NASKAH PUBLIKASI

PERBANDINGAN ALGORITMA BLOWFISH DAN ALGORITMA RC6 PADA APLIKASI ENKRIPSI DAN DEKRIPSI *SHORT MESSAGE SERVICE* (SMS) BERBASIS ANDROID

Disusun oleh:
Yoga Ade Novry
5130411395

PROGRAM STUDI INFORMATIKA
FAKULTAS TEKNOLOGI INFORMASI DAN ELEKTRO
UNIVERSITAS TEKNOLOGI YOGYAKARTA

2020

NASKAH PUBLIKASI

PERBANDINGAN ALGORITMA BLOWFISH DAN ALGORITMA RC6 PADA APLIKASI ENKRIPSI DAN DEKRIPSI *SHORT MESSAGE SERVICE* (SMS) BERBASIS ANDROID

Disusun oleh:
Yoga Ade Novry
5130411395

Pembimbing.

Suhirman, S.Kom., M.Kom., Ph.D.

Tanggal: 28-02-2020

Perbandingan Algoritma Blowfish Dan Algoritma RC6 Pada Aplikasi Enkripsi Dan Dekripsi *Short Message Service* (SMS) Berbasis Android

Yoga Ade Novry
Program Studi Informatika, Fakultas Teknologi Informasi dan Elektro
Universitas Teknologi Yogykarta
Jl. Ringroad Utara Jombor Sleman Yogyakarta
E-mail : yoga.novry@gmail.com

ABSTRAK

Dalam kegiatan mengirim pesan maupun menerima pesan banyak hal-hal yang dituliskan pada isi pesan tersebut baik teks secara umum maupun teks secara rahasia. Tetapi untuk melakukan teks secara rahasia, ternyata masih disimpan terlebih dahulu oleh operator atau yang disebut dengan Short Message Service Center (SMSC) sebelum dikirimkan kepada penerima, dengan adanya hal tersebut membuat keamanan pesan yang hanya ditujukan kepada penerima dapat dibaca oleh pihak ketiga atau yang dapat mengakses Short Message Servic Center (SMSC). Dengan demikian dibuatlah sebuah sistem yang dimana membuat teks yang dapat dibaca (plain text) menjadi sebuah kode yang tidak dapat dibaca (chiper text). Ada beberapa hal yang dapat dilakukan untuk membuat kode tersebut salah satunya adalah menggunakan enkripsi teks. Dan untuk membaca teks yang telah dienkripsi digunakanlah dekripsi teks agar dapat merubah teks yang berupa kode menjadi teks yang dapat dibaca. Algoritma yang digunakan dalam melakukan enkripsi dan dekripsi ada beberapa macam, salah satunya adalah algoritma blowfish dan algoritma RC6. Disini sistem akan membahas tentang kedua algoritma tersebut dan membandingkan tingkat keamanan dan kecepatan dalam proses enkripsi maupun dekripsi teks dengan sistem yang berbasis mobile (Android). Agar pengguna dapat mengetahui perbandingan keamanan dan kecepatan dari kedua algoritma dalam proses enkripsi dan dekripsi short message service (SMS). Dengan perbandingan kedua algoritma tersebut menghasilkan jumlah teks yang diperoleh saat enkripsi rata-rata dengan jumlah sebesar 0.60% lebih besar algoritma RC6 dibandingkan dengan algoritma Blowfish. Dan waktu rata-rata yang dihasilkan sebesar 0.0106 untuk algoritma Blowfish dan 0.0094 untuk algoritma RC6, jadi algoritma RC6 prosesnya lebih cepat dibanding dengan algoritma Blowfish.

Kata Kunci : Blowfish, RC6, Short Message Service (SMS).

1. PENDAHULUAN

1.1 Latar Belakang

Short Message Service (SMS) adalah salah satu layanan pesan teks yang dikembangkan dan distandarisasi oleh suatu badan bernama European Telecomunication Standars Institute (ETSI) sebagian dari pengembangan Global System for Mobile Communication (GSM) phase 2, yang terdapat pada dokumentasi GSM 03.40 dan GSM 03.38. Fitur SMS ini memungkinkan perangkat stasiun seluler digital (Digital Cellular Terminal, seperti Ponsel) untuk dapat mengirim dan menerima pesan-pesan teks dengan pangjang sampai dengan 160 karakter melalui jaringan GSM (Komputer, W., 2005). Adapun pengertian lain dari SMS adalah layanan yang banyak diaplikasikan pada sistem komunikasi tanpa kabel (nirkabel), memungkinkan dilakukannya pengiriman pesan dalam bentuk alphanumeric antar terminal pelanggan atau menggunakan sistem eksternal seperti e-mail, paging, voice mail dan lain-lain. SMS pertama kali muncul di belahan Eropa pada tahun 1991 bersama sebuah teknologi komunikasi wireless yang saat ini cukup banyak penggunanya, yaitu Global System for Mobile Communication (GSM).

Telepon seluler menyediakan komunikasi yang beragam, salah satunya adalah SMS. Penggunaan SMS semakin popular dikalangan masyarakat dikarenakan mudahnya bertukar informasi tanpa batasan jarak dan waktu. Celah keamanan terbesar pada komunikasi via sms adalah pesan yang dikirmkan akan disimpan terlebih dahulu di Short Message Service Center (SMSC), yaitu dimana SMS disimpan sebelum dikirim ke tujuan. Dengan adanya celah keamanan tersebut, siapa saja yang berhasil memiliki akses ke dalam SMSC akan dapat melihat informasi penting seperti password, nomor pin, dan lain-lain. Sehingga dapat disalahgunakan oleh orang yang tidak bertanggung jawab atau orang yang tidak berhak untuk mengetahui informasi tersebut. Salah satu cara untuk menanggulangi permasalahan yang ada, menggunakan Algoritma Kriptografi. Pengertian Kriptografi adalah ilmu yang bersandarkan pada teknik

matematika untuk berurusan dengan keamanan informasi seperti kerahasiaan, keutuhan dan otentikasi entitas. Adapun macam-macam Algoritma Kriptografi salah satunya adalah Algoritma Blowfish dan Algoritma RC6. Kedua algoritma tersebut dapat digunakan untuk menjaga kerahasiaan pesan teks dari SMS yang akan dikirimkan ke tujuan. Kedua algoritma menggunakan cara yang sama yaitu dengan membuat pesan teks yang akan dikirim menjadi kode acak sehingga tidak dapat dibaca oleh orang yang memiliki akses pada SMSC. Tetapi dengan kedua algoritma tersebut, memiliki perbedaan dan kelebihan masing-masing.

Dengan Algoritma yang ada, maka dibuatlah sistem yang dapat membuktikan perbedaan dari kedua Algoritma, judul yang akan dibuat adalah "Perbandingan Algoritma Blowfish dan Algoritma RC6 Pada Aplikasi Enkripsi dan Dekripsi Short Message Service (SMS) Berbasis Android". Dengan tujuan untuk dapat membuktikan perbandingan dari Algoritma Kriptografi Blowfish dengan Algoritma Kriptografi RC 6.

1.2 Batasan Masalah

Untuk membuat penelitian ini lebih terstruktur, maka dibuat batasan masalah berdasarkan rumusan masalah sebelumnya :

a. Algoritma Kriptografi yang dibandingkan adalah Algoritma Blowfish dan Algoritma RC6 dari segi keamanan dan kecepatan saat proses enkripsi.
b. Proses enkripsi dan dekripsi hanya digunakan untuk data text berupa huruf, angka dan simbol.

1.3 Tujuan Penelitian

Tujuan penelitian yang akan dicapai dalam penelitian ini yaitu:

a. Menghasilkan *game* susun kata Bahasa Inggris yang menarik dengan pengoreksian yang akurat.
b. Menghasilkan output nilai pengguna yang dapat dijadikan acuan kemampuan pengguna.

2. KAJIAN PUSTAKA DAN TEORI

2.1 Landasan Teori

Beberapa hasil penelitian yang pernah dilakukan oleh peneliti seblumnya yang memiliki bidang dan tema yang sama dengan penelitian yang akan dilakukan.

Penelitian [4] melakukan penelitian tentang Optimalisasi Beafourt Chiper Menggunakan Pembangkit Kunci RC4 Dalam Penyandian SMS. Penelitian yang dilakukan yaitu tentang mengoptimalkan pembentukan kunci pada Algoritma Beafourt dengan memanfaatkan proses pembangkitan kunci pada Algoritma RC4 yang diimplementasikan pada penyandian SMS yang saat ini belum bersifat point-to-point (tidak langsung dikirim kepada tujuan).

Penelitian oleh [7] melakukan penilitian tentang Penerapan Algoritma Huffman Untuk Aplikasi Pengamanan SMS Berbasis Android. Penelitian yang dilakukan yaitu menerapkan Algoritma huffman untuk keamanan SMS ketika akan mengirim kan pesan dimana pesan akan disimpan terlebih dahulu pada Short Message Service (SMSC) sebelum dikirimkan ke tujuan.

Penelitian oleh [1] melakukan penelitian tentang Mengukur Kecepatan Enkripsi dan Dekripsi Algoritma RSA pada Pengembangan Sistem Informasi Text Security. Penelitian yang dilakukan adalah membuat aplikasi instant messaging dengan menggunakan Algoritma RSA dan Algoritma CRT. Dimana Algoritma RSA pada proses dekripsi sering terjadi kendala karena ukuran kunci dekripsi yang relatif besar dapat memperlambat proses. Dengan memodifikasi Algoritma Chinese Remainder Theorem (CRT) pada Algoritma RSA atau biasa disebut dengan RSA-CRT dapat membuat proses dekripsi dua kali lebih cepat dibandingkan proses dekripsi RSA.

Penelitian oleh [5] melakukan penilitian tentang Perancangan Media Pengiriman Pesan Teks Dengan Penyandian Pesan Menggunakan Algoritma RC4 Berbasis WEB. Membahas tentang implementasi Algoritma RC4 untuk enkripsi dan dekripsi pesan yang dikirim melalui jaringan LAN maupun internet melalui jaringan. Dengan Algoritma RC4 yang merupakan salah satu Algoritma kunci simetris berbentuk stream cipher yang memproses unit atau bit (byte dalam hal RC4).

Penelitian oleh [2] melakukan penelitian tentang Optimasi Enkripsi Password Menggunakan Algoritma Blowfish. Dalam penelitiannya memberikan informasi tentang Algoritma Blowfish terbukti handal dalam mengamankan password. Algoritma Blowfish tidak mudah untuk diterjemahkan tanpa bantuan kunci, sampai kini belum ada Cryptanalysis yang dapat membongkar pesan tanpa kunci yang dienkripsi oleh Blowfish. Waktu proses untuk enkripsi dan dekripsi untuk masing-masing file memiliki sedikit perbedaan waktu dikarenakan ukuran antara plainteks dan chiperteks berbeda.

Penelitian oleh [6] melakukan penelitian tentang Implementasi Metode Chaesar Chiper Alphabet Majemuk Dalam Kriptografi Untuk Pengamanan

Informasi. Penelitiannya menjelaskan bahwa kriptografi digunakan dalam pengamanan data, dengan teknik Kriptografi dapat dipercaya untuk menangani masalah keamanan data atau informasi, karena Kriptografi selain menggunakan bahasa pemrograman komputer, Kriptografi juga menggunakan rumus matematika. Keamanan data menggunakan Kriptografi Caesar Chiper yang dikatakan bahwa sulit untuk dipecahkan.

Penelitian oleh [11] melakukan penelitian tentang Mengukur Kecepatan Enkripsi Dan Dekripsi Algoritma RSA pada Pengembangan Sistem Informasi Text Security. Penelitiannya menjelaskan bahwa dalam enkripsi dan dekripsi sebuah data memiliki kecepatan yang berbeda, hasil pengujiannya menyatakan bahwa Algoritma RSA dengan 1024 bit memiliki rata-rata kecepatan enkripsi sebesar 352.488 nano second dan rata-rata kecepatan dekripsi sebesar 109.347.917 nano second, sedangkan pada Algoritma RSA 2048 bit memiliki rata-rata kecepatan enkripsi sebesar 1.77.900 nano second dan rata-rata kecepatan dekripsi sebesar 775.282.334 nano second.

2.2 Algoritma Blowfish

Menurut [10] menjelaskan bahwa Blowfish alias "OpenPGP.Cipher.4" merupakan enkripsi yang termasuk dalam golongan Symmetric Cryptosystem , metode enkripsinya mirip dengan DES (DES like Cipher) diciptakan oleh seorang Cryptanalyst bernama Bruce Schneier Presiden perusahaan Counterpane Internet Security, Inc (Perusahaan konsultan tentang kriptografi dan keamanan komputer) dan dipublikasikan tahun 1994. Dibuat untuk digunakan pada komputer yang mempunyai mikroprosesor besar (32-bit keatas dengan cache data yang besar). Blowfish dikembangkan untuk memenuhi kriteria desain yang cepat dalam implementasinya dimana pada keadaan optimal dapat mencapai 26 clock cycle per Byte, kompak dimana dapat berjalan pada memori kurang dari 5 KB, sederhana dalam algoritmanya sehingga mudah diketahui kesalahannya, dan keamanan yang variabel dimana panjang kunci bervariasi (minimum 32 bit, maksimum 448 bit, multiple 8 bit, default 128 bit).

Blowfish dioptimasikan untuk berbagai aplikasi dimana kunci tidak sering berubah, seperti pada jaringan komunikasi atau enkripsi file secara otomatis. Dalam pengimplementasiannya dalam computer bermikroprosesor 32-bit dengan cache data yang besar (Pentium dan Power PC) Blowfish terbukti jauh lebih cepat dari DES. Tetapi Blowfish tidak cocok dengan aplikasi dengan perubahan kunci yang sering atau sebagai fungsi hash satu arah seperti pada aplikasi packet switching. Blowfish pun tidak dapat digunakan pada aplikasi kartu pintar (smart card) karena memerlukan memori yang besar. Algoritma Blowfish terdiri atas dua bagian: key expansion dan enkripsi data.

2.3 Algoritma RC6

Pada jurnal [8] menjelaskan bahwa Algoritma RC6 merupakan algoritma sederhana, fungsi yang digunakan merupakan fungsi yang sederhana dan hanya mengandalkan prinsip iterated cipher untuk keamanan. Tampilan hasil enkripsi dan data hasil enkripsi yang diterima harus diperhatikan, hal ini dikarenakan pada data hasil enkripsi, setiap karakternya akan memiliki panjang 8 bit. Dengan demikian dalam perancangan algoritma RC6 pada SMS karakter-karakter yang akan dienkripsi diubah kedalam nilai ASCII, di mana nilai karakter dalam table ASCII ditambah table karakter special adalah 0 sampai dengan 255, artinya satu karakter ASCII akan diwakili oleh 8 bit, dimana 28 = 256. Sehingga, dalam 1 blok plainteks (32 bit) akan menyimpan 4 karakter dan setiap kali iterasi, maka akan diambil 16 karakter dari plainteks. Panjang plain teks atau panjang kunci kurang dari 16 karakter, maka akan dilakukan padding, yaitu dengan menambah bit “0” (nol) di akhir teks, sehingga panjang teks mencukupi 116 karakter. Layar pada sebagian besar telepon selular hanya dapat menampilkan karakter dengan panjang 7 bit dan pesan yang telah terenkripsi akan berbentuk binary, sehingga layar tidak akan menampilkan dengan semestinya. Oleh karena itu, pada aplikasi yang akan dibangun, untuk menampilkan pesan yang telah terenkripsi, ditambahkan informasi karakter yang terdapat pesan tersebut dengan format heksadesimal agar dapat ditampilkan dilayar dan informasinya lebih terbaca. Algoritma RC6 yang akan digunakan dalam aplikasi SMS yang akan dibangun dengan w sebesar 32 bit, r sebesar 20 kali putaran dan panjang kunci beragam lebih dari 1 karakter (8 bit).

3. METODOLOGI PENELITIAN

3.1 Objek Penelitian

Objek penelitian adalah sasaran atau topik yang menjadi pokok bahasan dalam sebuah penelitian. Pada penelitian ini, penulis melakukan penelitian tentang perbandingan metode antara algoritma RC6 dan Blowfish dengan menggunakan data yang diambil melalui berbagai jurnal dan laporan-laporan.

3.2 Pengumpulan Data

Pengumpulan data adalah suatu metode yang digunakan untuk mendapatkan suatu informasi yang harus dikerjakan pada saat pembuatan sistem. Untuk mempermudah penelitian ini peneliti menggunakan beberapa metode pengumpulan data, diantaranya adalah:

a. Studi Literatur
   Studi literatur adalah teknik pengumpulan data yang dilakukan dengan cara membaca buku, laporan-laporan serta jurnal terkait dengan penelitian yang dilakukan.

b. Pengolahan Data
   Pengolahan data dilakukan setelah terkumpulnya data-data. Kemudian tahap-tahap yang dilakukan dalam pengolahan data diantaranya adalah:
   1. Editing
      Data yang terkumpul dari jurnal, laporan-laporan dan buku semakin lama semakin banyak sehingga perlu dilakukan analisis data melalui editing. Editing adalah merangkum, memilih hal-hal pokok dan memfokuskan hal-hal penting untuk data penelitian. Dalam hal ini peneliti akan mengumpulkan dari keseluruhan data yang sudah peneliti peroleh melalui metode studi literatur yang mengambil data dari berbagai jurnal serta buku yang sesuai dengan topik pembahasan penelitian.
   2. Tabulasi
      Setelah proses editing maka yang harus dilakukan oleh peneliti adalah melakukan tabulasi atau klasifikasi dari data-data yang sudah terkumpul, karena tidak semua bahan yang dikumpulkan oleh peneliti itu sesuai dengan materi yang diteliti. Peneliti bisa mengklasifikasikan dari buku-buku dan jurnal yang peneliti peroleh. Selain itu peneliti juga akan menyusun dan mensistematikan data-data yang telah diperoleh kedalam pola tertentu guna untuk mempermudah bahasan yang ada kaitannya dengan penelitian.
   3. Verifikasi
      Setelah editing data dan mengklasifikasikannya langkah yang kemudian dilakukan adalah verifikasi data yaitu mengecek kembali dari data-data yang sudah terkumpul untuk mengetahui keaslian datanya apakah benar-benar sudah valid sesuai dengan yang diharapkan oleh peneliti.
   4. Menganalisi Data
      Langkah selanjutnya adalah menganalisis data-data yang sudah terkumpul kemudian mengaplikasikannya pada sistem, dengan merubah format dari data yang telah terkumpul sesuai dengan format pada sistem agar sistem dapat berjalan dengan baik.

3.3 Analisis dan Perancangan Sistem

Pada tahap ini akan dilakukan analisa terhadap alur kerja sistem baru dalam pengolaan data yang sudah terkumpul akan dilakukan perancangan sistem baru sesuai dengan alur kerja sistem yang dibuat. Perancangan sistem akan digambarkan secara detail dengan menggunakan Unified Modeling Language (UML). Desain dan pembuatan program yang akan dibangun menggunakan bahasa pemrograman Android Studio.

3.4 Desain Sistem

Pada tahap ini akan menspesifikasikan bagaimana sistem dapat memenuhi kebutuhan pengguna. Untuk dapat memenuhi kebutuhan pengguna, sistem ini memerlukan tahapan desain seperti input, proses, database, output dan interface. Berikut ini akan dijelaskan secara lebih terperinci mengenai input, proses, database, output, dan interface yang akan dibuat adalah sebagai berikut:

a. Desain Input
   Desain ini digunakan untuk memasukkan data masukan ke dalam sistem yang diperlukan untuk memperoleh output. Data yang dimasukkan kedalam sistem diperoleh dari pengguna aplikasi yang berupa text yang akan dienkripsi maupun didekripsi.
b. Desain Proses
   Desain proses merupakan tahap untuk mengkalkulasi pesan text yang diinputkan oleh pengguna aplikasi sehingga menghasilkan output yang diinginkan.
c. Desain Output
   Desain output digunakan sebagai keluaran data yang telah diproses berupa text dekripsi atau text enkripsi yang telah diproses dan dikirimkan ke tujuan.
d. Desain Interface
   Desain interface adalah perancangan antarmuka dilakukan sesederhana mungkin (user friendly) agar mudah dipahami dan dimengerti oleh pengguna, tetapi tidak menghilangkan unsur-unsur penting dalam menyampaikan informasi dari sistem.

3.5 Implementasi Sistem

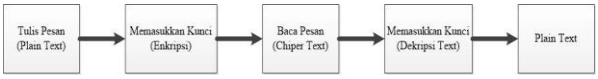
Implementasi merupakan tahap akhir dalam pembangunan sistem. Setelah dilakukan analisis pengumpulan data, pengujian, proses, dan perbaikan terhadap sistem, selanjutnya sistem diterapkan menjadi sistem perbandingan Algoritma Blowfish dan RC6 dalam kriptografi yang digunakan pada Short Message Service (SMS). Tujuan utama sistem ini

adalah mengimplementasikan perbandingan kedua algoritma dalam segi keamanan dan kecepatan enkrispi dekripsi pada android yang ditujukan pada pengguna aplikasi

4. ANALISA DAN PERANCANGAN SISTEM

4.1 Analisis Sistem yang berjalan

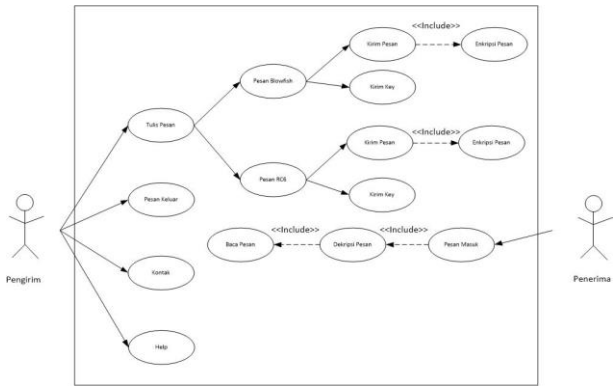
Sistem yang dibangun merupakan perbandingan dua aplikasi kirim pesan melalui internet (*chatting*) berbasis mobile dengan Algoritma Blowfish dan Algoritma RC6 dalam mengirim ataupun membuka pesan. Kedua algoritma digunakan untuk mengenkripsi pesan yang dikirim dengan menggunakan kunci (*key*) sehingga pesan berubah menjadi sebuah pesan yang tidak dapat dibaca oleh orang lain, selanjutnya pesan tersebut dikirim. Kedua Algoritma juga digunakan untuk mendekripsi pesan untuk melihat pesan asli penerima pesan harus memasukkan kunci yang sama pada saat pengirim mengenkripsi pesan. Dengan kesamaan proses yang dilakukan, akan terdapat beberapa perbandingan antara kedua algoritma tersebut baik dari segi keamanan maupun kecepatan dalam memproses pesan yang dikirim maupun diterima. Adapun blok diagram alur kerja sistem akan dijelaskan pada Gambar 1.



Gambar 1 *Blok Diagram Alur Data*

4.2 Use Case Diagram

Use case diagram bertujuan untuk mendeskripsikan sebuah interaksi antara satu atau lebih aktor dengan sistem informasi yang akan dibuat. Secara kasar, *use case* digunakan untuk mengetahui fungsi apa saja yang ada di dalam sebuah sistem informasi dan siapa saja yang berhak menggunakan fungsi-fungsi itu. *Use case* diagram untuk sistem yang akan dibangun terlihat pada Gambar 2.



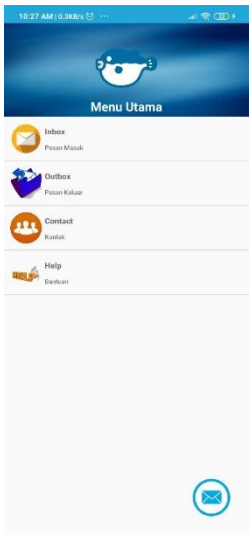
Gambar 2 *Use Case Diagram Aplikasi Chatting Blowfish dan RC6*

4.5 Implementasi

Implementasi bertujuan untuk menjelaskan source code dalam membangun aplikasi ,cara kerja aplikasi , bagaimana aplikasi berjalan. Pada tahap implementasi ini menghasilkan sebuah aplikasi mobile android untuk membandingkan dua algoritma dengan cara mengenkripsi dan mendekripsi pesan menggunakan algoritma Blowfish dan algoritma RC6 , untuk menggunakan aplikasi ini pengguna tidak perlu untuk mendaftar terlebih dahulu karena pesan text menggunakan nomor handphone yang digunakan pada handphone dan daftar kontak yang terpadat pada sistem diambil dari daftar kontak yang ada pada handphone. Proses enkripsi dan dekripsi pesan memerlukan *key* yang sudah diketahui oleh pengirim dan penerima sebelumnya *key* ini dapat berubah-ubah sesuai pengirim dan penerima kehendaki, pengirim dan penerima harus merahasiakn *key* supaya nantinya pesan tidak dapat didekripsi oleh pihak ketiga. *key* digunakan untuk menyamarkan pesan yang dikirim dan mengembalikan pesan yang disamarkan menjadi pesan asli yang dapat dibaca oleh penerima.

a. Halaman *Menu Utama*

Pada halaman menu utama terdapat menu-menu yang dapat digunakan untuk membuka halaman-halaman baru sesuai dengan menu yang dipilih, dalam menu utama terdapat beberapa menu diantaranya *inbox*, *outbox*, *contact*, *help*, dan terdapat tombol pesan. Halaman menu utama dapat dilihat pada Gambar 3.



Gambar 3 *Halaman Menu Utama*

Menu inbox, ketika dipilih akan menampilkan halaman *inbox* , *menu outbox* ketika dipilih akan menampilkan halaman *outbox*, *menu contact* ketika dipilih akan menampilkan halaman *contact*, *menu help* ketika dipilih akan menampilkan *menu help*, dan tombol bergambar pesan pada kanan bawah digunakan untuk menampilkan halaman tulis pesan.

b. Halaman Inbox

Halaman *inbox* terdapat beberapa pesan masuk yang terdapat pada handphone, jadi pada halaman *inbox* menampilkan pesan masuk yang berada pada handphone yang digunakan dalam membuka aplikasi atau sistem yang dibuat. Halaman inbox dapat dilihat pada Gambar 4.

Gambar 4 *Halaman Inbox*

Jika pesan yang ada pada daftar di klik atau dibuka maka akan menampilkan halaman dekripsi pesan atau membaca pesan. dengan format yang sesuai halaman dekripsi pesan.

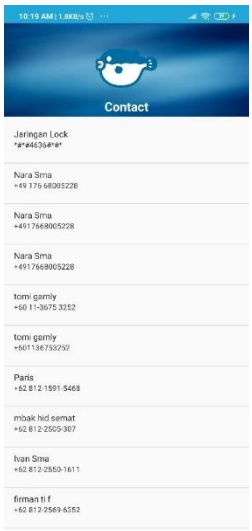
c. Halaman Outbox

Halaman *outbox* terdapat beberapa pesan keluar yang terdapat pada handphone, jadi pada halaman *outbox* menampilkan pesan keluar yang berada pada handphone yang digunakan dalam membuka aplikasi atau sistem yang dibuat. Halaman *outbox* dapat dilihat pada Gambar 5.

Gambar 5 *Halaman Outbox*

d. Halaman Kontak

Halaman kontak terdapat beberapa kontak yang terdapat pada handphone, jadi pada halaman kontak menampilkan kontak yang berada pada handphone yang digunakan dalam membuka aplikasi atau sistem yang dibuat. Halaman kontak dapat dilihat pada Gambar 6.

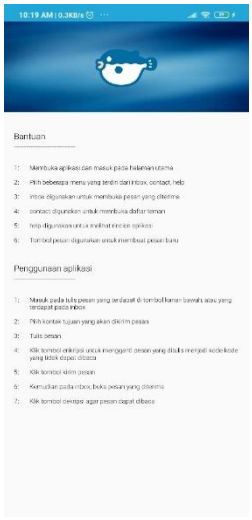


Gambar 6 *Halaman Kontak*

Jika kontak yang ada pada daftar di klik atau dibuka maka akan menampilkan halaman tulis pesan dimana pada halaman tersebut terdapat kontak yang harus diinputkan.

e. Halaman Help

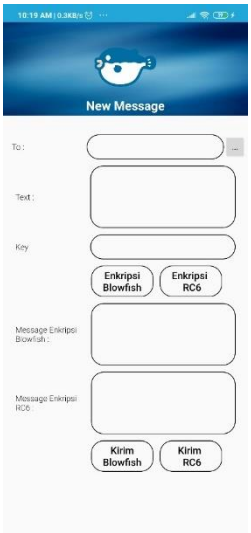
Halaman *help* digunakan untuk menampilkan cara penggunaan sistem yang telah dibuat, pada halaman tersebut terdapat informasi yang dapat membantu pengguna dalam menjalan aplikasi atau sistem. Halaman *help* dapat dilihat pada Gambar 7.



Gambar 7 Halaman Help

f. Halaman Tulis Pesan

Pada halaman tulis pesan terdapat beberapa tombol diantaranya adalah enkripsi blowfish, enkripsi RC6, kirim blowfish dan kirim RC6. Dan terdapat beberapa *input*an yang harus di*input*kan agar sistem dapat berjalan dengan baik dan dapat mengirim pesan pada pengguna lain. Halaman Tulis Pesan dapat dilihat pada Gambar 8.

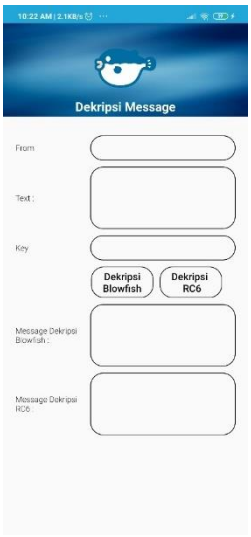


Gambar 8 *Halaman Tulis Pesan*

Pada tombol titik-titik digunakan untuk membuka kontak pada handphone untuk diinputkan nomor handphone kedalam sistem, kemudian teks berisi pesan yang akan dikirimkan, *key* atau kunci yang akan digunakan dalam proses enkripsi dan dekripsi teks yang hanya diketahui oleh pengirim dan penerima pesan, tombol enkripsi Blowfish digunakan untuk memproses pesan teks dan kunci dengan algoritma blowfish, tombol enkripsi RC6 digunakan dalam memproses pesan teks dan kunci dengan algoritma RC6, kemudian tombol yang kirim Blowfish dan tombol kirim RC6 digunakan untuk mengirim pesan teks yang berupa kode sandi yang telah diproses sebelumnya dan dikirim ke nomor tujuan yang telah di*input*kan.

g. Halaman Dekripsi Pesan

Halaman dekripsi pesan akan tampil setelah mengklik atau membuka pesan masuk pada halaman inbox, dan pada halaman dekripsi pesan sudah terdapat pesan yang telah dibuka sebelumnya pada halaman inbox. Halaman dekripsi pesan dapat dilihat pada Gambar 9.



Gambar 9 *Halaman Dekripsi Pesan*

4.6 Hasil Perbandingan

Perbandingan kedua algoritma pada *Short Message Service* (SMS) diimplementasikan pada sistem berupa perbandingan dari waktu yang dihasilkan ketika proses enkripsi dekripsi sedang berjalan dan hasil enkripsi berupa banyaknya teks yang dihasilkan setelah proses enkripsi dengan persentase dari kedua algoritma. Perbandingan kedua algoritma dapat dilihat pada Tabel 1.

Tabel 1. Perbandingan Algoritma Blowfish dan RC6

No	Message	Key	Enkripsi Blowfish	Enkripsi RC6	Text Field Blowfish	Text Field RC6	Percentage Text Field (EKB/ERC6) *100%	Time Blowfish (perdetik)	Time RC6 (perdetik)
1	No Atm BCA 264840173718	BCA	dk8jwcxfqqrHki4DtHG2S+MS9faOBu2t	BAD5188BC733B3421C01CAB09EE4AB13A215D177D3ACBC11EFD1DEC300A51497	32	64	0.5 %	0.014	0.012
2	Selamat Pagi	selamat	cDh9W60UWlZBUawf8ZBCHw	19E87665B8B1CCE109EDF37166F59581	22	32	0.6875 %	0.009	0.013
3	Terimakasih	Terimakasih	0w7YO19J3ReZGpNHzFjHZA	5CCF8828FEB2A29DBBB007F28FD671A1	22	32	0.6875 %	0.010	0.011
4	Saldo Rekening 20.000	saldo	Kl+e+GKmlyMV6iXZoJ/X0hDQWcO50db+	4551329C6DCFDAC2DE13164D46E870CC2E80C4CF57C5EC5369FCB79FEE088259	32	64	0.5 %	0.010	0.005
5	Bayar Asuransi sebesar 500.000	bayar	qaRRNEH2/o7txDOC3V4mX6+xTE5dkKmZYITAiDbjDmA	7BE57BDF3ACD7F3CE74C9B78BC4083EB1B38D124A5CA72149465 98D62AB835DA	43	64	0.6718 %	0.010	0.008
6	Bayar Utang 1.000.000	bayar	SdmrfEcvf1s1sKaqgxtIYmCEwIg24w5g	913C667E4B5C7C1C24421C1B21C13678134AD02F7A56BDEC3A39766B6157936A	32	64	0.5 %	0.008	0.007
7	Nomor hpnya 086547382928	nomor	OeCF047HmNQdvg+WA886yQ2OSPNpl3O/0mkpx0kyj/I	C0ADDA0AC20D62FC06BF1B7CA8A93ED3F13FCAA1C04D3E04CE90159C3521DC32	43	64	0.6718 %	0.013	0.010
Rata-rata							0.60%	0.0106	0.0094

Keterangan :

EKB	=	Enkripsi Blowfish
ERC6	=	Enkripsi RC6
TB	=	Time Blowfish
TRC6	=	Time RC6

Pada tabel 1. dijelaskan bahwa perbandingan kedua algoritma mendapatkan hasil rata rata *text field* yaitu 0.60% untuk perbandingan teks field yang dimana dari segi keamanan dapat dilihat bahwa Algoritma RC6 lebih baik dibandingkan dengan Algoritma Blowfish. Kemudian pada perbandingan waktu yang digunakan, Algoritma Blowfish memiliki rata-rata waktu sebesar 0.0106 detik dan Algoritma RC6 memiliki rata-rata waktu sebesar 0.0094. dan pada saat *plain text* tidak terdapat angka, waktu yang dibutuhkan Algoritma Blowfish untuk enkripsi teks lebih cepat dibandingkan Algoritma RC6. Sehingga dapat disimpulkan bahwa Algoritma RC6 untuk kecepatan saat proses enkripsi lebih cepat dibandingkan dengan Algoritma Blowfish dan Algoritma Blowfish lebih cepat pada saat *plain text* yang tidak terdapat angka.

5. PENUTUP

5.1 Kesimpulan

Berdasarkan penelitian atas sistem perbandingan algoritma Blowfish dan algoritma RC6 pada enkripsi dekripsi pesan teks, penulis mengambil kesimpulan sebagai berikut :

a. Pada penelitian ini Algoritma yang lebih baik adalah Algoritma RC6 karena hasil persentase *field text* yang dihasilkan sebesar 0.60% lebih banyak dibandingkan Algoritma Blowfish, selain itu dalam segi kecepatan, Algoritma Blowfish membutuhkan waktu sebesar 0.0106 detik dan Algoritma RC6 hanya membutuhkan waktu 0.0094 detik.
b. Implementasi perbandingan antara Algoritma Blowfish dan Algoritma RC6 dapat berjalan dengan baik pada aplikasi android.

5.2 Saran

Penelitian yang telah dilakukan dirasa masih jauh dari kata sempurna, untuk penelitian selanjutnya terdapat beberapa saran yang dapat digunakan untuk pengembangan yang lebih baik lagi.

a. Pengembangan aplikasi berbasis web.
b. Membuat tampilan lebih menarik, dan lebih *user friendly*.
c. Menambahkan beberapa fitur yang telah digunakan pada sms dengan versi yang baru.

DAFTAR PUSTAKA

[1] Arief, A. (2016), *Implementasi Kriptografi Kunci Publik dengan Algoritma RSA-CRT pada Aplikasi Instant Messaging*, , *3*(1), 46–54.

[2] Astuti, Y.P., Rachmawanto, E.H., Sari, C.A., Komputer, F.I. dan Nuswantoro, U.D. (2016), *Optimasi Enkripsi Password Menggunakan Algoritma Blowfish*, *15*(1), 15–21.

[3] Atmojo, W.P., Isnanto, R.R. dan Kridalukmana, R. (2016), *Implementasi Aplikasi Kriptografi Pada Layanan Pesan Singkat (SMS) Menggunakan Algoritma RC6 Berbasis Android*, , *4*(3), 450–453.

[4] Diana, M. dan Zebua, T. (2018), *Optimalisasi Beaufort Cipher Menggunakan Pembangkit Kunci RC4 Dalam Penyandian SMS*, , (1), 12–22.

[5] Pandiangan, H., Sijabat, S., Studi, P. dan Informatika, T. (2016), *Perancangan Media Pengiriman Pesan Teks Dengan Penyandian Pesan Menggunakan Algoritma Rc4 Berbasis Web*, *19*(1), 63–71.

[6] Pradipta, A. (2016), *Implementasi Metode Caesar Chiper Alphabet Majemuk Dalam Kriptografi Untuk Pengamanan Informasi*, , *5*(3), 3–6.

[7] Purwaningsih, F. dan Badrul, M. (2017), *Penerapan algoritma huffman untuk aplikasi pengamanan sms berbasis android*, , *4*(2).

[8] Sidin, U.S. (2016), *Pengembangan Aplikasi Secure Message*, , 78–93.

[9] Syaifudin, Y.W., Rozi, I.F., Mentari, M. dan Lestari, V.A. (2018), *Dasar Pemrograman:Dasar Pemrograman*, Polinema Press.

[10] Wardoyo, S., Fahrizal, R. dan Imanullah, Z. (2014), *Aplikasi Teknik Enkripsi Dan Dekripsi File Dengan Algoritma Blowfish Pada Perangkat Mobile Berbasis Android*, , *3*(1), 43–53.

[11] Wulansari, D., Setyawan, F.A. dan Susanto, H. (2016), *Mengukur Kecepatan Enkripsi dan Dekripsi Algoritma RSA pada Pengembangan Sistem Informasi Text Security*, , (Snik), 85–91.