semanTIK, Vol.3, No.2, Jul-Des 2017, pp. 237-244
ISSN : 2502-8928 (Online)

IMPLEMENTASI METODE ENKRIPSI *ADVANCE VIGENERE CIPHER* DALAM PENGAMANAN SISTEM TRANSAKSI *PAYMENT POINT ONLINE BANK*

Muh. Iskandar Z. A.*[1], Sutardi[2], Yuwanda Purnamasari Pasrun [3]
[*1,2,3]Jurusan Teknik Informatika, Fakultas Teknik, Universitas Halu Oleo, Kendari
e-mail: ***[1] izoelll@gmail.com,**[2]sutardi_hapal@yahoo.com, [3]yuwandapurnamasari@gmail.com

Abstrak

Advance vigenere cipher merupakan suatu modifikasi *vigenere cipher* yang memungkinkan metode enkripsi *vigenere* untuk tidak hanya mampu menyandikan karakter abjad, namun juga mampu menyandikan seluruh karakter yang ada termasuk angka dan simbol-simbol. Tujuan dari penelitian ini adalah membangun sistem transaksi *Payment Point Online Bank* (PPOB) yang aman dengan mengimplementasikan metode *Advance Vigenere Cipher* dalam pengamanan sistemnya.

Dalam penelitian ini, sistem pengamanan transaksi PPOB dibagi menjadi dua tahapan utama yaitu tahapan enkripsi dan tahapan dekripsi. Data yang dienkripsi menggunakan metode *Advance Vigenere Cipher* merupakan detail data tagihan dari transaksi yang akan dilakukan. Hasil dari enkripsi menghasilkan *ciphertext* yang akan dikirimkan dan didekripsi oleh pihak penyedia layanan PPOB.

Hasil dari penelitian ini menunjukkan karakteristik dari *ciphertext* yang dihasilkan sangat rumit, sehingga akan sulit bagi pihak luar untuk melakukan intervensi dan mengelola informasi yang dikirimkan dari pihak penyedia layanan PPOB kepada pengguna layanan PPOB.

Kata Kunci—Enkripsi *advance vigenere cipher*, sistem transaksi *Payment Point Online Bank* (PPOB)

Abstract

Advance vigenere cipher is a modification of vigenere cipher that allows the vigenere encryption method to not only be able to encode alphabetic characters, But also to encode all existing characters including numbers and symbols. The purpose of this research is to build a secure Payment Point Online Bank (PPOB) transaction system by implementing Advance Vigenere Cipher method to secure the system.

In this research, the security system of PPOB transaction is divided into two main step namely encryption step and decryption step. The data encrypted by using the Advance Vigenere Cipher method is the detail of the billing data of the transaction. The result of the encryption generates the ciphertext to be sent and decrypted by the PPOB service provider.

The results of this research indicate the characteristics of the resulting ciphertext is very unique, So it will be difficult for outsiders to intervene and manage the information that sent from PPOB service providers to the users of PPOB services.

Keywords—*Advance vigenere cipher encryption, Payment Point Online Bank (PPOB) transaction system*

1. PENDAHULUAN

Pada era telekomunikasi pada zaman sekarang ini, dunia transaksi bisnis berkembang begitu pesat. Salah satu lompatan perkembangan teknologi transaksi bisnis adalah sistem transaksi secara *online*. Hal tersebut memungkinkan pengguna untuk melakukan transaksi keuangan cukup dengan menggunakan *handphone* atau perangkat miliknya tanpa perlu pergi menuju bank atau tempat dimana pengguna melakukan transaksi secara manual. Secara kasat mata, teknologi ini sangat membantu pengguna di dalam mempermudah dan mempercepat pengguna

untuk melakukan transaksi secara elektronik. Namun demikian, apabila dipandang dari sisi teknis, metode transaksi *online* khususnya di Indonesia masih tergolong ke dalam metode transaksi yang kurang aman karena informasi yang dikirimkan pengguna melalui perangkat miliknya dapat dengan mudah disadap oleh pihak-pihak yang tidak bertanggung jawab [1].

PPOB (*payment point online bank*) adalah sistem transaksi *online* yang memanfaatkan pembayaran dengan fasilitas perbankan, seperti pembayaran tagihan PLN, Telkom, PDAM, cicilan motor dan lain-lain. PPOB tidak hanya melibatkan jasa perbankan sebagai lembaga keuangan, tetapi juga melibatkan lembaga *switching* sebagai pengatur lalu lintas data serta *outlet-outlet* atau loket-loket PPOB yang melayani langsung ke pelanggan [2].

Penyimpangan peranan teknologi informasi untuk tindakan kriminal yang dilakukan oleh organisasi atau pribadi contohnya kesempatan untuk mencuri dan mengubah informasi dalam distribusi data untuk tujuan kejahatan. Agar dapat memberikan kontribusi proteksi secara optimum kepada pengguna, tugas akhir ini akan memaparkan mengenai penerapan suatu metode enkripsi di dalam pengamanan transaksi *online*. Adapun metode enkripsi yang akan digunakan sebagai metode enkripsi yang mampu memberikan sistem keamanan maksimum untuk transaksi *online* adalah metode enkripsi *Advancevigenere cipher*.

Metode *Advance Vigenere Cipher* diambil karena metode ini dapat mencegah adanya intervensi dari pihak luar yang dapat mengakibatkan tidak sampainya data transaksi yang dikirimkan, melihat di dalam sistem transakasi PPOB terdapat proses pengiriman data transaksi dari pengguna layanan kepada penyedia layanan dan memerlukan metode pengamanan. Maka berdasarkan uraian diatas, maka judul tugas akhir yang akan diangkat yaitu, "Implementasi Metode Enkripsi *Advance Vigenere Cipher* Dalam Pengamanan Sistem Transaksi *Payment Point Online Bank*".

Penelitian ini didasarkan pada penelitian sebelumnya mengenai penerapan metode enkripsi pada sistem transaksi elektronik serta penelitian yang menggunakan metode *Advance Vigenere Cipher*. Salah satu penelitian sebelumnya yang mendasari tugas akhir ini adalah penelitian yang dilakukan oleh [3] yang berjudul "Penerapan Metode Enkripsi *Vigenere Cipher* dalam Pengamanan Transaksi *Mobile Banking*". Dari hasil penelitian yang dilakukan, ditarik kesimpulan bahwa 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.

Penelitian lain juga dilakukan oleh [4] yang berjudul "Implementasi Algoritma *Affine Cipher* Dan *Vigenere Cipher* Untuk Keamanan *Login* Sistem Inventori TB Mita Jepara". Hasil dari penelitian ini menunjukkan bahwa keamanan *login* pada sistem yang menggunakan *Affine cipher* dan *Vigenere cipher* yang lebih aman dibandingkan sistem *login* menggunakan algoritma MD5.

Penelitian lainnya mengenai sistem keamanan transaksi data adalah penelitian yang dilakukan oleh [5] yang berjudul "Sistem Keamanan Transaksi Data Dengan Menerapkan *XML* Enkripsi Dan *XML Signature* Dengan Menggunakan Metode *Fast*". Hasil dari penelitian tersebut menyimpulkan bahwa Pengiriman data terenkripsi dalam *XML* dan tanda tangan digital dalam *XML* membatasi ruang gerak *intruder* untuk membaca isi dokumen pesan *SOAP* melalui *protocol http web server* ke *web service* atau sebaliknya.

Berdasarkan dari beberapa tinjauan pustaka diatas, maka disimpulkan bahwa metode *Advance Vigenere Cipher* dapat mencegah adanya intervensi dari pihak luar yang dapat mengakibatkan tidak sampainya data transaksi yang dikirimkan, sehingga dapat menciptakan keamanan dalam sistem transaksi PPOB. Maka judul tugas akhir yang akan diangkat yaitu, "Implementasi Metode Enkripsi *Advance Vigenere Cipher* Dalam Pengamanan Sistem Transaksi *Payment Point Online Bank*".

2. METODE PENELITIAN

2.1 Metodologi Pengumpulan Data

Adapun beberapa metode pengumpulan data yang digunakan dalam membangun aplikasi ini, diantaranya:

1. Kepustakaan, merode ini digunakan untuk mencari dan mempelajari literatur atau sumber pustaka yang berkaitan sistem yang akan dibangun dan mengenai metode *Advance Vigenere Cipher*.
2. Pengambilan data, metode ini digunakan untuk mengumpulkan data yang dibutuhkan di dalam sistem yang akan dibangun. Data ini merupakan data tagihan lunas yang diambil dari loket pembayaran PPOB.

2.2 *Vigenere Cipher*

Vigenere Cipher adalah suatu algoritma kriptografi klasik yang ditemukan oleh Giovan Battista Bellaso. Beliau menuliskan metodenya tersebut pada bukunya yang berjudul La Cifradel. 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.

Algoritma *vigenere cipher* ini menggunakan bujursangkar *vigenere* untuk melakukan enkripsi. Setiap baris di dalam bujursangkar menyatakan huruf-huruf *ciphertext* yang diperoleh dengan *Caesar cipher*. 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 : ITUHO
Plaintext : TEKNIK INFORMATIKA

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

Kunci : ITUHO
Plaintext : TEKNIK INFORMATIKA
Ciphertext : BXEUWS BHMCZFUAWST

Hal tersebut 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 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. Metode *vigenere cipher* ini dapat ditranslasikan ke dalam suatu algoritma pemrograman. Notasi algoritmik yang digunakan untuk mengenkripsi suatu karakter alphabet *plaintext* (*P*) menjadi *ciphertext* (*C*) dengan kunci (*K*) ditunjukkan oleh Persamaan (1).

$$C_i = (P_i + K_i) \; mod \; 26 \qquad (1)$$

Keterangan:
Ci : Karakter ke-i *ciphertext* hasil enkripsi
Pi : Karakter ke-i *plaintext* yang akan dienkripsi
Ki : Karakter ke-i kunci yang akan digunakan untuk enkripsi
mod 26 : Total karakter yang bisa dienkripsi

2.3 *Advance Vigenere Cipher*

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, termasuk 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*) ditunjukkan oleh Persamaan (2).

$$C_i = ((P_i + K_i - 2Ca) \; mod \; 95 + Ca \qquad (2)$$

Sedangkan untuk notasi algoritmik yang digunakan untuk dekripsi ditunjukkan oleh Persamaan (3).

$$C_i = ((P_i - K_i + 95) \; mod \; 95 + Ca \qquad (3)$$

Keterangan:
Ci : Nilai dari karakter ke-i *ciphertext* hasil enkripsi

Pi : Nilai dari karakter ke-i *plaintext* yang akan dienkripsi
Ki : Nilai dari karakter ke-i kunci yang akan digunakan untuk enkripsi
mod 95 : Total karakter yang bisa dienkripsi
Ca : Nilai dari karakter awal dari total keseluruhan karakter yang bisa dienkripsi

Dimana proses penambahan yang terjadi $(P_i + K_i)$ dilakukan dengan menambahkan kode ASCII P_i dengan kode ASCII K_i yang hasil penambahan tersebut dikonversikan ke dalam suatu simbol C_i yang sesuai dengan kode ASCII yang dihasilkan dari proses penambahan kode ASCII P_i + kode ASCII K_i. Pada persamaan (2) total karakter yang dapat dienkripsi adalah 95. Dimana 95 karakter tersebut merupakan karakter-karakter *printable*. 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).

2.4 *Payment Point Online Bank (*PPOB*)*

PPOB atau *Payment Point Online Bank* adalah salah satu sistem layanan pembayaran *online* yang diselenggarakan oleh Perusahaan Listrik Negara (PLN), PT. Telkom, PDAM bekerjasama dengan pihak Perbankan dan *Provider* rekanan. Dengan sistem PPOB *Online* ini, masyarakat umum dapat dengan leluasa membuka loket pembayaran dengan maksud untuk mendekatkan pelayanan loket PLN, Telkom, PDAM, dan lain-lain kepada masyarakat (pelanggan). Dengan adanya sistem PPOB ini, maka diharapkan BUMN sebagai salah satu Badan Usaha Milik Negara dapat memberi peluang usaha baru untuk masyarakat guna membantu menekan angka pengangguran, dan pemberdayaan ekonomi kecil di daerah sebagai salah satu program pemerintah.

Sistem PPOB sendiri merupakan pengembangan dari SOPP *(Semi Online Payment Point)*, dimana transaksi berlangsung secara semi *online*, dan memiliki *delay* (jeda waktu) sehingga *update* data dan arus keuangan memerlukan waktu. Sedangkan pada sistem PPOB, semua berlangsung secara *online*, dimana transaksi manual hanya terjadi pada pelanggan dan loket PPOB, sehingga *update* data dan arus keuangan berlangsung *real time*[2].

2.5 Enkripsi

Tahapan enkripsi terdiri dari beberapa poin, memasukkan data tagihan, menampilkan data transaksi, memasukkan username dan password, kemudian melakukan enkripsi AVC. Berikut penjelasan untuk masing-masing poin dalam tahapan enkripsi:

1. Pertama-tama pengguna layanan PPOB memilih jenis tagihan yang akan diproses, dalam aplikasi ini pilihan pembayaran ada tiga yaitu pembayaran tagihan listrik, pembayaran tagihan PDAM dan pembayaran tagihan pascabayar. Kemudian pengguna memasukkan nomor pelanggan. Setelah nomor pelanggan nomor pelanggan dimasukkan, sistem kemudian mencari apakah nomor pelanggan yang dimasukkan sudah ada didalam *database*.
2. Selanjutnya, apabila nomor pelanggan yang dimasukkan sudah dituemukan di dalam *database*, aplikasi akan menampilkan detail tagihan dari nomor pelanggan yang dimasukkan sebelumnya. Pengguna kemudian memeriksa ulang detail tagihan sebelum melakukan proses enkripsi. Apabila data tagihan sudah benar, maka pengguna akan memasukkan username dan password untuk otentikasi *user* yang dapat melakukan proses transaksi. Sistem kemudian memeriksa *database* apakah *username* dan *password* yang dimasukkan sudah terdaftar atau belum.
3. Apabila data username dan password sudah dikonfirmasi oleh sistem, selanjutnya dilakukan enkripsi terhadap data tagihan menggunakan metode *Advance Vigenere Cipher*. Didalam

sistem ini, data yang akan dienkripsi atau *plaintext* merupakan data tagihan, sedangkan untuk kunci atau key yang akan digunakan merupakan *password* dari pengguna.

4. Untuk mendapatkan gambaran lebih jelas dalam proses enkripsi AVCini, maka akan dicoba dengan menggunakan data sebagai berikut:
   Plaintext : 123-aBx
   Key : Ms^9
   Karena panjang karakter *key* tidak sesuai dengan panjang karakter *plaintext*, maka karakter *key*akan diulangi sampai jumlah karakternya sama dengan jumlah karakter *plaintext*. Maka *plaintext* dan *key*akan menjadi seperti berikut.
   Plaintext : 123-aBx
   Key : Ms^9Ms^
   Kemudian setiap karakter dari *plaintext* dan *key* dikonversi menjadi nilai desimal dari karakter ASCII masing-masing. Sehingga *plaintext* dan *key*akan menjadi seperti berikut.
   Plaintext : 49 50 51 45 97 66 120
   Key : 77 115 94 57 77 115 94
   Dengan menggunakan persamaan (2) maka nilai-nilai dari setiap karakter akan dihitung sehingga akan mendapatkan karakter *ciphertext*. Sebagai contoh untuk perhitungan, akan dicoba dimasukkan kedalam persamaan karakter pertama dari *plaintext* yaitu '1' dan karakter pertama dari *key* yaitu 'M'. Maka perhitungannya akan seperti berikut.

$$C_1 = (P_1 + K_1 - 2 * Ca)\ mod\ 95 + Ca$$
$$= (49 + 77 - 2 * 32)\ mod\ 9 + 32$$
$$= 94$$

   Setelah dimasukkan kedalam persamaan, maka didapatkan untuk karakter *ciphertext* untuk C_1yaitu 94. Dimana karakter untuk desimal ASCII dari 94 adalah '^'. Kemudian akan dilanjutkan sampai C_8sehingga akan didapatkan *ciphertext* sebagai berikut.
   Plaintext : 123-aBx
   Key : Ms^9Ms^
   Ciphertext : ^&qF/6W
   Setelah semua *plaintext* dimasukkan kedalam persamaan, maka didapatkan *ciphertext* '^&qF/6W'.
   Setelah didapatkan *ciphertext* dari hasil enkripsi menggunakan algoritma metode AVC, ciphertext tersebut akan dimasukkan kedalam *database* transaksi. Selanjutnya penyedia layanan PPOB yang akan mengelola *ciphertext* hasil dari enkripsi tersebut.

2.6 Dekripsi

Tahapan dekripsi terdiri dari beberapa poin, menampilkan data transaksi, dan mengkonfirmasi proses transaksi, dimana proses dekripsi dengan metode AVC akan dilakukan. Berikut penjelasan untuk masing-masing poin dalam tahapan dekripsi.

1. Setelah proses enkripsi selesai, maka akan didapatkan data transaksi yang berisikan *ciphertext*. Selanjutnya penyedia layanan PPOB akan melihat dan memilih data transaksi yang akan dikonfirmasi dan dilakukan proses transaksinya.
2. Setelah data transaksi sudah dipastikan, maka proses transaksi akan dilakukan. Kemudian proses dekripsi *ciphertext* dilakukan dalam tahapan ini. Apabila setelah proses dekripsi selesai dan *plaintext* sudah sama dengan *plaintext* awal, maka proses transaksi dilakukan.
3. Untuk mendapatkan gambaran lebih jelas dalam proses dekripsi AVCini, maka akan dicoba dengan menggunakan data yang sama dengan hasil enkripsi pada sub-bab 4.2.1:
   Ciphertext : ^&qF/6W
   Key : Ms^9
   Karena panjang karakter *key* tidak sesuai dengan panjang karakter *ciphertext*, maka karakter *key*akan diulangi sampai jumlah karakternya sama dengan jumlah karakter *ciphertext*. Maka *ciphertext* dan *key*akan menjadi seperti berikut.
   Ciphertext : ^&qF/6W
   Key : Ms^9Ms^
   Kemudian setiap karakter dari *ciphertext* dan *key* dikonversi menjadi nilai desimal dari karakter ASCII masing-masing. Sehingga *ciphertext* dan *key*akan menjadi seperti berikut.
   Ciphertext : 94 38 113 70 47 54 87
   Key : 77 115 94 57 77 115 94
   Dengan menggunakan Persamaan (3) maka nilai-nilai dari setiap karakter akan dihitung sehingga akan mendapatkan kembali karakter *plaintext*. Sebagai contoh untuk perhitungan, akan dicoba

dimasukkan kedalam persamaan karakter pertama dari *ciphertext* yaitu '^' dan karakter pertama dari *key* yaitu 'M'. Maka perhitungannya akan seperti berikut.

$P_1 = (C_1 - K_1 + 95)\ mod\ 95 + Ca$
$= (94 - 77 + 95)\ mod\ 95 + 32$
$= 49$

Setelah dimasukkan kedalam persamaan, maka didapatkan untuk karakter *plaintext* untuk P_1yaitu 49. Dimana karakter untuk desimal ASCII dari 49 adalah '1'. Kemudian akan dilanjutkan sampai P_8sehingga akan didapatkan *plaintext* sebagai berikut.

Ciphertext : ^&qF/6W
Key : Ms^9Ms^
Plaintext : 123-aBx

Setelah semua *ciphertext* dimasukkan kedalam persamaan, maka didapatkan *plaintext* '123-aBx'. Dimana *plaintext* tersebut sudah sama dengan *plaintext* awal, maka proses transaksipun dilakukan dan bukti transaksi akan diterbitkan.

3. HASIL DAN PEMBAHASAN

3.1 Hasil Analisis

Hasil analisis diimplementasikan dalam bentuk sistem keamanan transaksi *Payment Point Online Bank* dengan menggunakan bahasa pemrograman Java. Aplikasi ini merupakan aplikasi *executeable* berformat *.jar.

Spesifikasi perangkat lunak dan perangkat keras yang digunakan dalam implementasi adalah sebagai berikut:

1. Perangkat lunak
   a. Sistem operasi : *Windows* 10
   b. *Builder* : *NetbeansIDE* 8.0
2. Perangkat keras
   a. *Processor* : *Intel® Core™* i3-2370M *CPU* @ 2.40GHz
   b. *RAM* : 4.00 GB
   c. *SystemType* : 64-bit *OperatingSystem*, x64-*basedprocessor*

Spesifikasi perangkat lunak dan perangkat keras minimum yang pernah dicoba dan disarankan untuk menggunakan aplikasi ini adalah sebagai berikut:

1. Perangkat lunak
   a. Sistem operasi : *Windows7*
   b. *NetFramework* : *NetFramework* 4.5.1.

2. Perangkat keras
   1. *Processor* : *Intel® DualCoreCPU* @ 1.30GHz
   2. *RAM* : 2.00 GB
   3. *SystemType* : 32-bit *OperatingSystem*, x32-*basedprocessor*

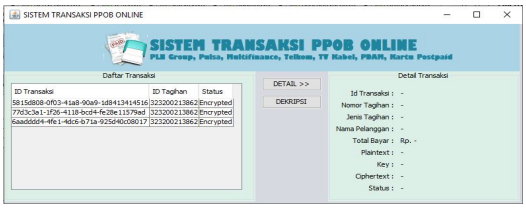
Seperti yang telah dijelaskan pada bab IV, sistem ini terdiri dari dua tahapan utama, yaitu tahapan enkripsi dan tahapan dekripsi. Berikut merupakan implementasi dari tahapan-tahapan tersebut.

1. Enkripsi

Pada tahap enkripsi ini, *userinterface* yang digunakan adalah *userinterfaceform* pengguna. dimana seperti yang telah di jelaskan pada bab sebelumnya, disini pengguna memasukkan data transaksi dan melakukan enkripsi. Gambar 1 merupakan tampilan *userinterface* untuk *form* pengguna.

Gambar 1 *User Interface Form* Transaksi

Ada tambahan untuk tampilan pada tahap enkripsi ini, setelah pelanggan memilih jenis transaksi, memasukkan nomor pelanggan dan kemudian menekan tombol cek tagihan, maka akan muncul jendela baru yang berisi detail tagihan yang tampilannya seperti Gambar 2



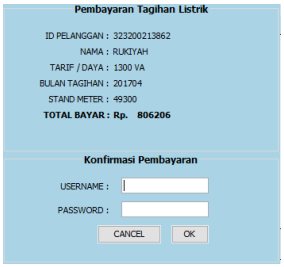
Gambar 2 *User Interface Form* Detail Tagihan

Dibagian bawah *form* detail tagihan terdapat pilihan konfirmasi pembayaran, disini

pengguna memasukkan *username* dan *password* kemudian menekan tombol *ok* untuk mengkonfirmasi pembayaran. Kemudian sistem akan melakukan proses enkripsi dan mengirimkan data transaksi kepada penyedia.

2. Dekripsi

Pada tahap dekripsi ini, *userinterface* yang digunakan adalah *userinterfaceform* penyedia. dimana seperti yang telah di jelaskan pada bab sebelumnya, disini penyedia memilih data transaksi dan melakukan dekripsi. Gambar 3 merupakan tampilan *userinterface* untuk *form* penyedia.



Gambar 3 *User Interface Form* Pembayaran

Implementasi pada *form* penyedia, pada bagian sebelah kanan *form*, terdapat tampilan detail transaksi. Disini data yang telah terpilih di tabel, selanjutnya akan muncul detail transaksinya secara lengkap di bagian kanan *form*. Setelah data yang dimaksud telah terpilih, kemudian pengguna dapat menekan tombol dekripsi untuk melakukan proses dekripsi dan mengkonfirmasi transaksi yang telah dilakukan oleh pengguna.

3. Pengujian

Pengujian dalam penelitian ini yaitu dengan melakukan proses enkripsi dengan menggunakan metode *Advance Vigenere Cipher* kepada data transaksi serta melakukan dekripsi kembali terhadap data transaksi yang sudah terenkripsi sebelumnya. Dalam pengujian sistem ini, akan dilakukan tiga kali pengujian dengan menggunakan tiga data tagihan sebagai *plaintext* dan juga menggunakan tiga *key* yang berbeda. Untuk data tagihan yang akan dienkripsi merupakan data tagihan dari tiga jenis tagihan yang berbeda yaitu, tagihan listrik, tagihan PDAM dan tagihan pascabayar. Sedangkan *key* yang akan digunakan untuk melakukan enkripsi maupun dekripsi merupakan *password* dari tiga user yang berbeda yaitu. Tabel 2 adalah data tagihan (*plaintext*) yang akan digunakan dalam pengujian.

Tabel 2. Data tagihan

Nomor Tagihan	Jenis Tagihan	Nama Pelangggan	Bulan Tagihan	Total Bayar
323200213862	LISTRIK PASCABAYAR	RUKIYAH	201704	806206
08113327778	HALO PASCABAYAR	SUJIANTO	201704	430100
0030700449	PDAM	ADRIANA ZAINUDIN	201703	213500

Tabel 3 merupakan data pengguna yang akan digunakan dalam pengujian.

Tabel 3. Data pengguna

Pengguna	Password (*key*)	Nomor Tagihan	Jenis Tagihan
User1	AhVfO	323200213862	Tagihan listrik
User2	298374	08113327778	Tagihan pascabayar
User3	a2*9=51|X_d#	0030700449	Tagihan PDAM

Seperti yang bisa dilihat pada tabel diatas password yang akan digunakan sebagai *key* untuk melakukan enkripsi dan dekripsi terdiri dari tiga susunan karakter yang berbeda-beda. Pengujian pertama menggunakan *key* yang terdiri dari karakter huruf kapital dan huruf kecil. Pengujian kedua menggunakan *key* yang terdiri dari karakter angka. Sedangkan pengujian ketiga menggunakan *key* yang terdiri dari karakter campuran huruf, angka dan simbol.

Setelah dilakukan tiga kali pengujian dengan menggunakan tiga jenis tagihan dan tiga *user* berbeda, maka didapatkan hasil pengujian sebagai berikut. Setelah melakukan pengujian ternyata metode *Advance Vigenere Cipher* dapat melakukan enkripsi terhadap data transaksi dan menghasilkan *ciphertext* yang dimana bisa dilihat pada Tabel 4.

Tabel 4. Tabel data hasil pengujian

Pengguna	Jenis transaksi	Nomor tagihan	*Password* (*key*)	*Ciphertext*
User1	Tagihan listrik	323200213862	AhVfO	Tzix_QzgygWzVcOm2*;"j4V7pt,w)pz*)fLA;,2xz*~fLAzfwfQ|VcOYxnrfQ~VcO
User2	Tagihan pascabayar	08113327778	298374	BQIDJGDPOJO4/9`Tcc2iYfZUTZqTi4/9kha]Sglb712KHDNDF953KGDENCG4/9
User3	Tagihan PDAM	0030700449	a2*9=51|X_d#	qB=ITEA1lxdabNZj5.|y$7L#`K9wVZK.$.Qa/*KMFH-k_a#sC@EMEA|U_

Dengan karakteristik *ciphertext* yang seperti ini, maka akan sulit pihak luar untuk melakukan intervensi dan mengelola informasi yang dikirimkan dari pihak penyedia layanan PPOB dan pengguna layanan PPOB. Adapun

untuk hasil durasi dari proses enkripsi dan enkripsi bisa dilihat pada Tabel 5.

Nomor tagihan	*Ciphertext*	Durasi enkripsi (detik)	Durasi dekripsi (detik)
323200213862	Tzix_QzgygWzVcO m2*;"j4V7pt,w)pz*)f LA:,2xz*~fLAzfwfQ| VcOYxnrfQ~VcO	0.000348096	0.000309181
08113327778	BQIDJGDPOJO4/9` Tcc2iYfZUTZqTi4/9 kha]Sglb712KHDND F953KGDENCG4/9	0.000183029	0.000241723
0030700449	qB=ITEA1lxd abNZj5.|y$7L#¨K9w VZK.$.Qa/*KMFH- k_a#sC@EMEA|U_	0.000222371	0.000209115

Tabel 5. Tabel waktu durasi enkripsi dan dekripsi

Berdasarkan pada Tabel 5, durasi dari proses enkripsi maupun proses dekripsi dari ketiga data uji tidak jauh berbeda. Karena panjang karakter dari ketiga *plaintext* yang diujikan tidak jauh berbeda yaitu sekitar 50-70 karakter, sehingga durasi proses enkripsi dan dekripsi yang dibutuhkan juga tidak jauh berbeda.

4. KESIMPULAN

Berdasarkan penelitian dan hasil pengujian yang dilakukan terhadap aplikasi penyisipan pesan pada gambar, maka dapat disimpulkan :

1. Metode *Advance Vigenere Cipher* dapat diimplementasikan kedalam pengamanan sistem transaksi *Payment Point Online Bank* melalui aplikasi sistem transaksi PPOB yang dibangun dengan menggunakan bahasa pemrograman *java* dan *NetbeansIDE* 8.0 sebagai *builder*.
2. Dengan menerapkan metode *Advance Vigenere Cipher*, proses transaksi keuangan dapat diamankan dengan baik. Bisa dilihat *ciphertext* yang dihasilkan dari hasil pengujian, dimana *ciphertext* ini memiliki karakteristik yang unik dan tidak bisa dibaca kecuali melakukan dekripsi dengan menggunakan kunci yang sama dengan yang dipakai pada saat enkripsi. Sehingga dapat mencegah adanya intervensi dari pihak luar yang ingin mengelola data transaksi yang dikirimkan. Dibandingkan dengan metode *Vigenere Cipher* yang hanya bisa mengenkripsi karakter huruf yang terbatas, metode *Advance Vigenere Cipher* dapat mengenkripsi informasi elektronik, dimana dalam penelitian ini informasi elektronik yang dimaksud merupakan data transaksi yang dikirimkan dari pengguna layanan PPOB kepada penyedia layanan PPOB. Karena metode AVC ini dapat mengenkripsi semua karakter *printable* yang ada.

5. SARAN

Adapun saran-saran yang dapat penulis berikan untuk pengembangan lebih lanjut terhadap penelitian ini adalah :

1. Perlu adanya penelitian lebih lanjut untuk penerapan metode *Advance Vigenere Cipher* ke sistem transaksi *Payment Point Online Bank* yang transaksinya dilakukan secara online.
2. Perlu adanya penelitian lebih lanjut untuk metode enkripsi lain atau menggunakan metode *hashing* yang bisa diterapkan ke sistem transaksi PPOBserta perlunya distribusi key untuk lebih meningkatkan keamanan.

DAFTAR PUSTAKA

[1] Stiawan, D., 2012, *Makalah Keamanan Jaringan Komputer*, Makalah, Jurusan Teknik Informatika UMS, Surakarta.

[2] Zulkarnaini, 2010, *"Bongkar Rahasia Sukses Bisnis Tour dan Travel"*, Buku, Jakarta

[3] Husodo, A. Y., 2014, *Penerapan Metode Enkripsi Vigenere Cipher dalam Pengamanan Transaksi Mobile Banking, 15 Juni 2014.*

[4] Religia, Y., 2014, *Implementasi Algoritma Affine Cipher Dan Vigenere Cipher Untuk Keamanan Login Sistem Inventori Tb Mita Jepara*, Jepara.

[5] Widodo, S., 2012, *Sistem Keamanan Transaksi Data Dengan Menerapkan XML Enkripsi Dan XML Signature Dengan Menggunakan Metode Fast, Jurnal*, Palembang.