Penerapan Metode Enkripsi *Vigenere Cipher* dalam Pengamanan Transaksi *Mobile Banking*

Ario Yudo Husodo – NIM : 13507017

Program Studi Teknik Informatika, Institut Teknologi Bandung

Jl. Ganesha 10, Bandung

E-mail : if17017@students.if.itb.ac.id

Abstrak

Pada era telekomunikasi pada zaman sekarang ini, dunia transaksi bisnis berkembang begitu pesat. Salah satu lompatan perkembangan teknologi transaksi bisnis adalah *Mobile Banking*. *Mobile Banking* merupakan suatu metode transaksi perbankan elektronik dengan menggunakan *mobile* (*handphone*) yang memungkinkan nasabah suatu bank untuk melakukan transaksi keuangan cukup dengan menggunakan *handphone* miliknya tanpa perlu pergi menuju bank tempat dana nasabah tersebut disimpan. Secara kasat mata, teknologi ini sangat membantu pengguna di dalam mempermudah dan mempercepat nasabah untuk melakukan transaksi perbankan secara elektronik. Namun demikian, apabila dipandang dari sisi teknis, metode *mobile banking* khususnya di Indonesia masih tergolong ke dalam metode transaksi perbankan yang kurang aman karena informasi yang dikirimkan nasabah melalui *handphone* miliknya dapat dengan mudah disadap oleh pihak-pihak yang tidak bertanggung jawab.

Penyadapan ilegal terhadap informasi perbankan nasabah oleh pihak yang tidak bertanggung jawab tentu saja meresahkan dan merugikan nasabah bank yang bersankutan. Pasalnya, dengan bermodalkan informasi perbankan nasabah resmi, pihak *intruder* mampu "melarikan" uang nasabah secara ilegal. Untuk mengantisipasi persoalan tersebut, pada dasarnya pihak bank sampai saat ini, khususnya di Indonesia, sudah menerapkan beberapa metode enkripsi terhadap informasi yang dikirimkan nasabah *mobile banking*. Namun sayangnya, metode enkripsi yang sudah ada saat ini merupakan metode enkripsi yang masih dapat "ditembus" oleh para *intruder*.

Agar dapat memberikan kontribusi proteksi secara optimum kepada nasabah *mobile banking*, pada makalah ini penulis akan memaparkan mengenai penerapan suatu metode enkripsi di dalam pengamanan transaksi *mobile banking*. Adapun metode enkripsi yang diusulkan penulis sebagai metode enkripsi yang mampu memberikan sistem keamanan maksimum untuk transaksi perbankan secara *mobile* adalah metode enkripsi *Vigenere cipher*. *Vigenere cipher* merupakan salah satu metode enkripsi klasik yang digunakan untuk menyembunyikan pesan berupa teks dengan menggunakan teknik substitusi dimana tiap huruf pada *plaintext* diganti (disubstitusi) menjadi huruf lain berdasarkan kunci yang digunakan.

Di dalam pengamanan transaksi *mobile banking*, penulis menggunakan nomor mesin *handphone* nasabah sebagai kunci *Vigenere* guna mengenkripsi informasi yang dikirimkan dalam transaksi *mobile banking*. Dikarenakan nomor mesin *handphone* ataupun informasi transaksi *mobile banking* tidak hanya tersusun atas karakter alphabetis, maka metode enkripsi *Vigenere* yang digunakan telah sedikit dimodifikasi sehingga mampu melakukan substitusi terhadap karakter lain selain huruf alphabet. Dengan metode ini, meskipun *Vigenere cipher* bisa dipecahkan dengan metode kasiski yang menganalisis selang antara pola huruf yang sama di dalam *ciphertext* beserta frekuensi kemunculannya, dikarenakan nomor mesin setiap *handphone* adalah unik dan karena informasi nasabah yang dikirimkan di dalam transaksi *mobile banking* tergolong sedikit (sebatas *username* nasabah, nomor rekening, sandi lewat, atau PIN), maka metode kasiski memiliki probabilitas kecil untuk dapat diterapkan dalam memecahkan metode *Vigenere cipher* di dalam pengamanan informasi transaksi *mobile banking*. Dengan diterapkannya metode *Vigenere cipher* sebagai sistem enkripsi informasi *mobile banking*, diharapkan kepercayaan nasabah bank terhadap metode *mobile banking* semakin bertambah serta diharapkan implementasi *Vigenere cipher* ini dapat berkontribusi terhadap terjaganya dana nasabah di suatu bank.

Kata kunci : *Mobile banking, keamanan informasi, Vigenere cipher*

1. Pendahuluan

Kriptografi atau yang sering dikenal dengan sebutan ilmu penyandian data adalah suatu bidang ilmu dan seni yang bertujuan untuk menjaga kerahasiaan suatu pesan yang berupa data-data dari pihak lain yang tidak berhak sehingga tidak menimbulkan kerugian. Pada masa sekarang ini, kriptografi atau ilmu penyandian data sering diklasifikasikan menjadi dua jenis yaitu kriptografi klasik dan kriptografi modern.

Kriptografi klasik sudah mulai dipelajari manusia sejak tahun 400 SM, yaitu pada zaman Yunani kuno. Kriptografi klasik ini lebih menekankan pada perubahan tiap karakter dalam upaya menjaga kerahasiaan pesan. Contoh kriptografi klasik adalah *Vigenere cipher* dan *Caesar cipher*. Sedangkan kriptografi modern lebih menekankan pada pengoperasian bit-bit. Contohnya adalah DES dan GOST. Pada kriptografi klasik terdapat 2 algoritma, yaitu *cipher* substitusi dan *cipher* transposisi. Pada *cipher* substitusi, setiap huruf dalam *plaintext* akan tepat berkorespondensi satu-satu dengan huruf dalam *ciphertext*-nya, sedangkan pada *cipher* transposisi huruf-huruf pada *plaintext* hanya dimanipulasi letak posisinya (*transpose*) untuk menjadi *ciphertext*.

Vigenere chiper merupakan salah satu algoritma kriptografi klasik untuk menyandikan suatu *plaintext* dengan menggunakan teknik substitusi.*Vigenere cipher* pada dasarnya cukup rumit untuk dipecahkan. Meskipun begitu, *Vigenere cipher* tetap memiliki kelemahan. Salah satunya adalah dapat diketahui panjang kuncinya dengan menggunakan metode kasiski. Hal ini disebabkan karena umumnya terdapat frasa yang berulang-ulang pada *ciphertext* yang dihasilkan.

Jika diamati lebih lanjut, seiring dengan majunya perkembangan dunia pemrograman, teknik dasar *Vigenere cipher* dapat sedikit dimodifikasi sehingga tidak hanya mampu melakukan enkripsi terhadap karakter alphabetis saja, namun juga karakter angka dan simbol khusus. Untuk memudahkan penyebutannya, kedepannya penulis akan menamakan teknik *Vigenere cipher* yang mampu mengenkripsi seluruh jenis karakter sebagai *Advance Vigenere Cipher* (AVC). Modifikasi ini secara praktik sangatlah membantu sistem keamanan informasi pada saat ini karena semua karakter yang ada di dunia komunikasi dapat dienkripsi menggunakan metode AVC.

Dengan sedikit memodifikasi teknik *Vigenere cipher*, maka penggunaan metode enkripsi *Vigenere* dapat diterapkan dalam segala aplikasi informasi dunia elektronik secara global. Dikarenakan secara konseptual metode *Vigenere cipher* sangat mudah diterapkan, pengembangan AVC tentu akan mempercepat dan mempermudah aplikasi yang menerapkan AVC untuk mengenkirpsi dan mengamankan informasi yang ingin dilindungi aplikasi tersebut.

Dunia transaksi elektronik seperti *mobile banking* merupakan salah satu contoh aplikasi "dunia maya" yang sangat membutuhkan sistem keamanan informasi yang dikandungnya dalam setiap transaksi perbankan. Sistem enkripsi informasi perbankan *mobile banking* yang ada sampai saat ini, khususnya di Indonesia, masih memungkinkan terdapat *intruder* yang dapat menyadap informasi nasabah *mobile banking* dan "memecahkan" kode enkripsi sistem sehingga *intruder* tersebut dapat membobol akun nasabah secara ilegal.

Dengan menerapkan metode AVC sebagai metode pengamanan informasi perbankan *mobile banking*, probabilitas *intruder* untuk memecahkan kode enkripsi sistem dapat ditekan secara optimal sehingga mampu berkontribusi dalam peningkatan keamanan transaksi perbankan nasabah *mobile banking*. Adapun detail penerapan metode enkripsi AVC di dalam mengamankan informasi perbankan *mobile banking* akan dijelaskan pada bab selanjutnya.

2. Konsep Dasar

2.1 Vigenere Cipher

Vigenere Cipher adalah suatu algoritma kriptografi klasik yang ditemukan oleh Giovan Battista Bellaso. Beliau menuliskan metodenya tersebut pada bukunya yang berjudul La Cifra del. Sig. Giovan Battista Bellaso pada tahun 1553. Nama vigenere sendiri diambil dari seorang yang bernama Blaise de Vigenere. Nama vigenere diambil sebagai nama algoritma ini karena beliau menemukan kunci yang lebih kuat lagi untuk algoritma ini dengan metode *autokey cipher* meskipun algoritma dasarnya telah ditemukan lebih dahulu oleh Giovan Battista Bellaso.

Gambar 1. Sketsa Blaise de Vigenere

Algoritma ini menjadi terkenal karena cukup sulit dipecahkan. Matematikawan Charles Lutwidge Dodgson menyatakan bahwa algoritma ini tidak terpecahkan. Pada tahun 1917, ilmuwan Amerika menyebutkan bahwa *Vigenere cipher* adalah sesuatu yang tidak mungkin untuk ditranslasikan. Namun hal ini terbantahkan sejak Kasiski berhasil memecahkan algoritma pada abad ke-19.

Pada dasarnya *Vigenere Cipher* serupa dengan *Caesar Cipher*, perbedaannya adalah pada *Vigenere Cipher* setiap huruf pesan aslinya digeser sebanyak satu huruf pada kuncinya sedangkan pada *Caesar Cipher* setiap huruf pesannya digeser sebanyak 1 huruf yang sama.

Algoritma *Vigenere Cipher* ini menggunakan bujursangkar *Vigenere* untuk melakukan enkripsi. Setiap baris di dalam bujursangkar menyatakan huruf-huruf *ciphertext* yang diperoleh dengan *Caesar cipher*. Untuk lebih jelasnya perhatikan gambar 2 di bawah ini. Deretan huruf kuning mendatar merepresentasikan *plaintext*, sedangkan deretan huruf hijau menurun merepresentasikan kunci.

Contoh, misalkan *plaintext* dengan huruf P disandikan dengan kunci K, maka hasil *ciphertext* yang dihasilkan adalah huruf Z.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Gambar 2. Bujur Sangkar Vigenere

Jika panjang kunci lebih pendek daripada panjang *plaintext*, maka kunci tersebut akan diulang secara periodik. Bila panjang kunci adalah x, maka periodenya adalah x. Contohnya adalah sebagai berikut :

Kunci : ITB
Plaintext : TEKNOLOGI KRIPTOGRAFI

Maka proses yang dilakukan adalah setiap huruf dicek pada *bujursangkar Vigenere* dan hasilnya berupa *ciphertext*.

Plaintext	: TEKNOLOGI KRIPTOGRAFI
Kunci	: ITB I TB ITB I TBITB I T BIT
Ciphertext	: BXLVHMWZJ SKJXMPOKBNB

Hal diatas merupakan karakteristik dari *cipher* abjad majemuk. Pada *cipher* substitusi sederhana, setiap huruf *ciphertext* selalu menggantikan huruf *plaintext* tertentu, sedangkan pada *cipher* abjad majemuk setiap huruf *ciphertext* dapat memiliki kemungkinan banyak huruf *plaintext*. Sehingga kita dapat mencegah terdeteksinya frekuensi kemunculan huruf-huruf di dalam *ciphertext* yang mempunyai pola tertentu yang sama sebagaimana yang diperlihatkan pada *cipher* substitusi sederhana atau abjad tunggal.

Apabila metode *Vigenere cipher* ini ditranslasikan ke dalam suatu algoritma pemrograman, secara sederhananya, notasi algoritmik yang digunakan untuk mengenkripsi suatu karakter alphabet *plaintext* (P) menjadi *ciphertext* (C) dengan kunci K adalah sebagai berikut.

$$C_i \equiv (P_i + K_i) \mod 26$$

2.2 *Advance Vigenere Cipher* (AVC)

AVC merupakan suatu modifikasi *Vigenere cipher* yang memungkinkan metode enkripsi *Vigenere* untuk tidak hanya mampu menyandikan karakter alphabetis, namun juga mampu menyandikan seluruh karakter yang ada di "dunia elektronik", seperti angka dan simbol simbol khusus (%, ^, *, $, #, @, |, dan lain sebagainya).

Berbeda dengan notasi algoritmik enkripsi *Vigenere cipher* pada umumnya, notasi algoritimik yang digunakan AVC untuk mengenkripsi suatu karakter alphabet *plaintext* (P) menjadi *ciphertext* (C) dengan kunci K adalah sebagai berikut.

$$C_i \equiv (P_i + K_i)$$

Dimana proses penambahan yang terjadi (Pi + Ki) dilakukan dengan menambahkan kode ASCII Pi dengan kode ASCII Ki yang hasil penambahan tersebut dikonversikan ke dalam suatu simbol Ci yang sesuai dengan kode ASCII yang dihasilkan dari proses penambahan kode ASCII Pi + Kode ASCII Ki.

Kelebihan utama metode enkripsi AVC adalah metode ini dapat diterapkan dalam penyandian segala informasi elektronik pada masa sekarang yang memungkinkan penggunanya untuk menggunakan segala macam karakter yang tersedia di dalam transaksi informasi elektronik. Dengan kemampuan ini, metode AVC dapat diterapkan sebagai metode global penyandian data yang dapat diterapkan secara cepat dan mudah. Selain itu, dilihat dari sisi keamanan, metode enkripsi AVC sangatlah sulit dipecahkan karena selang kemungkinan karakter kunci dan plaintext sangatlah banyak, yaitu 2^8 kemungkinan karakter (setiap huruf ASCII tersusun atas 8 bit, bandingkan dengan kemungkinan karakter metode enkripsi Vigenere standar yang hanya memiliki 26 kemungkinan karakter).

3. Permasalahan Utama

Seperti yang telah dipaparkan penulis pada bagian awal makalah ini, penulis memfokuskan pembahasan makalah ini kepada penerapan metode *Advance Vigenere Cipher* di dalam mengamankan informasi transaksi elektronik *mobile banking*. Alasan utama pemilihan *mobile banking* sebagai kajian penerapan AVC dikarenakan sistem *mobile banking* merupakan sistem yang notabenanya merupakan sistem transaksi elektronik yang sangat dibutuhkan masyarakat namum saat ini masih tergolong ke dalam sistem transaksi elektronik yang kurang aman.

Dengan diterapkannya AVC sebagai sistem enkripsi informasi *mobile banking*, diharapkan kepercayaan dan animo masyarakat terhadap sistem *mobile banking* semakin meningkat sehingga setiap transaksi perbankan dapat dilakukan dengan mudah dan cepat. Dengan adanya hal ini, arus perekonomian suatu masyarakat, terutama masyarakat Indonesia, tentu dapat semakin berkembang pesat sehingga diharapkan penerapan AVC ini mampu berkontribusi dalam peningkatan kesejahteraan ekonomi masyarakat luas.

3.1 Perkembangan *Mobile Banking*

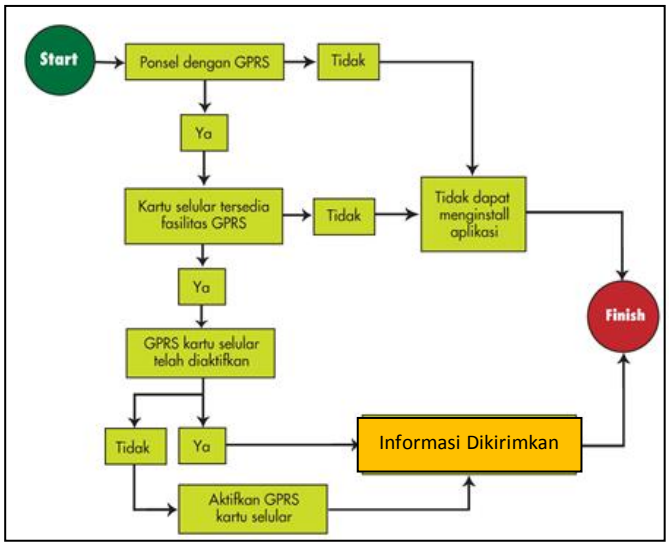
Pada masa yang serba canggih seperti ini, kepraktisan sudah menjadi suatu kebutuhan yang perlu dipenuhi oleh manusia. Salah satu kepraktisan yang sering menjadi perhatian masyarakat modern adalah kepraktisan dalam melakukan transaksi

keuangan. Terdapat berbagai macam metode transaksi keuangan yang terdapat pada zaman sekarang, salah satu di antaranya yang menyorot banyak perhatian publik adalah metode transaksi *mobile banking*. *Mobile banking* merupakan suatu metode transaksi keuangan dengan menggunakan peralatan berupa *handphone*. *Mobile banking* memungkinkan seorang nasabah bank untuk melakukan audit, transfer, dan transaksi penting lainnya. Dikarenakan kemudahan penggunaannya, *mobile banking* sudah banyak dipakai oleh masyarakat pada beberapa tahun belakangan ini.

3.2 Ruang Lingkup Masalah

Meskipun sangat membantu nasabah bank untuk melakukan transaksi keuangan dimanapun mereka berada, sayangnya sistem *mobile banking* yang ada saat ini, khususnya di Indonesia, masih jauh dari "aman". Yang dimaksud dengan aman dalam hal ini adalah keamanan informasi nasabah, nomor rekening, *password*, dan kunci PIN nasabah yang bersangkutan di sebuah Bank. Informasi penting di atas biasanya sering dapat "dicuri" oleh pihak-pihak yang tidak bertanggung jawab ketika informasi tersebut dikirimkan melalui suatu media transmisi. Akibatnya, apabila orang lain yang tidak berhak mengetahui informasi dari seorang nasabah, maka orang tersebut mampu melakukan transaksi keuangan terhadap akun nasabah tersebut, yang notabenanya tindakan ini tergolong tindakan ilegal.

Perhatikan gambar 3. Skema gambar ini menunjukkan secara sederhana metode penerapan *mobile banking* dalam suatu sistem perbankan. Pada tahapan pengiriman informasi *mobile banking*, sebelum informasi tersebut diterima oleh pihak bank, informasi tersebut dapat disadap oleh *intruder*. Hal ini tentu bisa sangat merugikan pihak bank dan konsumen. Pada bagian pengiriman informasi *mobile banking* dari *handphone* nasabah ke pihak bank inilah diterapkan metode enkripsi AVC sehingga apabila terdapat *intruder* yang melakukan penyadapan terhadap informasi nasabah, maka *intruder* tersebut tidak akan mampu memecahkan *ciphertext* yang terkandung di dalamnya



Gambar 3. Skema Sederhana Transaksi Mobile Banking

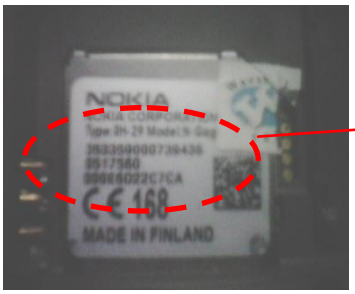
4. Metode Penyelesaian Masalah

4.1 Nomor Mesin *Handphone*

Nomor mesin *handphone* merupakan suatu untaian nomor yang tertera di suatu mesin *handphone* yang berguna untuk memberikan informasi identitas suatu mesin *handphone*. Seperti layaknya nomor mesin kendaraan bermotor pada umumnya, nomor mesin *handphone* adalah unik sehingga tidak terdapat dua *handphone* berbeda memilki nomor mesin yang sama.

Perhatikan gambar 4. Gambar 4.a menunjukkan *mainboard* secara umum suatu *handphone*, sedangkan gambar 4.b menunjukkan lokasi keberadaan nomor mesin suatu *handphone*.

(a)



(b)

Nomor mesin suatu *handphone*

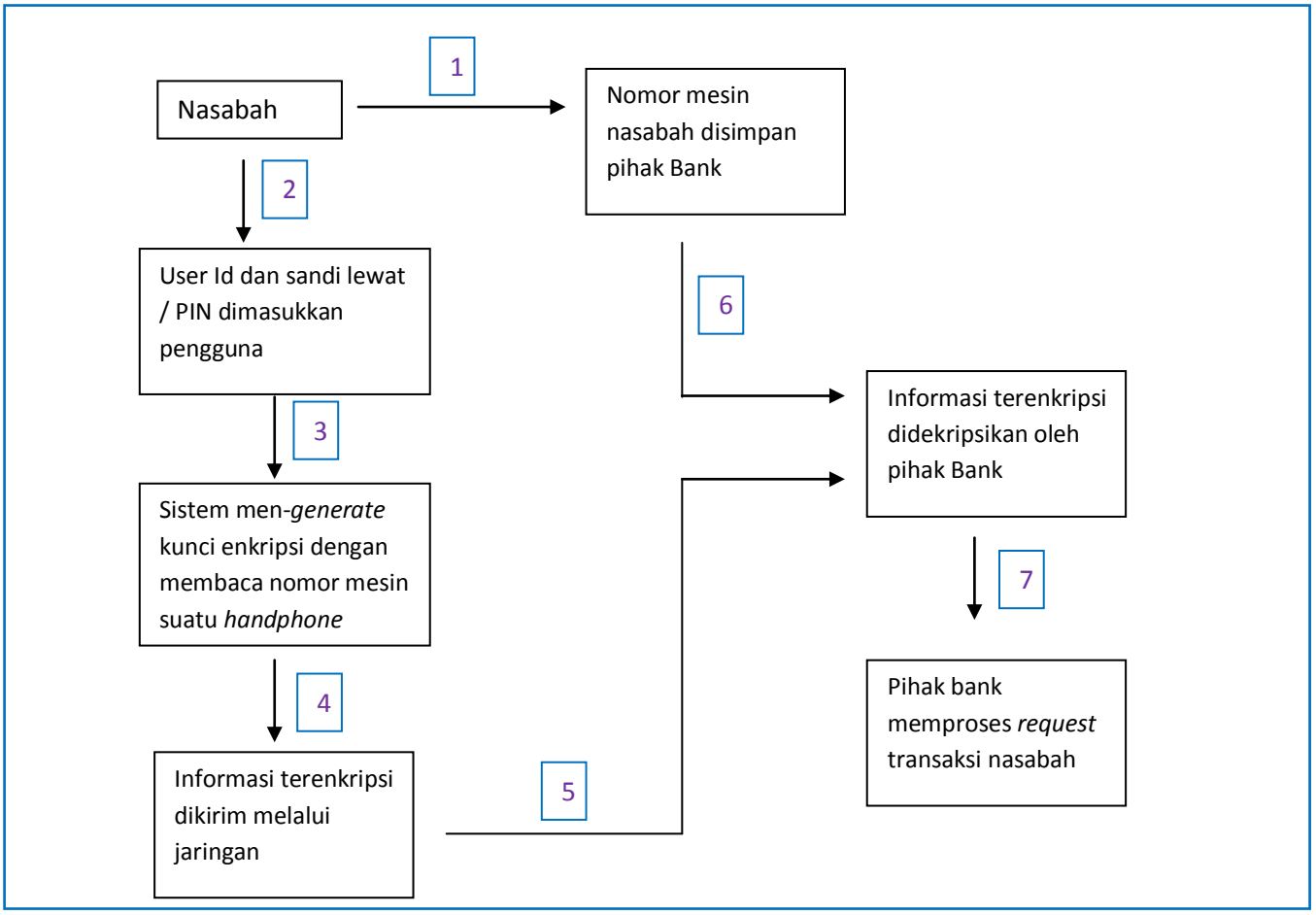
Gambar 4. Tampilan Mesin *Handphone*

4.2 Prosedur Pengamanan AVC

Untuk dapat mengamankan informasi yang dikirimkan nasabah dalam sistem *mobile banking*, selain informasi yang dikirimkan perlu dienkripsi, perlu dibuat suatu metode tambahan yang mampu membuat suatu akun nasabah hanya mampu diakses oleh satu alat unik saja, dalam hal ini alat unik tersebut adalah *handphone* nasabah yang bersangkutan saja. Artinya, meskipun terdapat penyadap yang berhasil "mencuri" informasi yang ditransmisikan dalam sistem *mobile banking*, apabila penyadap tersebut tidak memiliki handphone nasabah resmi yang bersangkutan, maka penyadap tersebut tidak dapat mengakses akun nasabah yang disadapnya.

Prinsip pengamanan ini dapat diterapkan dengan melakukan enkripsi *Vigenere* terhadap informasi yang dikirimkan pengguna dengan menggunakan kunci enkripsi yang berasal dari nomor mesin *handphone* pengguna. Setiap *handphone* pada masa sekarang ini, seperti layaknya kendaraan bermotor, memiliki nomor mesin yang unik bila dibandingkan dengan *handphone* lain (tidak ada dua *handphone* berbeda memiliki nomor mesin yang sama). Hal ini tentunya akan membuat penyadap kesulitan di dalam memecahkan enkripsi informasi yang disadapnya.

Agar metode pengamanan AVC dapat diterapkan, ketika seorang pengguna ingin membuka sebuah akun *mobile banking*, pengguna yang bersangkutan perlu melaporkan terlebih dahulu nomor mesin *handphone* yang dimilikinya ke pihak bank. Pihak bank selanjutnya akan mencatat nomor mesin *handphone* tersebut untuk disimpan sebagai kunci dekripsi pesan yang nantinya akan dikirimkan oleh nasabah ketika melakukan transaksi *mobile banking*. Selanjutnya, ketika nasabah ingin melakukan transaksi *mobile banking*, sistem program *mobile banking* yang ter-*install* di *handphone* nasabah tersebut akan "mengambil" informasi mengenai nomor mesin *handphone* nasabah, kemudian sistem akan menggunakannya sebagai kunci enkripsi. Setelah sistem melakukan enkripsi terhadap informasi yang dimasukkan pengguna, barulah sistem mentransmisikan informasi tersebut. Perhatikan skema berikut



Gambar 5. Skema Alur Informasi Penerapan AVC pada Transaksi *Mobile Banking*

Keterangan Skema

1	Nasabah mendaftarkan nomor mesin *handphone* miliknya ke pihak bank
2	Jika pihak bank telah menyimpan nomor mesin *handphone* milik nasabah, nasabah dapat langsung menggunakan aplikasi *mobile banking*
3	Program sistem membaca nomor mesin *handphone* nasabah
4	Informasi dari nasabah dienkripsi menggunakan kunci V*igenere* yang berasal dari nomor mesin *handphone* pengguna
5	*Ciphertext* dikirim melalui jaringan dengan ditambahkan *header* untuk mengetahui bagaimana cara mencari kunci *Vigenere* dari basis data pihak bank
6	Dengan membaca *header ciphertext*, pihak bank dapat mencari di basis data bank mengenai nomor mesin *handphone* nasabah *mobile banking*
7	Pihak bank melakukan interpretasi terhadap informasi yang dikirimkan nasabah.

4.3 Notasi Algoritmik Penerapan AVC pada Mobile Banking

```
//variable global
String information_from_user;
String ciphertext;
String plaintext;

//proses di handphone nasabah
Input(information_from_user);
Int key = System.get_HP_machine_number( );
Ciphertext = Vigenere_encrypt(information_from_user, key)
Add_Header(Ciphertext);
Send_to_Network(Ciphertext);

// Proses di server bank
Int index_nasabah = Read_Header(CipherText);
Int key_from_database = look_up(index_nasabah);
Plaintext = Vigenere_decrypt(Ciphertext, key_from_database)
Interprete(Plaintext);
```

//Keterangan beberapa fungsi

System.get_HP_machine_number() merupakan fungsi yang mengembalikan nomor mesin *handphone* dimana program ini dijalankan.

Vigenere_encrypt (string input, int key) merupakan fungsi yang mengembalikan string hasil enkripsi *Vigenere* dari *string* input dengan kunci key

Vigenere_decrypt (string input, int key) merupakan fungsi yang mengembalikan string hasil dekripsi *Vigenere* dari *string* input dengan kunci key

Add_Header(string input) merupakan fungsi yang berguna menambahkan *header* pada *string* input agar program yang mendekripsi *string* input dapat mengetahui bagaimana cara mendekripsi *string* input yang dimaksudkan

Read_Header(string input) merupakan fungsi yang mengembalikan nomor index nasabah yang disimpan di basis data bank dengan membaca *header* pada *string* input

Look_up(int index) merupakan fungsi yang mengembalikan integer yang merupakan nomor mesin *handphone* nasabah dengan nomor index "index" di basis data pihak bank

Interprete(string input) merupakan fungsi yang menginterpretasikan kemudian mengeksekusi perintah yang dikandung pada *string* input.

5. Analisis Metode *Advance Vigenere Cipher*

5.1 Kelebihan Penerapan AVC di dalam Sistem *Mobile Banking*

Seperti yang telah dipaparkan pada bagian awal makalah ini, sistem pengamanan informasi *mobile banking* yang menerapkan AVC menggunakan nomor mesin *handphone* sebagai kunci *Vigenere*. Apabila diperhatikan lebih lanjut, selain nomor mesin setiap *handphone* adalah unik, nomor mesin setiap *handphone* bisa dikatakan tidak memiliki pola aturan tertentu. Perhatikan kembali gambar 4.

Pada gambar di atas, terlihat bahwa handphone tersebut memiliki nomor mesin 353350000739434851756080066022C7CA. Nomor mesin *handphone* tersebut terlihat tidak memiliki aturan pola tertentu. Selain itu, nomor mesin suatu *handphone* juga tersusun lebih dari 30 karakter. Jika dibandingkan dengan informasi yang dikirimkan oleh

nasabah pada transaksi *mobile banking*, seperti *id user* ataupun nomor kunci PIN akun nasabah yang bersangkutan, bisa dikatakan nomor mesin suatu *handphone* memiliki panjang yang cukup untuk mengenkripsi informasi nasabah *mobile banking* sehingga metode *crypt analysis* dengan menganalisis frekuensi kemunculan pola huruf yang sama, misalkan metode kasiski, tidak dapat diterapkan. Hal ini mengindikasikan bahwa AVC merupakan sistem enkripsi yang tergolong *high-secure*.

Dilihat dari sisi pengguna, pengguna tidak akan merasa terbebani dengan sistem AVC ini karena nasabah *mobile banking* tidak perlu mengingat kunci yang ia gunakan di dalam mengenkripsi informasi yang ia kirimkan ketika melakukan transaksi *mobile banking*. Pengguna cukup memasukkan input *id user* dan sandi rahasia nasabah di dalam setiap transaksi *mobile banking* yang ia lakukan, selanjutnya sistem akan secara otomatis "mengambil" nomor mesin *handphone* sebagai kunci enkripsi *Vigenere*.

Kekuatan keamanan metode AVC ini terdapat pada panjang kunci *Vigenere* (nomor mesin *handphone*) dan pola karakter penyusun kunci Vigenere (tidak memiliki pola khusus, seperti misalkan 12345678 yang memiliki pola *increment* antara 1 digit dengan digit lain). Panjang kunci enkripsi dengan menggunakan nomor mesin *handphone* bila dibandingkan dengan data yang dienkripsi (nomor PIN dan nomor rekening nasabah pengguna *mobile banking*) tergolong relatif panjang, akibatnya metode analisis frekuensi kemunculan huruf (metode kasiski) tidak dapat diterapkan untuk memecahkan metode AVC.

5.2 Kekurangan Penerapan AVC di dalam Sistem *Mobile Banking*

Secara umum, seperti yang telah dipaparkan pada bagian kelebihan AVC, AVC merupakan metode pengamanan informasi transaksi *mobile banking* yang tergolong *high-secure*. Namun demikian, konsekuensi yang perlu dilakukan agar keamanan metode AVC dapat terjaga adalah pengguna perlu mengalokasikan sedikit waktunya untuk mendaftarkan nomor mesin *handphone* yang dimilikinya kepada pihak bank sebelum menggunakan fasilitas transaksi *mobile banking* dengan sistem pengamanan AVC.

Apabila diperhatikan secara seksama, terlihat bahwa pihak bank mendekripsi pesan dari nasabah dengan menggunakan nomor mesin *handphone* nasabah yang tersimpan di dalam basis data pihak bank. Oleh karenanya, agar pihak bank dapat mendekripsikan pesan dari nasabah, nasabah perlu mendaftarkan terlebih dahulu kepada pihak bank mengenai nomor mesin *handphone* yang digunakannya untuk transaksi *mobile banking*. Jika pada suatu saat nasabah kehilangan atau mengganti *handphone* yang biasanya ia gunakan untuk transaksi *mobile banking*, maka nasabah yang bersangkutan perlu untuk mendaftarkan ulang nomor mesin *handphone* baru yang akan digunakannya untuk melakukan transaksi *mobile banking*.

Dengan menerapkan sistem AVC, nasabah memang diharuskan untuk hanya dapat menggunakan satu buah *handphone* di dalam mengakses akun bank yang ia miliki di dalam transaksi *mobile banking*. Hal ini dimaksudkan untuk meningkatkan keamanan informasi dalam sistem *mobile banking*. Jika dibandingkan dengan keamanan yang dihasilkan dari diterapkannya metode AVC, tentu saja konsekuensi "kerepotan" nasabah merupakan hal kecil yang tidak terlalu merugikan pihak nasabah.

6. Kontribusi Bagi Masyarakat

Dikarenakan begitu banyak masyarakat pada masa sekarang yang sering melakukan transaksi keuangan, khususnya di dunia bisnis, penerapan metode pengamanan AVC tentu sangat memberikan kontribusi besar. Ambil contoh saja kasus pembobolan bank yang terjadi beberapa bulan belakangan ini, ratusan miliar rupiah uang-nasabah hilang dibobol. Sebagian dari korban ini adalah pengguna *mobile banking*. Hal ini tentu membuat kepercayaan nasabah terhadap sistem *mobile banking* menjadi menurun. Konsekuensinya, nasabah akan lebih cenderung untuk melakukan transaksi perbankan dengan transaksi "langsung", yang notabenanya memperlambat arus keuangan bisnis orang yang bersangkutan, dan tentunya secara tidak langsung memperlambat arus perekonomian suatu negara.

Apabila metode pengamanan AVC diterapkan, ratusan miliar rupiah uang nasabah akan dapat diamankan. Kepercayaan nasabah terhadap bank akan semakin meningkat, dan pada akhirnya, kekuatan perekonomian suatu negara, khususnya bangsa Indonesia dapat semakin bertambah untuk bersaing dengan negara negara lain.

7. Kesimpulan

Vigenere cipher merupakan salah satu metode enkripsi klasik yang digunakan untuk menyembunyikan pesan berupa teks dengan menggunakan teknik substitusi dimana tiap huruf pada *plaintext* diganti (disubstitusi) menjadi huruf lain berdasarkan kunci yang digunakan. Teknik pada *Pure Vigenere* hanya mampu mensubsitusi huruf alphabetik menjadi huruf alphabetik lain.

Advance Vigenere Cipher (AVC) merupakan metode enkripsi serupa dengan *Pure Vigenere*, namun memiliki kemampuan untuk melakukan enkripsi terhadap berbagai macam karakter selain karakter alphabetik. AVC dapat diterapkan sebagai metode enkripsi pada sistem keamanan transaksi *mobile banking*.

Kekuatan keamanan metode AVC ini terdapat pada panjang kunci *Vigenere* (nomor mesin *handphone*) dan pola karakter penyusun kunci *Vigenere* yang tidak beraturan. Hal ini mengindikasikan bahwa AVC dapat dijadikan sebagai metode enkripsi pesan transaksi *mobile banking* yang *high-secure* dan dapat dengan mudah diterapkan serta memiliki waktu eksekusi yang relatif cepat. Dengan diterapkannya AVC di dalam sistem enkripsi informasi transaksi *mobile banking*, secara tidak langsung kekuatan perekonomian suatu negara, khususnya bangsa Indonesia, dapat semakin bertambah untuk bersaing dengan negara-negara lain. Hal ini tentunya dapat meningkatkan kesejahteraan masyarakat di suatu negara, khususnya Indonesia.

Daftar Referensi

Munir, Rinaldi, Kriptografi, Institut Teknologi Bandung, 2006.

http://www.perlmonks.org/?node_id=139710

http://www.tecways.com/index.php?id=22

http://www3.telus.net/Voiculescu/vigenere/index.html