TEKNIK PENGAMANAN DATA PADA LAYANAN PESAN SINGKAT MENGGUNAKAN ALGORITMA RIVEST CODE 6

Kiki Kusumawati[1], Robby Darmawan[2]
Dosen Teknik Informatika[1], Mahasiswa Teknik Informatika[2]
Universitas Satya Negara Indonesia

ABSTRAK

Alat komunikasi telepon seluler pada masa kini bukan lagi sebagai alat komunikasi yang mahal maupun langka, namun sudah menjadi kebutuhan dan gaya hidup yang bisa dikatakan penting dan berarti bagi setiap individu. Karena dengan adanya alat komunikasi seluler ini setiap individu maupun kelompok dapat berkomunikasi secara langsung melalui pengiriman suara, tulisan, gambar, video, maupun kombinasi semuanya tanpa terhalang ruang dan waktu. Dengan semakin meningkatnya fasilitas yang ditawarkan oleh alat komunikasi seluler, maka akan semakin terbuka luas penyalahgunaan atau pengambilan data dari akun pribadi pemilik seluler oleh orang-orang yang tidak bertanggungjawab. Meskipun pada masa sekarang layanan pesan singkat sudah banyak dilakukan melalui media layanan Whatsapp, namun layanan pesan singkat atau Short Messages Service (SMS) juga masih banyak digunakan oleh pengguna. Komunikasi yang melalui media SMS ini bukanlah merupakan jalur yang aman, dikarenakan pesan yang dikirimkan tidak langsung sampai kepada sipenerima melainkan masuk ke jaringan server SMS terlebih dahulu, sehingga SMS yang terkirim bisa saja terbaca oleh pihak yang tidak bertanggungjawab. Untuk meningkatkan keamanan pesan yang bersifat umum dan lebih utama pesan singkat yang bersifat khusus, maka teknik pengamanan data pesan dapat dilakukan melalui teknik enkripsi data pesan teks yang akan dikirimkan dan deskripsi data yang diterima agar dapat dibaca dengan menggunakan Algoritma Rivest Code 6.

Kata Kunci : Kriptografi, Algoritma *Rivest Code 6, Short Message Service, Android*

ABSTRACT

Mobile phones communication foreseeable are not of communication tools is expensive or scarce, but already a needs and lifestyles which can be said to be important and meaningful to every individual.Because of the existence of this mobile communication device of each individual and group can communicate directly through the delivery of voice, text, images, video, or a combination of all without being obstructed by time and space. Ever increasing facilities offered by mobile means of communication, then it will be more widely open to abuse or the taking of data from private owners of mobile accounts by people who were not responsible. Although the current short message service has been done through the media service Whatsapp, however short message service or Short Messages Service (SMS) is also still widely used by mobile. Communication through the media this SMS is not a safe line, because messages sent not directly to the received but rather go into SMS server network in advance, so SMS sent could have been read by the who is not responsible. To improve the security of a message that is both common and more mainstream a special short message, then the message

data security techniques can be done through the technique of data encryption text messages that will be delivered and description of data received in order to be read by using Rivest Code 6 Algorithm.

Keywords: *Cryptography, Rivest Code 6 Algorithm, Short Message Service, Android*

PENDAHULUAN

Media komunikasi manusia salah satunya adalah telepon seluler dimana pada masa sekarang ini telepon seluler sudah menjadi kebutuhan yang tak dapat dihindarkan, karena mampu mengurangi jarak dan waktu untuk berkomunikasi yang digunakan oleh manusia dalam kegiatan pribadi, maupun pekerjaan. Telepon seluler pada masa kini bukan lagi sebagai alat komunikasi yang mahal maupun langka, namun sudah menjadi kebutuhan dan gaya hidup yang bisa dikatakan penting dan berarti bagi setiap individu. Karena dengan adanya alat komunikasi seluler ini setiap individu maupun kelompok dapat berkomunikasi secara langsung melalui pengiriman suara, tulisan, gambar, video, maupun kombinasi semuanya tanpa terhalang ruang dan waktu. Dengan semakin meningkatnya fasilitas yang ditawarkan oleh alat komunikasi seluler, maka akan semakin terbuka luas penyalahgunaan atau pengambilan data dari akun pribadi pemilik seluler oleh orang-orang yang tidak bertanggungjawab. Meskipun pada masa sekarang layanan pesan singkat sudah banyak dilakukan melalui media layanan Whatsapp atau yang lainnya, namun layanan pesan singkat atau Send Messages Service (SMS) juga masih banyak digunakan oleh pengguna seluler. Komunikasi yang melalui media SMS ini bukanlah merupakan jalur yang aman, dikarenakan pesan yang dikirimkan tidak langsung sampai kepada sipenerima melainkan masuk ke jaringan server SMS terlebih dahulu, sehingga SMS yang terkirim bisa saja terbaca oleh pihak yang tidak bertanggungjawab. Untuk meningkatkan keamanan pesan yang bersifat umum dan lebih utama pesan singkat yang bersifat khusus, maka teknik pengamanan data pesan dapat dilakukan melalui teknik enkripsi data pesan teks yang akan dikirimkan dan dekripsi data yang diterima agar dapat dibaca dengan menggunakan Algoritma Rivest Code 6.

TINJAUAN PUSTAKA

Sistem Informasi

Secara umum kata sistem dapat didefinisikan sebagai sebuah kesatuan yang bersifat kompleks dan tersusun atas sejumlah komponen atau elemen yang saling terhubung satu sama lain sehingga memudahkan di dalam jalannya satu atau beberapa buah proses untuk mencapai tujuan tertentu. Menurut John Mc. Manama: 2010, Sistem adalah sebuah struktur konseptual yang tersusun dari fungsi-fungsi yang saling berhubungan, yang bekerja sebagai suatu kesatuan sistem untuk mencapai suatu hasil yang diinginkan secara efektif dan efisien. Sistem merupakan bagian yang melekat dengan elemen teknologi informasi. Perlu diketahui lebih jauh bahwasannya teknologi informasi sendiri terdiri dari dua kata, yaitu teknologi dan informasi. Dimana teknologi merupakan hasil cipta, karsa, dan pemikiran manusia di berbagai bidang kehidupan dalam bentuk produk sebagai hasil dari pembelajaran. Sedangkan informasi merupakan data yang telah diolah, sehingga memberikan arti, nilai, fungsi, dan manfaat bagi pengguna. Menurut William & Sawyer:2007, menyatakan bahawa teknologi informasi adalah teknologi yang menggabungkan antara proses komputasi dengan jalur komunikasi kecepatan tinggi yang membawa data, suara, dan video. Sedangkan menurut Hanif Al-Fattah:2009, sistem informasi merupakan suatu perkumpulan data yang terorganisasi beserta tatacara

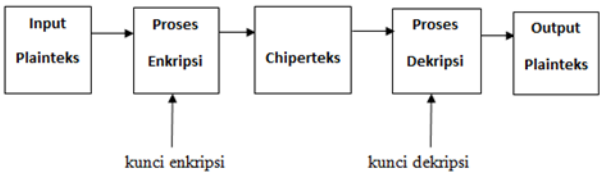
penggunaanya yang mencangkup lebih jauh dari pada sekedar penyajian. Istilah tersebut menyiratkan suatu maksud yang ingin dicapai dengan jalan memilih dan mengatur data serta menyusun tata cara penggunaanya.

Kriptografi

Kriptografi sendiri merupakan suatu ilmu yang mempelajari bagaimana cara menjaga agar data atau pesan tetap aman saat dikirimkan, dari pengirim ke penerima tanpa mengalami gangguan dari pihak ketiga. Menurut Rifki Sadikin, 2012 kriptografi adalah ilmu pengetahuan dan seni menjaga message-message agar tetap aman (secure). Dimana konsep kriptografi itu sendiri telah lama digunakan oleh manusia, misalnya pada peradaban Mesir dan Romawi walau masih sangat sederhana. Untuk lebih lanjut terdapat 4 (empat) prinsip yang mendasari kriptografi yakni:

a) Confidelity (kerahasiaan) yang merupakan layanan agar isi pesan yang dikirimkan tetap rahasia dan tidak diketahui oleh pihak lain (kecuali pihak pengirim, pihak penerima atau pihak-pihak yang memiliki ijin).
b) Dataintegrity (keutuhan data) yang merupakan layanan yang mampu mengenali/mendeteksi adanya manipulasi (penghapusan, pengubahan atau penambahan)data yang tidak sah (oleh pihak lain).
c) Authentication (keotentikan) yang merupakan layanan yang berhubungan dengan identifikasi. Baik otentikasi pihak-pihak yang terlibat dalam pengiriman data maupun otentikasi keaslian data/informasi.
d) Non-repudiation (anti-penyangkalan) yaitu layanan yang dapat mencegah suatu pihak untuk menyangkal aksi yang dilakukan sebelumnya (menyangkal bahwa pesan tersebut berasal dirinya).

Dalam hal ini kriptografi memiliki dua proses utama yaitu proses enkripsi dan proses dekripsi. Seperti yang terlihat pada gambar 1.



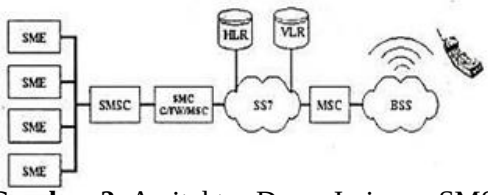
Gambar 1. Diagram proses enkripsi dan deskripsi

Dari gambar 1 di atas dapat dijelaskan beberapa fungsi yang terlibat didalam proses enkripsi dan dekripsi, dimana Plaintext (M) adalah pesan yang hendak dikirimkan (berisi data asli). Ciphertext (C) adalah pesan ter-enkrip (tersandi) yang merupakan hasil enkripsi. Enkripsi (fungsi E) adalah proses pengubahan plaintext menjadi ciphertext. Dekripsi (fungsi D) adalah kebalikan dari enkripsi yakni mengubah ciphertext menjadi plaintext, sehingga berupa data awal/asli. Kunci adalah suatu bilangan yang dirahasiakan yang digunakan dalam proses enkripsi dan dekripsi.

***Short Message Service* (SMS)**

Short Message Service (SMS) dapat diartikan sebagai layanan yang banyak diaplikasikan pada sistem komunikasi tanpa kabel (nirkabel), memungkinkan dilakukannya pengiriman pesan dalam bentuk alphanumeric antar terminal pelanggan atau antar terminal pelanggan dengan sistem eksternal seperti e-mail, paging, voice mail dan lain-lain. Layanan SMS pertama kali muncul di belahan Eropa pada tahun 1991 bersama sebuah teknologi komunikasi wireless yang saat ini cukup banyak penggunanya, yaitu Global Sistem for Mobile Communication (GSM). Dipercaya bahwa pesan pertama

yang dikirim menggunakan SMS dilakukan pada bulan Desember 1992, dikirim dari sebuah Personal Computer (PC) ke telepon mobile dalam jaringan GSM milik Vodafone Inggris. Perkembagan kemudian merambah ke benua Amerika, dipelopori oleh beberapa operator komunikasi bergerak berbasis digital seperti PrimeCo, Nextel, dan beberapa operator lain. Teknologi digital yang digunakan sangat bervariasi dari yang berbasis GSM, Time Division Multiple Access (TDMA), hingga Code Division Multiple Access (CDMA). Secara sistemik cara kerja sistem SMS adalah melakukan pengiriman short message dari satu terminal pelanggan ke terminal yang lain. Hal ini dapat dilakukan berkat adanya sebuah entitas dalam sistem SMS yang bernama Short Message Service Centre (SMSC), disebut juga Message Centre (MC). SMSC merupakan sebuah perangkat yang melakukan tugas store and forward trafik short message. Didalamnya termasuk penentuan atau pencarian rute tujuan akhir dari sort message. Pada gambar 2. terlihat gambaran arsitektur dasar jaringan SMS.



Gambar 2. Arsitektur Dasar Jaringan SMS

Android

Perlu kita ketahui pula definisi dari Android itu sendiri yang merupakan bagian dari sebuah sistem operasi untuk perangkat mobile berbasis linux yang mencangkup sistem operasi, middleware dan aplikasi. Dimana Android itu sendiri mampu menyediakan plartfrom terbuka bagi para penegembangnya untuk menciptakan aplikasi mereka.

Android-SDK merupakan tools bagi para programmer yang ingin mengembangkan aplikasi berbasis google android. Android SDK mencangkup seperangkat alat pengembangan yang komprehensif. Android SDK terdiri dari debugger, libraries, handset emulator, dokumentasi, contoh kode, dan tutorial.

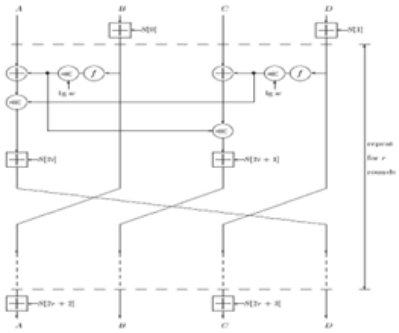
Android Development Tools (ADT) adalah plugin yang didesain untuk IDE Eclipse yang memberikan kemudahan dalam mengembangkan aplikasi android dengan menggunakan IDE Eclipse. Dengan menggunakan ADT untuk Eclipse akan memudahkan dalam membuat aplikasi project android, membuat GUI aplikasi, dan menambahkan komponen-komponen yang lainnya, begitu juga kita dapat melakukan running aplikasi menggunakan android SDK melalui Eclipse. Dengan ADT juga kita dapat melakukan pembuatan package android (.apk) yang digunakan untuk distribusi aplikasi android yang kita rancang.

Algoritma Rivest Code 6 (RC6)

Algoritma RC6 merupakan salah satu kandidat Advanced Encryption Standard (AES) yang diajukan oleh RSA Security Laboratories 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. RC6 adalah algoritma yang menggunakan ukuran blok hingga 128 bit, dengan ukuran kunci yang digunakan bervariasi antara 128, 192 dan 256 bit.

Enkripsi Kriptografi RC6

Pada RC6 memecah blok 128 bit menjadi 4 buah blok 32 bit, maka algoritma ini bekerja dengan 4 buah register 32-bit A, B, C, D. Byte yang pertama dari plaintext atau ciphertext ditempatkan pada byte A, sedangkan byte yang terakhirnya ditempatkan pada byte D. Dalam prosesnya akan didapatkan (A, B, C, D) = (B, C, D, A) yang diartikan bahwa nilai yang terletak pada sisi kanan berasal dari register disisi kiri. Diagram pada proses enkripsi yang terjadi pada algoritma RC6 dapat digambarkan pada gambar 3.



Gambar 3. Proses DiagramBlok Enkripsi

Deskripsi

Proses dekripsi ciphertext pada algoritma RC6 merupakan pembalikan dari proses enkripsi. Pada proses whitening, bila proses enkripsi menggunakan operasi penjumlahan, maka pada proses dekripsi menggunakan operasi pengurangan. Sub kunci yang digunakan pada proses whitening setelah iterasi terakhir diterapkan sebelum iterasi pertama, begitu juga sebaliknya sub kunci yang diterapkan pada proses whitening sebelum iterasi pertama digunakan pada whitening setelah iterasi terkahir. Akibatnya, untuk melakukan dekripsi, hal yang harus dilakukan semata-mata hanyalah menerapkan algoritma yang sama dengan enkripsi, dengan tiap iterasi menggunakan sub kunci yang sama dengan yang digunakan pada saat enkripsi, hanya saja urutan sub kunci yang digunakan terbalik.

Penjadwalan kunci

Pengguna memasukkan sebuah kunci yang besarnya b byte, dimana 0□b□255.byte kunci ini kemudian ditempatkan dalam array c w-bit words L[0]…L[c-1]. Byte pertama kunci akan ditempatkan sebagai pada L[0], byte kedua pada L[1], dan seterusnya. (Catatan, bila b=0 maka c=1 dan L[0]=0). Masing-masing nilai kata w-bit akan dibangkitkan pada penambahan kunci round 2r+4 dan akan ditempatkan pada array S[0,…,2r+3].

Konstanta P32 = B7E15163 dan Q32 = 9E3779B9 (dalam satuan heksadesimal) adalah “konstanta ajaib”yang digunakan dalam penjadwalan kunci pada RC6. nilai P32 diperoleh dari perluasan bilangan biner e-2, dimana e adalah sebuah fungsi logaritma. Sedangkan nilai Q32 diperoleh dari perluasan bilanganbiner □-1, dimana □ dapat dikatakan sebagai “golden ratio” (rasio emas).

Penjadwalan Kunci

Penjadwalan kunci pada RC6 menggunakan sebuah sBox untuk melakukan iterasi awal terhadap S[0]…S[43]. Nilai konstanta P32=B7E15163 (heksadesimal) didefinisikan sebagai inisialisasi awal terhadap S[0] dan inisialisasi awal S[1] hingga S[43] didapatkan dengan menambahkan Q32=9E3779B9 (heksadesimal) terhadap inisialisasi awal

subkunci-subkunci sebelumnya. Pada proses utama penjadwalan kunci, digunakan beberapa operasi seperti pergeseran bit dan operasi penjumlahan yang menyebabkan proses penjadwalan kunci pada RC6 mempunyai kekuatan yang sama dengan RC6 cipher itu sendiri.

Arsip *Ciphertext*

Arsip ciphertext mempunyai ukuran yang lebih besar dari arsip plaintext. Hal ini terjadi karena adanya proses pedding. Pada mode EBC maupun pada metode CBC, perubahan maksimum besarnya arsip ciphertext adalah sebesar satu blok penyandian data (16 byte). Hal ini terjadi semata-mata karena adanya proses padding (16 byte). Walaupun pada metode CBC terdapat proses inisial vektor, namun yang terjadi hanyalah operasi XOR antara inisial vektor dan blok 128 bit sehingga tidak akan merubah besar ukuran ciphertext menjadi lebih besar dibanding mode EBC.

Avallanche Effect

Salah satu karakteristik untuk menentukan baik atau tidaknya suatu algoritma kriptografi adalah dengan melihat avalanche effect-nya. Perubahan yang kecil pada plaintext maupun keyakan menyebabkan perubahan yang signifikan terhadap ciphertext yang dihasilkan. Atau dengan kata lain, perubahan satu bit pada palintext maupun keyakan menghasilkan perubahan banyak bit pada ciphertext. Suatu avalanche effect dikatakan baik jika perubahan bit yang dihasilkan berkisar antara 45-60% (sekitar separuhnya, 50 % adalah hasil yang sangat baik). Hal ini dikarenakan perubahan tersebut berarti membuat perbedaan yang cukup sulit untuk kriptanalis melakukan serangan. RC6 memperlihatkan sebuah avalanche effect yang baik. Hasil yang ditunjukan ini sesuai dengan parameter yang ditetapkan yaitu 50% dari besar blok penyandian.

Java

Java merupakan teknologi dimana teknologi tersebut mencangkup Java sebagai bahasa pemrograman yang memiliki syntax dan aturan pemrograman tersendiri, juga mencangkup Java sebagai plartfrom dimana teknologi ini memiliki virtual machine dan library yang diperlukan untuk menulis dan menjalankan program yang ditulis dengan pemrograman Java.

Extensible Markup Laguage (XML)

Extensible Markup Language (XML) adalah bahasa markup serba guna yang direkomendasikan oleh W3C (World Wide Web Consortium) untuk mendeskripsikan berbagai macam data. XML menggunakan markup tags seperti halnya HTML (Hypertext Markup Language) namun penggunanya tidak terbatas pada tampilan halaman web saja.

Unified Modeling Language (UML)

UML adalah sebuah bahasa yang telah menjadi standar dalam industri untuk visualisai, merancang dan mendokumentasikan sistem piranti perangkat lunak. Diagram UML yang digunakan dalam implementasi sistem ini adalah use case diagram, activity diagram, class diagram dan sequence diagram.

Konversi Bilangan

Konversi bilangan merupakan suatu proses dimana satu sistem bilangan dengan basis tertentu akan dijadikan bilangan dengan basis yang lain. Ada beberapa konversi bilangan, yang salah satunya adalah konversi dari sistem bilangan biner:

a) Konversi bilangan biner ke decimal, proses ini dilakukan dengan cara mengalikan masing-masing bit dalam bilangan dengan position valuenya.
b) Konversi bilangan biner ke Oktal, proses ini dilakukan dengan cara mengkonversikan tiap-tiap tiga buah digit biner yang dimulai dari bagian belakang.
c) Konversi bilangan biner ke Hexademial, proses ini dilakukan dengan cara mengkonversikan tiap-tiap empat buah digit biner yang dimulai dari bagian belakang

METODE PENELITIAN

Penelitian dilakukan untuk mengamankan data dalam layanan pesan singkat dengan menggunakan algoritma Rivest Code 6.

HASIL DAN PEMBAHASAN

Analisa Perhitungan Manual Algoritma RC6

Analisa perhitungan manual algoritma RC6 dengan contoh kasus sebagai berikut, pada perhitungan manual algoritma RC6 ini diberikan kunci sebesar 16 byte dan plainteks sebesar 128 bit (16 byte). Kunci dan plainteks yang menjadi contoh masing-masing sebagai berikut :

Kunci : robby darmawan01
Plainteks : universitassatya

Langkah pertama adalah membagi painteks kedalam 4 blok yaitu A, B, C, D yang masing-masing blok terdiri dari 32 bit (4 karakter)

A	B	C	D
univ	ersi	tass	atya

Ubah tiap karakter dalam masing-masing blok kedalam nilai ASCII, selanjutnya ubah nilai ASCII tersebut menjadi bilangan biner masing-masing sepanjang 8 bit, sehingga pada masing-masing blok akan dihasilkan bilangan biner sepanjang 32 bit.

Blok A				
Plainteks	u	n	i	v
ASCII	117	110	105	118
Biner	01110101	01101110	01101001	01110110

Blok B				
Plainteks	e	r	s	i
ASCII	101	114	115	105
Biner	01100101	01110010	01110011	01101001

Blok C				
Plainteks	t	a	s	s
ASCII	116	97	115	115
Biner	01110100	01100001	01110011	01110011

Blok D				
Plainteks	a	t	y	a
ASCII	97	116	121	97
Biner	01100001	01110100	01111001	01100001

Kemudian bilangan biner digabungkan kembali, dengan aturan byte pertama plainteks diletakan pada *lest significant bit* blok A. dan byte terakhir plainteks diletakan pada *most significant bit blok* D

Blok A : 01110110 01101001 01101110 01110101
Dalam decimal : 1.986.621.045
Blok B : 01101001 01110011 01110010 01100101
Dalam decimal : 1.769.173.605
Blok C : 01110011 01110011 01100001 01110100
Dalam decimal : 1.936.941.428
Blok D : 01100001 01111001 01110100 01100001
Dalam decimal : 1.635.349.601

Setelah didapat nilai pada masing-masing blok, maka dilanjutkan dengan langkah-langkah berikut :

1) Whitening Awal

Whitening awal, dengan menjumlahkan B dengan subkunci S(0), dan D dengan subkunci S(1). Penjumlahan dilakukan dalam modulo 2^{32}

B = B + S(0)
D = D + S(1)
B = 1.769.173.605 + 5.004.899.269 mod ^32
= 6.774.072.874 mod 4.294.967.296
= 2.479.105.578
D = 1.635.349.601 + 4.686.601.755 mod ^ 32
= 6.321.951.356 mod 4.294.967.296
= 2.026.984.060

2) Iterasi

Iterasi dilakukan sebanyak 20 kali. Setiap iterasi mengikuti aturan sebagai berikut:

t ß ROTL ((X [1] * (2*X[1]+1)), 5)
u ß ROTL ((X[3] * (2*X[3]+1)), 5)
x[0] ß (ROTL ((X[0] XOR t), u)) + S[2*i]
x[2] ß (ROTL ((X[0] XOR u), t)) + S[2*i+1]
Temp ß X[0]

X [0] ß X[1]
X [1] ß X[2]
X [2] ß X[3]
X [3] ß Temp

Nilai t dan u didapat dari blok B dan D di proses dengan fungsi f(x)=x(2x+1), kemudian dilanjutkan dengan menggeser nilai t dan u kekiri sejauh 5 bit.

t = (B * (2*B+1))
= (2.479.105.578 * (2 * 2.479.105.578 + 1)) mod 2^32
= (2.479.105.578 * 4.958.211.158) mod 4.294.967.296
= 6.154.815.135.009.912.292 mod 4.294.967.296
= 1.953.936.384

T : (dalam biner) 01110100011101101011010000000000
T : (digeser 5 bit) 10001110110101101000000000
T : (dalam desimal) 2.396.422.158

Nilai 5 bit terakhir dari t yaitu 01110, atau dalam desimal sebesar 14, akan dipergunakan sebagai nilai penggeser blok C pada proses berikutnya, sejauh 14 bit
u = (D * (2 * D +1) mod 2^32
= (2.026.984.060 * (2*2.026.984.060 + 1)) mod 2^32
= (2.026.984.060 * (4.053.968.121+ 1)) mod 2^32
= (2.026.984.060 * 4.053.968.122) mod 2^32
= 8.217.328.763.042.135,320 mod 4.294.967.296
= 625.203.201

u : (dalam biner) 00100101010000011110110000000001
u : (digeser 5 bit) 10101000011110110000000001
u : (dalam desimal) 2.826.633.252
Nilai 5 bit terakhir dari u yaitu 00100, atau dalam desimal sebesar 4, akan dipergunakan sebagai pergeseran blok A pada proses berikutnya sejauh 4 bit
Maka didapatkan nilai-nilai sebagai berikut :
t = 2.396.422.158
u = 2.826.633.252
penggeser t = 14
penggeser u = 4

Langkah selanjutnya adalah memproses blok A dan C dengan nilai-nilai yang telah dihasilkan.
A = (ROTL ((A XOR t), u)) + S[2*i]
A : 1.986.621.045 dalam biner 01110110011010010110111001110101
t : 2.396.422.158 dalam biner 01110100011101101011010000000000
A : (hasil XOR) 00000010000111111101101001110101
A : (digeser 14 bit) 11110110100111010100000010000111
A : (dalam desimal) 4.137.500.807
Nilai A dijumlahkan dengan sub kunci S(2), dalam modulo 2^{32} :
A = 4.137.500.807 + 4.574.206.767 mod 2^32
= 8.711.707.574 mod 4.294.967.296
= 121.772.982

C = (ROTL ((C XOR u), t)) + S[2*i+1]
C : 1.936.941.428 dalam biner 01110011011100110110000101110100
u : 2.826.633.252 dalam biner 10101000011110110000000000100100

C : (hasil xor) 11011011000010000110000101010000
C : (di geser 4 bit) 10110000100001100001010100001101
C : (dalam desimal) 2.961.577.229
Nilai C dijumlahkan dengan subkunci S(3), dalam modulo 2^{32}
C = 2.961.577.229 + 4.289.047.017 mod 2^32
= 7.250.624.246 mod 4.294.967.296
= 2.955.656.950
Maka didapat nilai masing-masing blok adalah :
A : 121.772.982
B : 1.953.936.384
C : 2.955.656.950
D : 625.203.201

Langkah berikutnya adalah mempertukarkan nilai blok dengan aturan (A, B, C, D) dengan (B, C, D, A), sehingga pada iterasi pertama didapatkan nilai pada masing masing blok sebagai beikut :
A : 1.953.936.384
B : 2.955.656.950
C : 625.203.201
D : 121.772.982
Nilai masing-masing blok akan dilanjutkan pada iterasi selanjutnya sebanyak 20 kali.

Implementasi Antarmuka
Adapun hasil implementasi dari antarmuka sistem yang akan dipaparkan tergambar dalam implementasi sistem antar muka yang tersusun secara sistematik dari halaman menu utama sampai dengan hasil akhir dari proses enkripsi dan dekripsi data dalam bentuk teks yang dikirim hingga diterima oleh sipenerima berita.

a) Tampilan Halaman Menu Utama

Gambar 4. Halaman antarmuka menu utama

b) Tampilan Halaman Antarmuka Tulis Pesan

Gambar 5. Halaman antarmuka tulis pesan

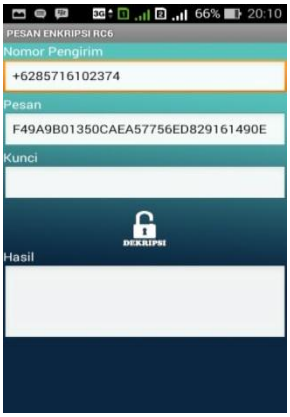
c) Tampilan Halaman Antarmuka Tulis Pesan Terenkripsi

Gambar 6. Halaman antarmuka tulis pesan terenkripsi

d) Tampilan Halaman List Lihat Pesan Masuk

Gambar 7. Halaman antarmuka list lihat pesan masuk

e) Tampilan Halaman Antarmuka Pesan Masuk



Gambar 8. Halaman antarmuka pesan masuk

f) Tampilan Halaman Antarmuka Dekripsi Pesan

Gambar 9. Halaman antarmuka dekripsi pesan

KESIMPULAN DAN SARAN

Kesimpula

Dari hasil penelitian dapat diambil kesimpulan sebagai berikut :

1) Dengan menggunakan metode algoritma RC6 telah dapat diaplikasikan ke dalam aplikasi berbasis android untuk pengamanan data teks pada layanan pesan singkat.
2) Semakin besar jumlah rotasi pada algoritma RC6, maka tingkat keamanan semakin baik, namun waktu yang diperlukan untuk melakukan enkripsi maupun dekripsi semakin lama

Saran

Dalam penelitian ini tentu saja masih mempunyai kekurangan. Masih banyak hal yang dapat dilakukan untuk pengembangannya agar menjadi lebih baik lagi, sebagai berikut :

1. Tahapan iterasi dalam penelitian ini dalam perhitungan manual hanya satu kali diharapkan untuk penelitian selanjutnya menambahkan jumlah iterasi agar keamanan data lebih baik.
2. Aplikasi secure message ini hanya dapat mengenkripsi dan mendekripsi teks pada layanan pesan singkat saja diharapkan untuk pengembang selanjutnya dapat mengengkripsi dan mendekripsi file, music dan gambar agar aplikasi ini dapat memenuhi kebutuhan pengguna.
3. Aplikasi yang telah dibuat ini tidak menangani pengiriman kunci enkripsi dan dekripsi, jadi penerima harus dapat mengetahui kunci enkripsi agar dapat membuka pesan yang dikirimkan.
4. Aplikasi secure message ini berjalan pada plartfrom berbasis android, diharapkan aplikasi secure message ini dapat dijalankan pada multiplartfrom sehingga dapat memudahkan pengguna dalam menjalankan dan mengamankan data teks pada layanan pesan singkat.

DAFTAR PUSTAKA

Al Fattah, Hanif. 2007, Analisis dan Perancangan Sistem Informasi, Yogyakarta: Andi Publisher.

Ariyus, Dony. 2010, Kriptografi Keamanan Data dan Komunikasi.Yogyakarta: Graha Ilmu.

Indra, Muhammad. 2014, Algoritma RC6 untuk enkripsi dan dekripsi SMS, Teknik Informatika, Jurusan Teknik Informatika, Sekolah Tinggi Manajemen Informatika dan Komputer, Amikom, Yogyakarta.

Manama, John Mc. 2010, Design danPerencanaanSistemInformasi. Jakarta: Luxima

Muchlisin Riadi. 2012, Teori SMS (Short Message Service).http://www.kajianpustaka.com/2012/12/teori-sms-short-message-service.html. Diakses pada 23 Maret 2018, Pukul 13.35.

Munandar, Dede. 2013, Aplikasi mengamankan pesan mail client menggunakan algoritma RC6, Teknik dan Ilmu Komputer, Jurusan Teknik Informatika, Universitas Komputer Indonesia.

Nugroho, Adi. 2010, Rekayasa Perangkat Lunak Menggunakan UML dan Java, Yogyakarta: Andi Publisher.

Rivest, Ronald L; Robshaw, M.J.B; Sidney, R; and Yin, Y.L. 1998, The RC6 Block Cipher, AES Submission.

Sadikin, Rifki. 2012, Kriptografi Untuk Keamanan Jaringan. Yogyakarta :Andi.

Safaat, Nazarudin H. 2012, Pemprograman Aplikasi Mobile Smartphone dan Tablet Pc Berbasis Android. Bandung: Informatika Bandung.

Safaat, Nazarudin H. 2013, Berbagai Implementasi dan Pengembangan Aplikasi Mobile Berbasis Android. Bandung: Informatika Bandung.

Setiawan, Iwan. 2014, Rancang bangun aplikasi enkripsi dan dekripsi dengan algoritma kriptografi RC-6 pada plartfrom berbasis android, Teknik Informatika, Jurusan Teknik dan Ilmu Komputer, Universitas Komputer Indonesia.

Uswiratri, Yuli. 2011, Implementasi algoritma RC6 untuk enkripsi citra pada MMS dengan menggunakan J2ME, Teknik Informatika, Jurusan Teknik Informatika, Sekolah Tinggi Manajemen Informatika dan Komputer, Amikom, Yogyakarta.

Williams and Stacey C. Sawyer, 20017, Using information technology : a practical introduction to computers & communications, Boston : McGraw Hill Irwin.

Wisnu Adi Permana, Rangga. 2010, Implementasi Algoritma RC6 untuk enkripsi SMS pada telepon selular, Jurusan Teknik Informatika, Fakultas Teknik, Institut Teknologi Bandung.