem perbankan dan di berbagi service keuangan untuk memastikan data transaksi dapat diproses secara aman. Kriptografi secara singkatnya merupakan suatu ilmu untuk menyamarkan pesan agar tidak dapat dibaca oleh pihak lain yang bukan penerima pesan.

Prinsip kerja dari kriptografi adalah enkripsi dan dekripsi dimana enkripsi merupakan proses untuk mengubah data informasi menjadi data yang tidak dapat dibaca atau disebut *cipher* sedangkan dekripsi merupakan proses untuk mengubah *cipher* menjadi data semula.Sistem perbankan saat ini telah menggunakan enkripsi data menggunakan metodologi kriptografi yang kuat pada sistem komunikasi untuk memastikan transaksi data aman dan menghindari adanya manipulasi oleh pihak yang tidak diinginkan.

II. DASAR TEORI

A. AES

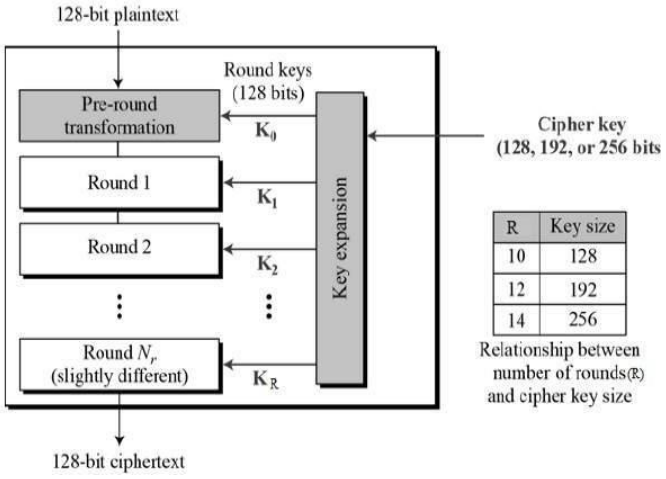
Dikembangkan pertama kali oleh NIST (National Institute of Standards and Technology) pada tahun 1997, Advanced Encryption Standard atau AES merupakan algoritma block cipher simetris yang dipilih oleh pemerintah US untuk menjaga informasi penting. AES dirancang agar mudah diimplementasikan pada hardware dan softaware hingga pada *smart card* sebagai pengganti dari DES yang semakin rentan terhadap serangan *brute force*.

AES terdiri dari 3 jenis block cipher yaitu AES-128, AES-192 serta AES-256. . Masing-masing cipher memiliki ukuran 128-bit, dengan ukuran kunci masing-masing 128, 192, dan 256 bit. Setiap cipher akan melakukan enkripsi dan dekripsi data pada blok 128 bit menggunakan ukuran kunci 128,192 dan 256 bits.Dikarenakan AES merupakan algoritma kunci simetris, maka kunci rahasia yang digunakan untuk enkripsi dan dekripsi adalah sama sehingga pengirim dan penerima wajib mengetahui kunci rahasia.

Konsep dari AES adalah adanya penggunaan *round table*.Semakin panjang key,maka semakin banyak jumlah putaran yang diimplementasikan. Satu *round* terdiri dari beberapa operasi yakni *substitution*, *transpose*, dan campuran dari input plaintext untuk menghasilkan ciphertext akhir.

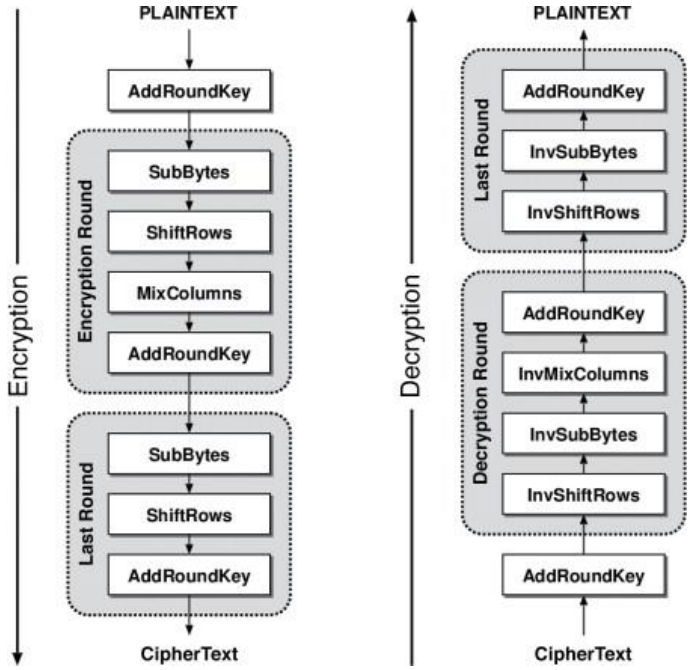
	Jumlah Putaran (Nr)
AES-128	10
AES192	12
AES-256	14

Tabel perbandingan jumlah putaran per block cipher AES



Gambar A Struktur semantik dari AES
Sumber :
https://www.tutorialspoint.com/cryptography/advanced_encryption_standard.htm

1. Proses Enkripsi
   Proses enkripsi pada AES menggunakan konsep *round*. Secara general, setiap *round* terdiri dari 4 sub proses. Adapun sub proses pada suatu round adalah sebagai berikut:
   a. Substitution
      Substitution yang dilakukan merupakan *byte substitution* dimana dilakukan pengganti byte secara non linear yang dilakuakn secara individual pada setiap rount menggunakan sebuah tabel *substitution* atau tabel S. Hasil dari proses ini adalah sebuah matrix berukuran nxn. Input bytes berukuran 16 (dikarenakan dalam blok 128 bits) maka hasil matrix nya adalah 4x4.
   b. Transpose
      Transpose matrix dari hasil dari proses sebelumnya. Adapun transpose yang dilakukan ada dua yakni *shiftrows* serta *mixcolumns*. *Shiftrows* merupakan proses menggeser row pada matrix kekiri dimana baris pertama tidak akan digeser, baris kedua akan di geser satu byte ke kiri, baris ketiga akan digeser dua byte ke kiri dan baris terakhir atau baris keempat akan digeser tiga byte ke kiri. Untuk *mixcolumns*, setiap kolom akan di transformasi menggunakan perkalian matrix ditambah dengan operasi bitwise XOR pada hasil perkalian. Adapun perkalian yang dilakukan antara matrx 4x4 dengan format *Gallois field* dengan setiap data kolom matrix 4x1. Operasi *mixcolumns* tidak akan dilakukan pada putaran terakhir
   c. *Add round key*
      Hasil matrix yang di transpose kemudian akan di XOR dengan subkey pada round tersebut.
2. Proses Dekripsi
   Proses dekripsi pada AES mirip dengan proses enkripsi dengan perbedaan urutan langkah yang dilakukan merupakan kebalikan dari proses enkripsi.

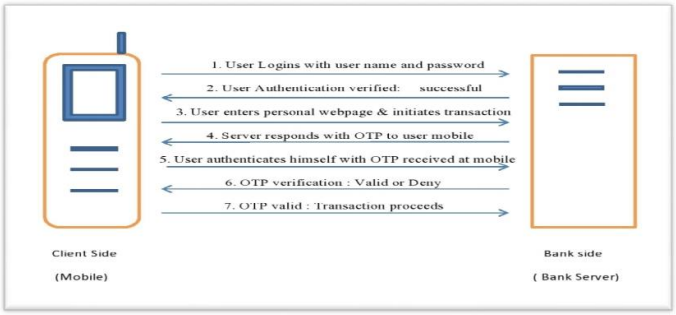


Gambar B Proses enkripsi dekripsi pada AES
Sumber [2]

B. OTP

OTP atau *One Time Password* merupakan suatu mekanisme untuk masuk ke dalam network atau service menggunakan password yang hanya dapat digunakan sekali. Untuk setiap login yang dilakukan dengan kredential yang sama, password yang diberikan akan selalu berubah. Panjang password yang diberikan beragam denga minimal panjang nya adalah 4 angka acak dengan memiliki batas waktu untuk menginput OTP pada service.

Penggunaan OTP diharapkan dapat menambah keamanan pada saat melakukan transaksi. Umumnya, OTP dikirimkan melalui SMS ke nomor pengguna yang telah terdaftar.



Gambar C Skema OTP dari server bank ke client
Sumber : https://www.rroij.com/open-access/otp-encryption-techniques-in-mobiles-forauthentication-and-transaction-security.pdf)

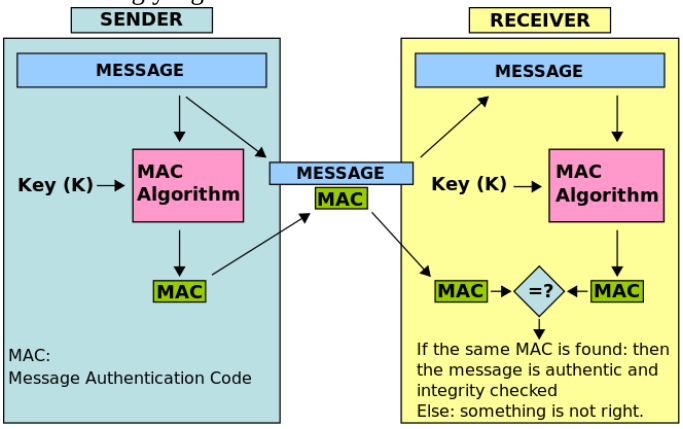
OTP rentan terhadap serangan *man-in-the-middle*. Selain itu, keamanan OTP bergantung pada pengguna dimana pengguna terkadang rentan terhadap *phising* dimana pengguna memberikan kode OTP mereka kepada pihak lain ketika melakukan transaksi.

C. MAC

Message Authentication Code atau MAC merupakan kode yang dihasilkan oleh fungsi hash satu arah dengan menggunakan kunci rahasia dalam melakukan pembangkitan nilai hash.

Kegunaan dari MAC adalah memastikan integritas informasi dimana informasi yang dikirimkan tidak mengalami perubahan. MAC biasanya dibutuhkan untuk berbagai akses yang berhubungan dengan finansial.

Terdapat tiga algortima dasar dari MAC, algoritma untuk mengenerate key, algoritma *signing* serta algorima *verifying*. Algoritma *signing* berfungsi untuk mengirimkan tag ketika diberikan kunci dan pesan sedangkan algoritma *verifying* berfungsi untuk memverifikasi originalitas pesan berdasarkan kunci dan tag yang diberikan.



Gambar D Penggunaan MAC
Sumber [3]

D. Kartu elektronik

Setiap bank memberikan kartu elektronik untuk transaksi bagi nasabahnya. Adapun jenis kartu yang biasanya diberikan adalah kartu debit serta kartu kredit. Kartu debit digunakan untuk melakukan penarikan tunai di ATM. Pada saat ini, pada bank tertentu, kartu kredit dapat digunakan untuk melakukan penarikan tunai. Kedua kartu tersebut dapat digunakan ketika melakukan transaksi.

Setiap kartu elektronik berupa kartu plastik yang memenuhi standar ISO/IEC 7810 ID-1 dengan magnetic chip didalamnya.Setiap kartu memiliki algoritma kriptografi sendiri. Umumnya untuk menjaga komunikasi ketika melakukan transaksi, terdapat dua model yang digunakan yakni kartu yang menggunakan MAC serta kartu yang menggunakan tanda tangan digital.

Adapun pada setiap kartu memiliki 16 digit angka yang berperan penting ketika melakukan transaksi menggunakan kartu. 16 digit angka tersebut di generate menggunakan alrgoritma Luhn untuk memastikan bahwa akun nasabah merupakan akun yang legal.

Kartu yang menggunakan algoritma kriptografi simetris memiliki pengenal statik yang telah ditanda tangani oleh *card issuer* dimana ketika saat melakukan transaksi akan dikirimkan. Setiap kartu memiliki nilai rahasia yang hanya diketahui oleh bank dimana nilai tersebut akan digunakan sebagi kunci untuk melakukan MAC pada detil transaksi.

Model yang kedua yakni kartu dengan tanda tangan digital memiliki kunci privat yang tidak diketahui oleh pihak manapun termasuk pihak bank yang mengeluarkan kartu. Kunci publik yang berkorespon di sertifikasi oleh bank.

Gambar E Contoh Kartu Kredit
Sumber : https://www.cimb.com.my/en/personal/day-to-day-banking/cards/credit-card.html

Pada saat ini, setiap transaksi penarikan tunai maupun ketika menggunakan kartu ketika melakukan transaksi pembelanjaan memerlukan inputan pin. Walau sepertinya tergolong aman, namun penulis merasa bahwa hal tersebut masih memiliki celah dan diperukan suatu layer tambahan dikarenakan transaksi masih dapat dilakukan oleh pihak lain meskipun membutuhkan pin dalam melakukan transaksi.

E. ATM

Automated Teller Machine atau yang lebih dikenal sebagai ATM merupakan service yang diberikan dari instansi keuangan agar nasabah dapat melakukan penarikan tunai dan lainnya yang beroperasi 24 jam.

Kartu elektronik untuk melakukan transaksi di ATM memiliki data PIN dari akun tersebut. Namun untuk mendapat PIN dari kartu, hal tersebut tidak mungkin dilakukan. Hal ini dikarenakan tiap bank memiliki proses enkripsi tersendiri untuk mengenkripsi PIN yang ada pada kartu. Umumnya enkripsi dilakukan dengan bantuan dari Triple DES maupun dengan AES.

ATM melakukan komunikasi dengan central host melalui Internet Service Provider atau ISP dimana semua network ATM tersedia bagi pengguna. Mesin ATM terhubung dengan central host melalui kabel telepon menggunakan modem.Ketika pengguna melakukan transaksi, pengguna memberikan detail PIN ditambah dengan kartu elektronik. Mesin ATM akan merequest ke bank nasabah melalui central host. Apabila nasabah ingin menarik tunai, central host akan melakukan *electronic fund transfer* dari akun bank nasabah ke akun dari ATM central host. Setelah transfer berhasil, central host akan mengirimkan kode persetujuan ke mesin atm untuk mengeluarkan tunai.

Gambar F Arsitektur ATM
Sumber : https://www.elprocus.com/automatic-teller-machine-types-working-advantages/#:~:text=When%20a%20cardholder%20wants%20does,through%20card%20reader%20and%20keypad.&text=Once%20the%20funds%20are%20transferred,machine%20to%20dispense%20the%20cash.

F. *Card Skimming Attack*

Skimming merupakan suatu tindakan menggunakan *skimmer* untuk mengambil data dari magnetik strip pada kartu elektronik secara ilegal. Permasalahan ini mudah terjadi pada saat kita melakukan transaksi di restoran dikarenakan kartu yang kita gunakan dibawa pergi ketika sedang membayar. Apabila server yang digunakan merupakan *skimmer*, sebelum kartu dikembalikan kepada kita, data yang ada pada magnetik strip dapat diambil. Data yang berhasil diambil tersebut kemudian dapat dijual maupun dikopikan ke kartu kosong yang memiliki magnetik strip yang kemudian dapat digunakan untuk melakukan transaksi.

III. RANCANGAN

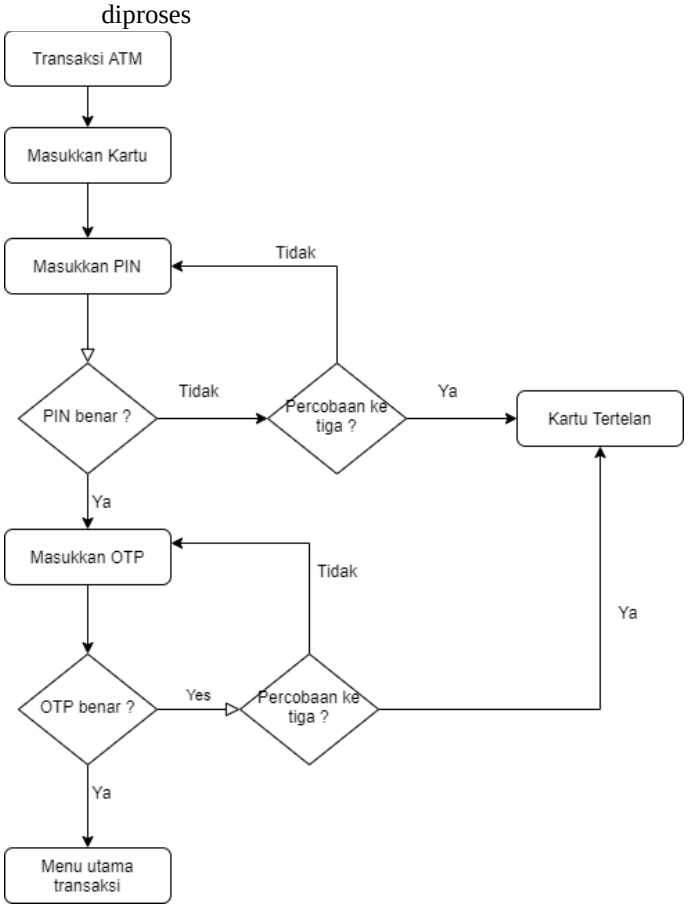
Pada bagian ini, penulis akan memberikan gambaran menambah layer keamananan ketika melakukan transaksi menggunakan kartu baik pada saat penarikan tunai maupun pada saat melakukan transaksi pembelian.

A. Transaksi ATM

Transaksi pada ATM saat penarikan tunai memerlukan dua hal, yaitu kartu eletronik dan PIN sebelum melakukan transaksi. Walaupun terkesan aman, penarikan tunai di ATM dapat diakali dengan pembuatan kartu palsu yang identik dengan kartu original. Apabila PIN tidak sengaja maupun sengaja tersebar, ditambah dengan kartu palsu tersebut maka transaksi di ATM dapat dilakukan. Hal ini dikarenakan untuk melakukan transaksi hanya membutuhkan kartu elektronik ditambah dengan PIN. Untuk menambah keamananan, penulis mempropose penambahan penggunaan OTP ketika melakukan transaksi.

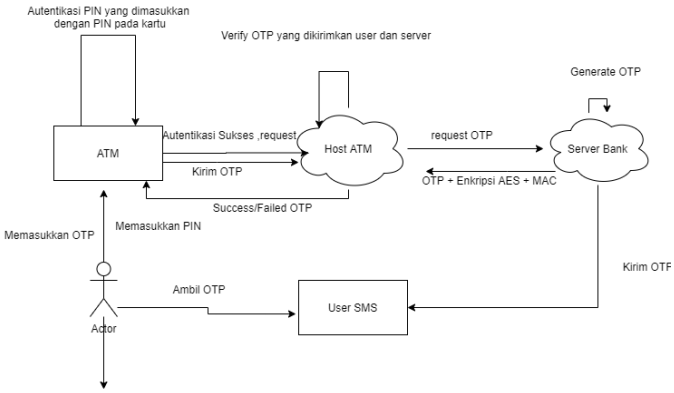
Adapun proses transaksi dengan penambahan OTP sebagai berikut:

1. Pengguna memasukkan kartu elektronik
2. Pengguna memasukkan PIN
3. Pengguna memasukkan OTP
4. Pengguna melakukan transaksi yang diinginkan
5. Pengguna memasukkan PIN sebelum transaksi diproses



Gambar G Skema Proses Transaksi dengan OTP

Komunikasi antara ATM dengan central host melalui ISP. .Ketika pengguna melakukan transaksi, pengguna memberikan detail PIN ditambah dengan kartu elektronik. Mesin ATM akan merequest ke bank nasabah melalui central host. Pada server bank nasabah, akan digenerate pin OTP dan dikirimkan ke sms nomor pengguna dari nasabah serta ke host ATM dalam bentuk terenkripsi menggunakan AES dan ditambahkan dengan MAC. Penambahan enkripsi ini dengan tujuan agar tidak ada yang dapat mengambil OTP pada saat dikirimkan.Sedangkan penambahan MAC untuk memastikan integritas dari informasi yang dikirimkan. Setelah pemasukkan OTP, akan dilakukan pengirimkan ke host ATM dalam bentuk terenkripsi menggunakan AES. Dekripsi akan dilakukan pada host ATM menggunakan kunci yang telah diassign pada host. Apabila OTP yang dimasukkan salah sebanyak 3x, kartu elektronik akan ditelan oleh mesin dan dilakukan pemberitahuan ke email dari nasabah. Jika benar, maka nasabah dapat melakukan transaksi. Ketika nasabah ingin menarik tunai, central host akan melakukan *electronic fund transfer* dari akun bank nasabah ke akun dari ATM central host. Setelah transfer berhasil, central host akan mengirimkan kode persetujuan ke mesin atm untuk mengeluarkan tunai.



Gambar H Rancangan Arsitektur Sistem

IV. ANALISIS RANCANGAN

Pada bagian ini, akan dibahas mengenai keuntungan dan kerugian dari rancangan yang dibahas pada bagian sebelumnya.

Pertama, penggunaan algoritma AES dan bukan algoritma lain untuk melakukan enkripsi OTP yang dilakukan dikarenakan algoritma AES memiliki kecepatan hingga 6 kali lebih cepat dari algoritma DES. AES menyediakan ukuran kunci yang lebih besar ditambah memastikan bahwa cara untuk mendekripsi pesan oleh pencuri data adalah mencoba segala kemungkinan kunci.Selain itu, saat ini algoritma DES telah rentan oleh serangan bruteforce.

	AES-256	DES
Kombinasi	2^{256}	2^{56}
Ketahanan Brute force	Mustahil	Dapat dilakukan <1 hari

Tabel perbandingan AES-256 dengan DES

AES-256 seharusnya sudah cukup aman. Namun, implementasi sistem AES ini haruslah benar untuk menghindari kemungkinan serangan *possible related-key*.

Penambahan OTP untuk lebih membuat transaksi aman. Ketika kartu yang kita gunakan mengalami *card skimming attack*, pencuri tidak akan dapat langsung melakukan transaksi di ATM. Hal ini dikarenakan, walau pencuri memiliki salinan kartu dan pin kita, untuk melaksanakan transaksi diperlukan OTP. Ketika kita dikirimkan OTP transaksi padahal kita tidak melakukan transaksi, maka kita dapat mengetahui bahwa kartu kita telah disalin dan sedang digunakan. Karenanya, kita bisa langsung melakukan tindakan preventif seperti menelepon kepada bank untuk segera memblokir kartu kita.

Penambahan MAC dan enkripsi ketika mengirimka OTP ke host adalah untuk menjaga agar informasi OTP yang dikirimkan tidak dapat dibaca oleh pihak lain maupun diubah.

Rancangan ini memiliki kesulitannya, yaitu menentukan kunci yang dapat digunakan ketika melakukan AES. Selain itu, host ATM yang digunakan haruslah memiliki software yang dapat melakukan enkripsi dekripsi untuk OTP yang dikirimkan dan diterima.

Kelemahan lain dari rancangan ini adalah dibutuhkan jaringan koneksi yang kuat dari pengguna serta bank server ketika melakukan autentikasi menggunakan OTP. Ditambah dengan transaksi yang dilakukan bersamaan, hal ini dapat meningkatkan beban pada server bank. Karenanya, hal yang dapat dilakukan adalah server bank untuk kegiatan transaksi ATM terpisah dari server bank utama. Disisi lain, hal ini berarti adanya tambahan biaya yang diperlukan untuk melakukan pemeliharaan pada server.

Waktu juga perlu menjadi pertimbangan pada rancangan ini. Waktu yang dibutuhkan untuk mengirimkan OTP ke pengguna dan waktu untuk memasukkan OTP tidak boleh terlalu lama. Umumnya waktu untuk memasukkan OTP adalah 20-30 detik. Untuk ATM, waktu untuk memasukkan OTP hendaknya lebih cepat agar meminimalkan kemungkinan adanya penyadapan data. Selain itu, apabila OTP tidak dimasukkan dalam jangka waktu yang ditentukan, kartu nasabah haruslah dikeluarkan dan bukan ditelan oleh mesin ATM.

V. KESIMPULAN DAN SARAN

Kriptografi berperan penting dalam kehidupan sehari hari. Walau terkesan tidak kelihatan berperan dimana, kriptografi menjaga keamanan data kita. Mulai dari industri perbankan hingga di pemrintahan, kriptografi sangatlah dibutuhkan. Semakin bagus algoritma kriptografi, maka semakin sulit bagi pencuri data untuk beraksi. Namun, tidak hanya algoritma kriptografi yang berkembang, kemampuan dari pencuri data juga semakin berkembang. Karenanya, algoritma kriptografi menjadi suatu tantangan tersendiri bagi para ilmuwan untuk menghasilkan suatu algoritma yang imun dari berbagai serangan. Sekuat kuatnya kriptografi dapat menjaga data kita, hal ini bukan berarti kita tidak waspada. Berbagai algoritma seperti OTP membutuhkan kewaspadaan dari pengguna agar tidak terjebak oleh pencuri data untuk memberikan kodenya. Karenanya, para pengguna juga seharusnya senantiasa awas terhadapat berbagai trik yang dapat digunakan oleh pencuri data.

Penambahan OTP pada transaksi diharapkan dapat menambah level keamanan pada saat melakukan transaksi. Dengan adanya OTP, yang melakukan transaksi dapat dipastikan merupakan pengguna itu sendiri dikarenakan OTP dikirimkan ke nomor handphone pengguna dimana pada saat ini handphone tidak dapat terlepas dari kehidupan manusia sehari hari.

Algoritma AES sendiri dianggap aman. Peneliti berusaha untuk mencari celah keamanan yang mungkin ada pada AES dan apabila ada maka akan segera diperbaiki. Adapun AES-192 dan AES-256 merupakan standar keamanan yang digunakan pada pemerintahan dan industri keuangan untuk menjaga kerahasiaan data. Semakin kompleks keynya, maka akan semakin sulit bagi kriptanalis untuk memecahkan enkripsi oleh algoritma AES.

VI. UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Tuhan Yang Maha Esa, karena berkat rahmat dan karunianya makalah ini dapat selesai pada waktunya. Tak lupa juga, penulis ingin menyampaikan terima kasih kepada Bapak Dr. Ir. Rinaldi Munir, MT selaku dosen mata kuliah IF4020 Kriptografi yang telah membagikan ilmunya kepada penulis. Selain itu, penulis juga ingin menyampaikan terima kasih kepada kedua orang tua , saudara serta teman teman penulis yang selalu mendukung penulis.

REFERENSI

[1] https://www.technofunc.com/index.php/domain-knowledge-2/banking-domain/item/history-of-banking

[2] https://www.sciencedirect.com/topics/computer-science/advanced-encryption-standard

[3] https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2020-2021/MAC-2020.pdf.

[4] Moshina Priyadharshini et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (2) , 2014, 2004-2007

[5] Selvaraju, N. & Ganapathy, Sekar. (2010). A Method to Improve the Security Level of ATM Banking Systems Using AES Algorithm. International Journal of Computer Applications. 3. 5-9. 10.5120/738-1037.

[6] https://www.nasatm.com/pages/how-do-atms-work

[7] Sankalp Jagga &Puneet Sharma, Rohtak, Haryana. Banking Authentication Technique. International Journal of Information & Computation Technology.ISSN 0974-2239 Volume 4, Number 13 (2014), pp. 1305-1314

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.

Medan, 20 Desember 2020

Vania Velda
13517090