Contents lists available at Scientia Sacra

Scientia Sacra: Jurnal Sains, Teknologi dan Masyarakat
journal homepage:
http://pijarpemikiran.com/index.php/Scientia

Penerapan Ilmu Kriptografi untuk Keamanan Informasi Konsumen Menggunakan Algoritma Vigenere Cipher dan RC6 Berbasis Android (Studi Kasus : PT BFI Finance Indonesia Tbk)

Surya Ade Pratama[1], Hadi Zakaria[2]
[1.2] Universitas Pamulang
suryaap1603@gmail.com[1] , dosen00274@unpam.ac.id[2]

Kata kunci:
Kriptografi, Enkripsi, Dekripsi, *RC6, Block cipher*

Abstrak

Saat ini penggunaan *smartphone* sangat digemari oleh banyak kalangan, khususnya *Smartphone* berbasis Android. Salah satu fitur *Smartphone* yang juga banyak diminati oleh masyarakat adalah SMS, namun ada satu masalah yang sering dihadapi oleh masyarakat dalam menggunakan SMS yaitu masalah keamanan pesan. Untuk itu dibutuhkan suatu aplikasi yang dapat menjaga kerahasiaan informasi tersebut. Kriptografi merupakan salah satu solusi yang dapat dimanfaatkan dan dikembangkan dalam menyelesaikan masalah keamanan pesan. Dengan melakukan enkripsi pada pesan SMS yang mengacak seluruh isi dari pesan asli, sehingga pesan asli tidak akan terbaca. Algoritma kriptografi yang digunakan pada laporan tugas akhir skripsi ini adalah algoritma *Rivest code 6* (RC6). Pada penerapannya, teks sms yang berupa *plaintext* akan ditukar menjadi *ciphertext* yang bersesuaian dengan *key* yang dimasukkan oleh *user*, kemudian mengirimkan ke nomor tujuan. Karakter *plaintext* akan diproses menggunakan metode *Rivest code 6* (RC6). Untuk penerimaan pesan SMS, sistem mendekripsi *ciphertext* dan untuk membacanya *user* harus memasukkan *key* yang sama dengan *key* yang digunakan saat proses enkripsi. Maka dengan otomatis *plaintext* akan terlihat. Setelah algoritma tersebut diterapkan pada pesan sms, maka didapatkan teknik mengenkripsi dan mendekripsi pesan sms yang baik. Aplikasi ini juga mampu untuk menerima, mengirim, menyimpan dan menghapus SMS, baik SMS yang diterima atau yang dikirim melalui aplikasi ini.

Pendahuluan

Sebelum era modern, kriptografi hanya bersangkutan dengan keterpercayaan pesan, dengan mengubah pesan yang dapat dimengerti menjadi tidak dapat dimengerti kemudian proses tersebut dibalikan untuk dapat dibaca, menyebabkan pesan tersebut tidak dapat dibaca oleh penyusup dan mata-mata tanpa pengetahuan khusus yang menyangkut dengan kunci-kunci dekripsi. Enkripsi digunakan untuk menjaga kerahasiaan dalam berkomunikasi, seperti mata-mata, pemimpin militer, dan diplomat. Tulisan rahasia yang pertama kali memerlukan tidak lebih dari sekedar pena dan kertas, karena kebanyakan orang pada masa itu tidak dapat membaca.

Telepon seluler merupakan salah satu hasil dari perkembangan teknologi komunikasi. *Short Message Service* (SMS) atau pesan singkat merupakan fungsi komunikasi yang banyak digunakan oleh pengguna telepon seluler. Salah satu alasan layanan SMS menjadi salah satu layanan yang paling penting dan dibutuhkan dikarenakan SMS mudah digunakan. Namun banyaknya pengguna telepon seluler yang menggunakan layanan SMS ini tidak diimbangi dengan faktor keamanan yang ada pada layanan tersebut.

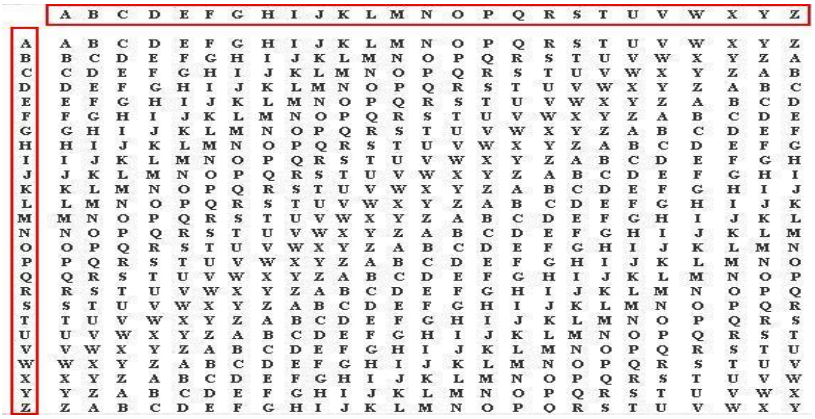
PT BFI Finance Indonesia Tbk adalah sebuah perusahaan pembiayaan di indonesia. Perusahaan pembiayaan ini berdiri pada tahun 1982 dengan nama PT Manufacturer Hanover Leasing Indonesia, yang merupakan perusahan merger antar pemegang saham local dengan Manufacturer Hanover Leasing Corporation. Pada prinsipnya BFI Finance bergerak dalam bidang leasing dan pembiayaan konsumen, termasuk sewa pembiayaan, pembiayaan konsumen, anjak piutang dan kartu kredit. Disini BFI Finance selalu berusaha untuk memberikan pelayanan yang terbaik sesuai dengan kebutuhan nasabah, dalam proses penukaran informasi dari cabang ke pusat. Masih belum adanya aplikasi pertukaran informasi dengan pengamanan berlapis, bila informasi tersebar luas karena ada nya penyadapan, pencurian yang akan menyebabkan kerugian bagi pemilik informasi. Salah satu cara untuk mengamankan data atau informasi dari tindak kejahatan tersebut di butuhkan nya konsep kriptografi.

Banyak karyawan yang belum mengetahui bahwa bertukar informasi melalui telepon seluler tidak menjamin integritas dan keamanan pesan yang disampaikan. Dalam berkomunikasi melalui SMS, pesan yang dikirim dapat dicuri informasinya oleh orang lain (Permana,2014). SMS *spoofing* merupakan pengiriman SMS di mana nomor pengirim yang tertera bukanlah nomor pengirim yang sebenarnya (Azannudin, 2013). Mekanisme SMS spoofing ini dimungkinkan karena lemahnya proteksi koneksi SMSC-gateway (Dwi, 2012). SMS *snooping* lebih sering terjadi karena kelalaian pengguna telepon seluler. Contohnya, ketika seseorang meminjamkan telepon selulernya pada orang lain, pada saat itu orang tersebut dengan sengaja atau tidak membuka isi pesan yang ada pada inbox SMS sehingga pesan yang seharusnya bersifat personal atau rahasia dapat dibaca dengan mudah oleh orang lain melalui cara ini. Sedangkan SMS *interception* merupakan pencurian data pesan SMS ketika pesan masih dalam transmisi dari pengirim ke penerima (Azannudin, 2013).

Untuk mengurangi risiko pada layanan SMS maka dibutuhkan sebuah sistem keamanan pada layanan SMS yang mampu menjaga integritas dan keamanan isi pesan. Enkripsi dan dekripsi pesan dapat digunakan sebagai faktor keamanan tambahan pada layanan SMS (Satyanegara, 2012). Dengan menerapkan algoritma *Vigenere Chipher*, dan *Rivest Code 6* (RC6) pada pesan yang dikirim, maka isi SMS menjadi sulit untuk dibaca karena telah dienkripsi sehingga hanya dapat dibaca dengan menggunakan kunci enkripsi. Tujuan dari penelitian ini adalah mengembangakan aplikasi enkripsi SMS berbasis Android. Dengan adanya aplikasi ini,pengguna dapat mengamankan isi pesan yang dikirim maupun yang diterima sehingga integritas pesan yang sifatnya personal atau rahasia dapat terjaga.

Metode

Pada penelitian ini menggunakan ilmu kriptografi untuk mengamankan informasi konsumen menggunakan algoritma *Vigenere Cipher* dan RC6 . Kriptografi adalah ilmu menulis pesan rahasia dengan tujuan menyembunyikan makna pesan tersebut (harahap, 2016). *Vigenère Cipher* adalah salah satu algoritma kriptografi klasik yang menggunakan metode substitusi abjad-majemuk. Substitusi abjad-majemuk mengenkripsi setiap huruf yang ada menggunakan kunci yang berbeda, tidak seperti *Caesar Cipher* yang menerapkan metode substitusi abjad-tunggal yang semua huruf di suatu pesan dienkripsi menggunakan kunci yang sama. Dengan menggunkan table pemetaan *Vigenère Cipher* dapat dipahami dan diimplementasikan dengan mudah. Table pemetaan *Vigenère Cipher* digunakan untuk memperoleh *ciphertext* dengan menggunkan kunci yang telah ditentukan. Apabila panjang dari kunci lebih pendek dari pada panjang *plaintext*, maka kunci diulang penggunaannya. Bila panjang kunci adalah m, maka priodennya dikatakan m.



Gambar 1. Tabel pemetaan *Vigenère Cipher*

Untuk melakukan enkripsi dengan *Vigenère Cipher*, pada table pemetaan *Vigenère Cipher* tarik garis vertikal dari huruf *plaintext* kebawah, lalu tarik garis horizontal dari huruf kunci kekanan. Perpotongan dari kedua garis tersebut menyatakan hufus *ciphertext*nya. Model matematika dari enkripsi pada algoritma *Vigenère Cipher* ini adalah seperti berikut :

Ci = Ek (Mi) = (Mi + Ki) mod 26
Dan model matematika untuk deskripsinya adalah:
Mi = Dk (Ci) = (Ci - Ki) mod 26

Dengan C memodelkan cipherteks, M memodelkan Plainteks, dan K memodelkan kunci. Contoh dari penerapan algoritma *Vigenère Cipher* adalah jika kita memiliki sebuah *plainteks* yang ingin dienkripsi:

MAKALAH KRIPTOGRAFI
Dan kita menggunakan kunci:

TUGAS
Maka plainteks akan dienkripsi dengan cara:
Plaintext : MAKALAH KRIPTOGRAFI
Kunci : TUGASTU GASTUGASTUG
Ciphertext : FUQADTB QRAINUGJTZO

Huruf pada kunci akan dikonversi menjadi sebuah nilai, misalnya A = 0, B = 1, sampai dengan Z = 25. Setelah itu prosesnya sama seperti pada Caesar cipher dimana setiap huruf pada plainteks akan digeser sejauh nilai kunci yang posisinya bersesuaian.

Algoritma RC6 merupakan salah satu kandidat Advanced Encryption Standard (AES) yang diajukan oleh RSA Laboratoriest kepada NIST. Dirancang oleh Ronald L Rivest, M.J.B. Robshaw, R. Sidney dan Y.L. Yin, algoritma ini merupakan pengembangan dari algoritma sebelumnya yaitu RC5 dan telah memenuhi semua kriteria yang diajukan oleh NIST. Algoritma RC6 adalah versi yang dilengkapi dengan beberapa parameter, sehingga dituliskan sebagai RC6-w/r/b, dimana parameter w merupakan ukuran kata dalam satuan bit, r adalah bilangan bulat bukan negatif yang menunjukan banyaknya iterasi selam proses enkripsi, dan b menunjukan ukuran kunci enkripsi dalam byte. Ketika algoritma ini masuk sebagai kandidat AES, maka ditetapkan nilai parameter w = 32, r = 20 dan b bervariasi antara 16, 24, dan 32 byte.[ABD02] RC6-w/r/b memecah block 128 bit menjadi 4 buah block 32 bit, dan mengikuti enam aturan operasi dasar sebagai berikut : A + B Operasi penjumlahan bilangan integer. A – B Operasi pengurangan bilangan integer. A B Operasi exclusive-OR (XOR)

A x B Operasi perkalian bilangan integer. A<<<B A dirotasikan ke kiri sebanyak variabel kedua (B) A>>>B A dirotasikan ke kanani sebanyak variabel kedua (B) (Prayudi, Yudi; Halik , Idham. 2005).

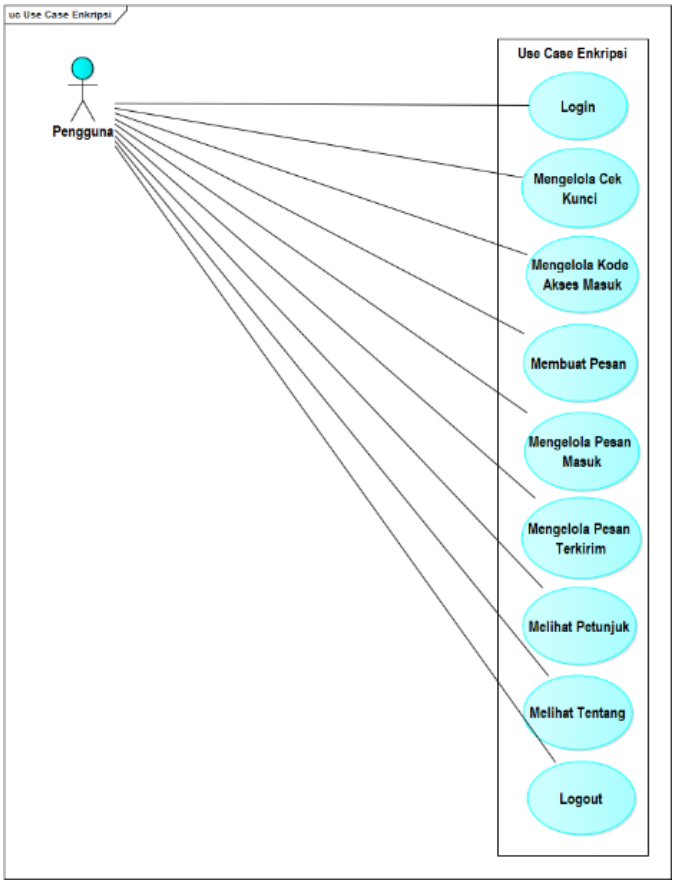
Hasil dan Pembahasan

Desain Sistem Pemodelan UML (Unifield Modeling Language)

Pada penelitian ini peneliti mengunakan perancangan dengan diagram UML yaitu diagram *Use case Diagram, Activity Diagram, dan Sequence Diagram*. Diagram yang digunakan dalam perancangan berorientasi objek berbasiskan UML sebagai berikut:

1. *Use Case Digaram*

Use case diagram menggambarkan fungsional dari suatu sistem yang akan dibangun sehingga dapat dipelajari oleh pengguna. Berikut merupakan *use case diagram* pada aplikasi SMS dengan menerapkan kriptografi menggunakan algoritma *vigenere chipher*, dan RC6 :

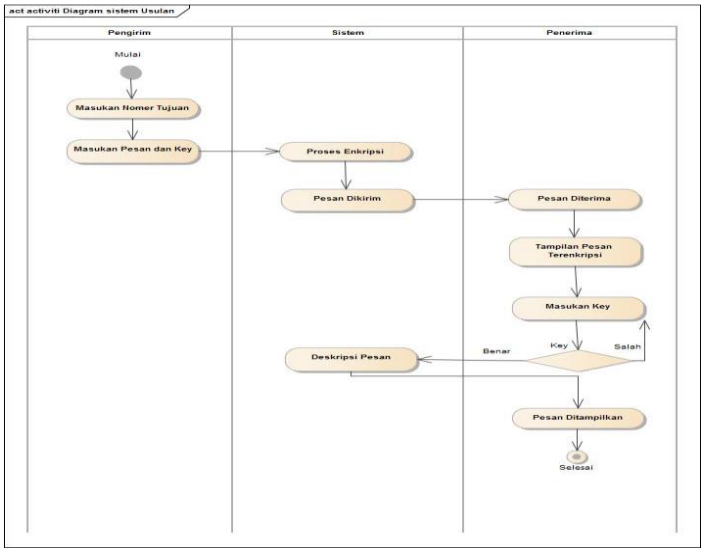


Gambar 2. *Use Case Diagram* Aplikasi SMS

Deskripsi pada gambar di atas pengguna adalah yang menjalankan aplikasi, Pengguna dapat login, mengelola kunci set, mengelola koda akses masuk, membuat pesan, mengelola pesan masuk, mengelola pesan terkirim, melihat petunjuk, melihat tentang, dan *logout*

2. *Activity Diagram*

Aliran kerja digambarkan dengan *activity diagram* untuk memberikan penjelasan mengenai proses kerja dari suatu sistem.

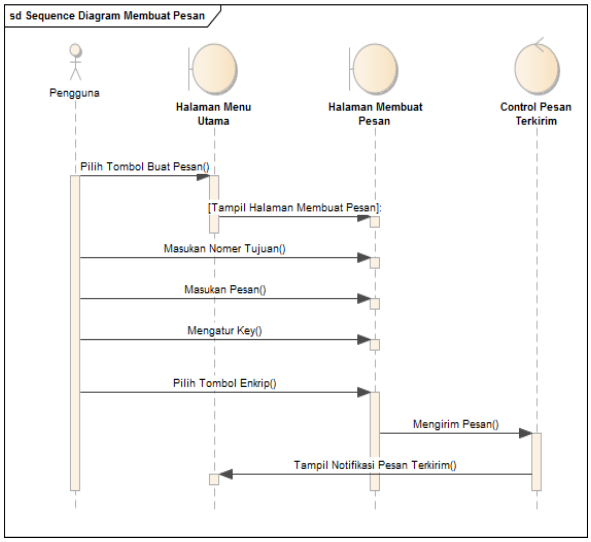


Gambar 3. *Activity Diagram*

3. *Sequence Diagram*

Sequence diagram menggambarkan kelakuan objek pada *use case* dengan mendeskripsikan pesan yang dikirimkan dan diterima antar objek. *Sequence diagram* yang digunakan dalam penelitian ini, yaitu:

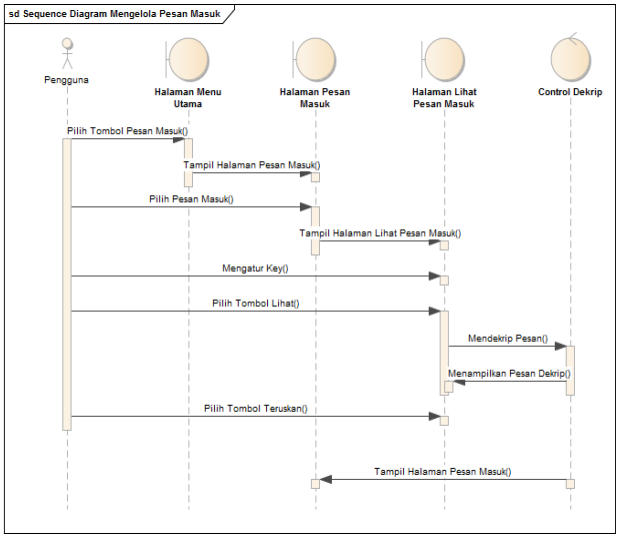
a. *Sequence Diagram* Membuat Pesan



Gambar 4. *Sequence Diagram* Membuat Pesan

Pada gambar *sequence diagram* membuat pesan menjelaskan pengguna ketika memilih menu buat pesan , maka sistem menampilkan halaman buat pesan , lalu pengguna memasukan nomer telpon, memasukan pesan, mengatur key, dan memilih tombol enkrip, makan sistem menampilkan notifikasi pesan telah di kirim.

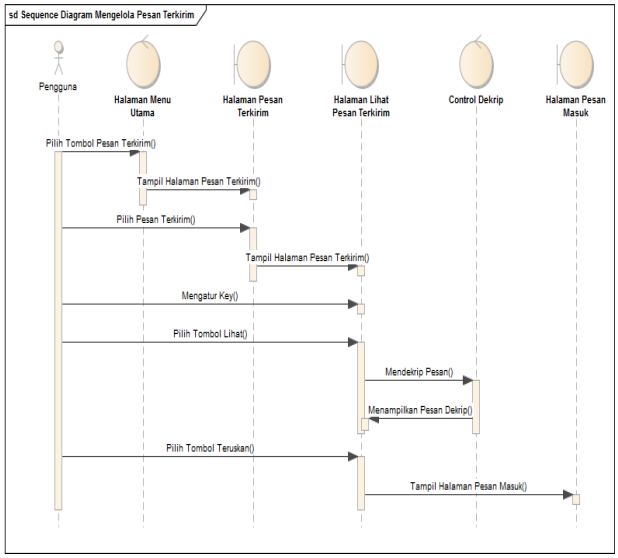
b. *Sequence Diagram* Mengelola Pesan Masuk



Gambar 5. *Sequence Diagram* Mengelola Pesan Masuk

Pada gambar *Sequence Diagram* mengelola pesan masuk menjelaskan ketika pengguna memilih tombol pesan masuk, maka sistem menampilkan halaman pesan masuk , lalu pengguna memilih pesan masuk , maka sistem menampilkan halaman lihat pesan masuk , lalu pengguna mengatur atau memasukan key dan pilih tombol lihat , maka sistem menampilkan pesan yang telah di dekrip , jika pengguna memilih tombol teruskan , maka sistem akan menampilkan halaman buat pesan, dan jika pengguna memilih tombol hapus , maka sistem akan menampilkan notifikasi pesan terhapus.

c. *Sequence Diagram* Mengelola Pesan Terkirim



Gambar 6. *Sequence Diagram* Mengelola Pesan Terkirim

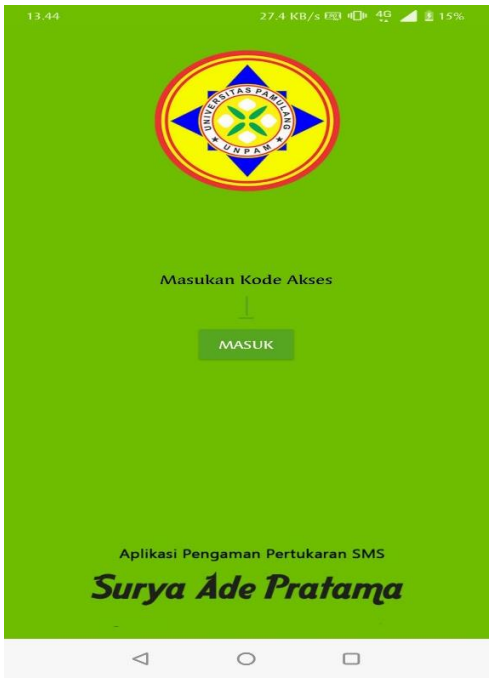
Pada gambar *Sequence Diagram* mengelola pesan terkirim menjelaskan ketika pengguna memilih menu pesan terkirim, maka sistem menampilkan halaman pesan

terkirim , lalu pengguna memilih pesan terkirim, maka sistem menampilkan halaman lihat pesan terkirim, lalu pengguna mengatur atau memasukan key dan pilih tombol lihat , maka sistem menampilkan pesan yang telah di dekrip , jika pengguna memilih tombol teruskan , maka sistem akan menampilkan halaman buat pesan, dan jika pengguna memilih tombol hapus , maka sistem akan menampilkan notifikasi pesan terhapus.

Implementasi

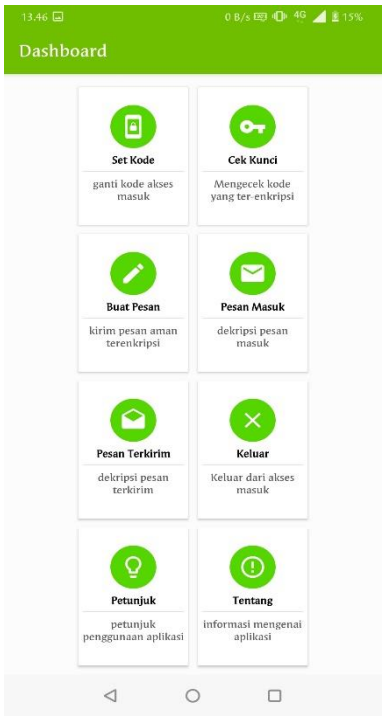
Tampilan hasil dari penerapan ilmu kriptografi untuk keamanan informasi konsumen menggunakan algoritma *Vigenere Cipher* dan RC6 berbasis android (studi kasus:PT BFI Finance Indonesia Tbk)sebagai berikut :

a. Tampilan Menu Login



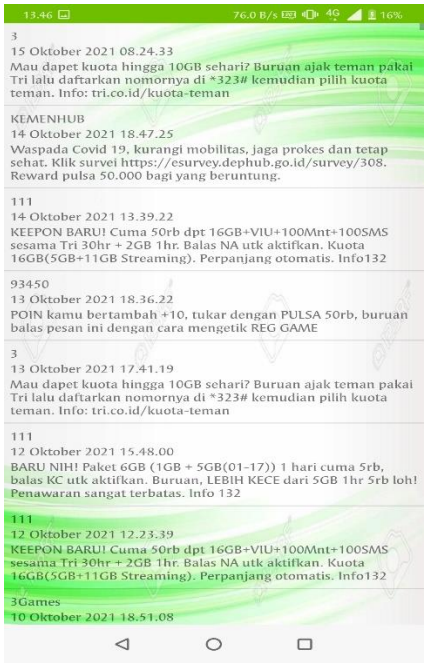
Gambar 7. *Menu Login*

b. Tampilan Menu Utama



Gambar 8. Halaman Menu Utama

c. Tampilan Menu Pesan Masuk



Gambar 9. Halaman Menu Pesan Masuk

d. Tampilan Pesan Keluar

Gambar 10. Tampilan Pesan Keluar

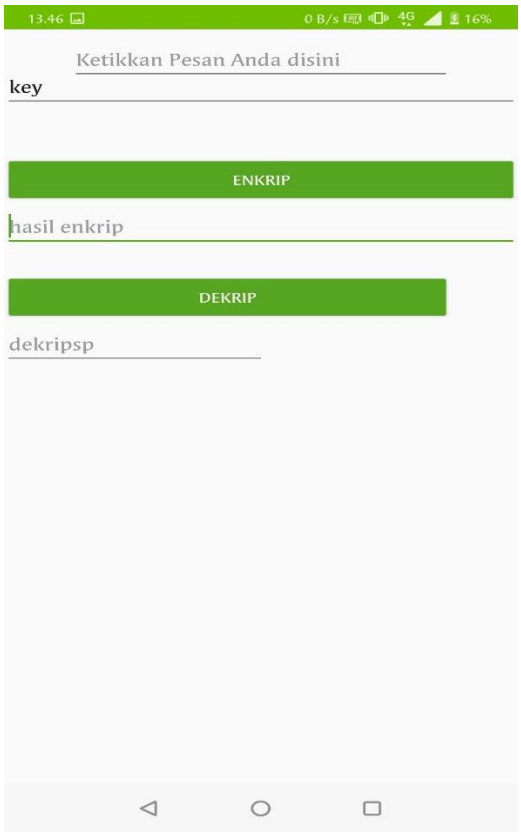
e. Tampilan Buat Pesan

Gambar 11. Tampilan Buat Pesan

f. Tampilan Set Kode

Gambar 12. Tampilan Set Kode

g. Tampilan Cek Key



Gambar 13. Tampilan Cek Key

Pengujian Sistem

Pengujian sistem dilakukan dengan mencoba semua kemungkinan yang terjadi dan pengujian menggunakan pengujian *black box*.

a. Pengujian Black Box

Pengujian *Black Box* dilakukan hanya mengamati hasil eksekusi melalui data uji dan memeriksa fungsionalitas dari aplikasi. Pengujian yang dilakukan berdasarkan sistem yang dibuat, yang akan difungsikan oleh user. Pengujian tersebut dapat digambarkan dalam tabel-tabel sebagai berikut:

Tabel 1. Rencana Pengujian

Item yang diuji	Detail Pengujian	Jenis Pengujian
Login Menu Utama	Validasi Kode	Black Box
Halaman Menu Utama	Mengelola Setiap Tombol Menu Utama	Black Box
Mengelola Cek Kunci	Mengelola Kunci Meng-enkripsi dan Dekripsi	Black Box
Mengelola Set Kode	Mengelola Set Kode	Black Box
Membuat Pesan	Membuat Pesan	Black Box
Mengelola Pesan Masuk	Mengelola Pesan Masuk	Black Box
Mengelola Pesan Terkirim	Mengelola Pesan Terkirim	Black Box
Melihat Petunjuk	Lihat Petunjuk	Black Box
Melihat Tentang	Lihat Tentang	Black Box
Logout	Lihat Halaman Login	Black Box

Berdasarkan rencana pengujian yang telah disusun, maka dapat dilakukan pengujian sebagai berikut:

Tabel 2. Pengujian *Login User*

Kasus dan hasil uji (data benar)			
Data uji	**Hasil yang diharap**	**Hasil yang didapat**	**Kesimpulan**
Input Kode Masuk	Tampil teks pada Kode Masuk	Tampil teks pada Kode Masuk	(√) Diterima ( ) Ditolak
Klik Tombol Masuk	Tampil Halaman Menu Utama	Tampil Halaman Menu Utama	(√) Diterima ( ) Ditolak

Tabel 3. Pengujian Halaman Menu Utama

Kasus dan hasil uji (data benar)			
Data uji	**Hasil yang diharap**	**Hasil yang didapat**	**Kesimpulan**
Klik menu Set Kode	Menampilkan Halaman Ganti Kode Akses	Menampilkan Halaman Ganti Kode Akses	(√) Diterima ( ) Ditolak
Klik menu Cek Kunci	Menampilkan Halaman Mengecek Kunci Enkripsi dan Dekrispsi	Menampilkan Halaman Mengecek Kunci Enkripsi dan Dekrispsi	(√) Diterima ( ) Ditolak
Klik menu Buat Pesan	Menampilkan Halaman Buat Pesan	Menampilkan Halaman Buat Pesan	(√) Diterima ( ) Ditolak
Klik menu Pesan Masuk	Menampilkan Halaman Pesan Masuk	Menampilkan Halaman Pesan Masuk	(√) Diterima ( ) Ditolak
Klik menu Pesan Terkirim	Menampilkan Halaman Pesan Terkirim	Menampilkan Halaman Pesan Terkirim	(√) Diterima ( ) Ditolak
Klik menu Logout	Menampilkan Halaman Login User	Menampilkan Halaman Login User	(√) Diterima ( ) Ditolak
Klik menu Petunjuk	Menampilkan Halaman Petunjuk	Menampilkan Halaman Petunjuk	(√) Diterima ( ) Ditolak
Klik menu Tentang	Menampilkan Halaman Tentang	Menampilkan Halaman Tentang	(√) Diterima ( ) Ditolak

Tabel 4. Pengujian Menu Set Kode

Kasus dan hasil uji (data benar)			
Data uji	**Hasil yang diharap**	**Hasil yang didapat**	**Kesimpulan**
Input Kode Akses Baru	Tampil teks pada Kode Akses Baru	Tampil teks pada Kode Akses Baru	(√) Diterima ( ) Ditolak
Input Konfirmasi Kode Akses Baru	Tampil teks pada Konfirmasi Kode Akses Baru	Tampil teks pada Konfirmasi Kode Akses Baru	(√) Diterima ( ) Ditolak
Klik tombol Ganti Kode	Sistem Menampilkan Pesan Kode Berhasil Diganti	Sistem Menampilkan Pesan Kode Berhasil Diganti	(√) Diterima ( ) Ditolak

Tabel 5. Pengujian Menu Cek Kunci

Kasus dan hasil uji (data benar)			
Data uji	**Data uji**	**Data uji**	**Data uji**
Input Pesan	*Input* Pesan	*Input* Pesan	*Input* Pesan
Input Key	*Input Key*	*Input Key*	*Input Key*
Klik Tombol Enkripsi	*Klik* Tombol Enkripsi	*Klik* Tombol Enkripsi	*Klik* Tombol Enkripsi
Klik Tombol Dekrispi	*Klik* Tombol Dekrispi	*Klik* Tombol Dekrispi	*Klik* Tombol Dekrispi

Tabel 6. Pengujian Menu Membuat Pesan

Kasus dan hasil uji (data benar)			
Data uji	**Hasil yang diharap**	**Hasil yang didapat**	**Kesimpulan**
Input No. Tujuan	Tampil teks pada No.Tujuan	Tampil teks pada No.Tujuan	(√) Diterima ( ) Ditolak
Input Pesan	Tampil teks pada Pesan	Tampil teks pada Pesan	(√) Diterima ( ) Ditolak

Input Key	Tampil *Key*	Tampil *Key*	(√) Diterima ( ) Ditolak
Klik Tombol Enkripsi	Mengirim Pesan ke Nomer Tujuan, Tampil "Pesan Berhasil Terkirim"	Mengirim Pesan ke Nomer Tujuan, Tampil "Pesan Berhasil Terkirim"	(√) Diterima ( ) Ditolak

Kesimpulan

Bedasarkan analisis penelitian dan pembahasaan tentang Penerapan Ilmu Kriptografi Untuk Keamanan Informasi Konsumen Menggunakan Algoritma *Vigenere Cipher* Dan RC6 Berbasis *Android* studi kasus di PT BFI Finance Indonesia Tbk dalam meningkatkan keamanan sistem yang lebih baik agar dapat menjaga kemanan data konsumen dengan menerapkan ilmu kriptografi menggunakan algoritma *Vigenere Chipher* pada sebuah data dalam pesan berbentuk *text* agar tidak bisa diakses oleh pengguna yang memang tidak mempunyai wewenang agar data tidak dapat dimanipulasi. Adapun kesimpulan yang dapat diambil dari pembahasan sebelumnya, yaitu sebagai berikut: 1) Dengan Menggunakan software Android Studio, tools Android sdk, dan mengimplementasikan algoritma *Vigenere Chipher*, dan RC6 pada keamanan pesan. 2) Dengan adanya aplikasi kriptografi ini dapat menambah wawasan kepada karyawan pentingnya menjamin integritas dan kemanan pesan berdasarkan kuesioner dari 20 responden dengan presentasi nilai sebesar 85%. 3) Dengan adanya aplikasi kriptografi ini dapat menjaga keamanan pesan berdasarkan hasil dari 20 responden bahwa aplikasi kriptografi ini dapat menjaga keamanan pesan dengan presentasi nilai sebesar 85%.

Daftar Pustaka

Andi, & Dwi. (2014). Penerapan Algoritma Vigenere Cipher pada Aplikasi SMS Android. *IMPLEMENTASI ALGORITMA CAESAR, CIPHER DISK, DAN SCYTALE PADA APLIKASI ENKRIPSI DAN DEKRIPSI PESAN SINGKAT, LumaSMS*, 467-472.

Azannudin. (2013). Penyandian Short Message Service (SMS) Pada Telepon Selular. *Pelita Informatika Budi Darma*, 1-50.

Basuki, A., & Paranita, U. (2016). PERANCANGAN APLIKASI KRIPTOGRAFI BERLAPIS MENGGUNAKAN ALGORITMA CAESAR, TRANSPOSISI, VIGENERE, DAN BLOK CHIPER BERBASIS MOBILE. *Seminar Nasional Teknologi Informasi dan Multimedia*, 1-5.

Efrandi, Asnawati, & Yupiyanti . (2014). APLIKASI KRIPTOGRAFI PESAN MENGGUNAKAN ALGORITMA VIGENERE CIPHER. *Jurnal Media Infotama* , 121.

Harahap , M. K. (2016). ANALISIS PERBANDINGAN ALGORITMA KRIPTOGRAFI KLASIK VIGENERE CIPHER DAN ONE TIME PAD. *InfoTekJar (Jurnal Nasional Informatika dan Teknologi Jaringan)* , 62.

harahap, m. k. (2016). ANALISIS PERBANDINGAN ALGORITMA KRIPTOGRAFI KLASIK VIGENERE CIPHER DAN ONE TIME PAD . *InfoTekJar (Jurnal Nasional Informatika dan Teknologi Jaringan)* , 62.

Juansyah, A. (2015). PEMBANGUNAN APLIKASI CHILD TRACKER BERBASIS ASSISTED – GLOBAL POSITIONING SYSTEM (A-GPS) DENGAN PLATFORM ANDROID. *Jurnal Ilmiah Komputer dan Informatika (KOMPUTA)*, 2-3.

Karman, J. (2017). SISTEM INFORMASI GEOGRAFIS LOKASI PEMETAAN MASJID BERBASIS ANDROID PADA KOTA LUBUKLINGGAU. *SISTEM INFORMASI GEOGRAFIS LOKASI PEMETAAN MASJID BERBASIS ANDROID PADA KOTA LUBUKLINGGAU*, 3.

Kusniyat, H. (2016). APLIKASI EDUKASI BUDAYA TOBA SAMOSIR BERBASIS ANDROID. *JURNAL TEKNIK INFORMATIKA*, 12.

Mandarani, P. (2014). Analisa Komputasi Enkripsi Dan Dekripsi Data Gambar, Teks Dan Audio Dengan Menggunakan Algoritma Rc4berbasis Visual Basic 6.0. *Junal Teknologi Informasi &*, 33.

Nyura, H. (2010). Pembuatan Aplikasi Pembelajaran Bahasa Inggris Pada. *Jurnal Informatika Mulawarman* , 18.

Paryati, P. (2008). KEAMANAN SISTEM INFORMASI . *Seminar Nasional Informatika 2008 (semnasIF 2008)*, 1.

Permana , T. (2015). Application Encryption and Decryption SMS (Short Message Service) Use RC6 Algorithm Based on Android Mobile Phone. *Sistem Informasi Universitas Gunadarma Jakarta*, 14-15.

Prayudi, Yudi; Halik , Idham ;. (2005). STUDI DAN ANALISIS ALGORITMA RIVEST CODE 6 (RC6) DALAM ENKRIPSI/DEKRIPSI DAT. *Seminar NAsional Aplikasi Teknologi Informasi*, 150.

Rahadi, D. R. (2014). Pengukuran Usability Sistem Menggunakan Use Questionnaire Pada Aplikasi. *Jurnal Sistem Informasi (JSI)*, 662.

Sasmita, I., & Sasmita, I. (2018). RANCANG BANGUN APLIKASI SISTEM INVENTORI PADA PT. BOGA. *Teknik Informatika Universitas Pamulang*, 5