PENERAPAN ALGORITMA DES DAN RC6 PADA APLIKASI ENKRIPSI SMS BERBASIS ANDROID

Hatsmi Faisal Anwar[1], Khafiizh Hastuti [2]
[1,2]Jurusan Teknik Informatika, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro
Jl. Imam Bonjol No. 205-207, Semarang, 50131, (024) 3517261
E-mail : faisanw3r@gmail.com[1], afis@dsn.dinus.ac.id[2]

Abstrak

Smartphone Android adalah telepon seluler yang sedang berkembang dan menjadi kebutuhan di era modern ini. Fasilitas dasar dari telepon seluler yang ada pada smartphone salah satunya adalah Short Message Service (SMS) yang berguna untuk melakukan komunikasi berupa pesan teks singkat. Walaupun masih banyak fitur lain yang lebih menarik, layanan SMS masih banyak digunakan oleh pengguna smartphone karena mudah dan praktis penggunaannya. Dengan banyaknya pengguna layanan SMS, bukan berarti SMS merupakan layanan yang terbaik jika ditinjau dari segi keamanan pesan teks tersebut. Maka dari itu, layanan SMS memerlukan sebuah fitur yang dapat meningkatkan keamanan pesan, salah satunya adalah dengan cara disandikan enkripsi. Enkripsi adalah proses mengamankan suatu informasi dengan membuat informasi tersebut tidak dapat dibaca tanpa bantuan pengetahuan dan atau alat khusus. Pada penelitian ini penulis mengimplementasikan dua algoritma DES dan RC6 untuk proses enkripsi dan deskripsi pesan SMS. Sehingga menghasilkan aplikasi enkripsi SMS berbasis android.

Kata Kunci: *enkripsi, dekripsi, SMS, kriptografi, DES, RC6, smartphone android*

Abstract

Android smartphone is a mobile phone that is growing and becoming a necessity in this modern era. The basic facilities of the existing cell phone to a smartphone one of which is the Short Message Service (SMS), which is useful for communication in the form of short text messages. Although there are many more interesting features, SMS services are still widely used by smartphone users as it is easy and practical to use. With the number of users of SMS services, SMS does not mean the best service in terms of safety if the text message. Therefore, the SMS service requires a feature that can increase the security of messages, one of which is by way of an encoded encryption. Encryption is the process of securing the information to make such information can not be read without the help of the knowledge or special tools. In this study, the authors implemented two DES algorithms and RC6 for encryption and description of the SMS message. Resulting in SMS encryption applications based on Android.

Keywords: encryption, decryption, SMS, cryptography, DES, RC6, android smartphone

1. PENDAHULUAN

Smartphone adalah telepon seluler yang sedang berkembang dan menjadi kebutuhan di era modern ini. Hampir semua golongan masyarakat menggunakan smartphone. Selain harganya yang terjangkau, smartphone juga memiliki fitur teknologi terbaru yang berfungsi layaknya komputer. Sehingga memudahkan pengguna sebagai alat bantu dalam kehidupan sehari-hari baik untuk kebutuhan pribadi maupun untuk memudahkan pekerjaan pengguna.

Tahun 2014 pengguna telepon seluler di dunia mencapai 7 miliar dan diprediksi tahun 2015 jumlah pengguna telepon seluler melampaui jumlah penduduk dunia [1]. Indonesia pada tahun 2015

telah menduduki peringkat kelima sebagai negara pengguna smartphone terbanyak di dunia [2]. Salah satu smartphone yang sering digunakan saat ini adalah smartphone Android. Dengan berbagai macam fasilitas dan fungsi yang memudahkan aktifitas pengguna, smartphone android menjadi salah satu smartphone yang paling banyak diminati. Fasilitas dasar dari telepon seluler yang ada pada smartphone salah satunya adalah *Short Message Service* (SMS) untuk melakukan komunikasi berupa pesan teks singkat. Walaupun masih banyak fitur lain yang lebih menarik, layanan SMS masih banyak digunakan oleh pengguna smartphone karena mudah dan praktis penggunaannya.

Dengan banyaknya pengguna layanan SMS, bukan berarti SMS merupakan layanan yang terbaik jika ditinjau dari segi keamanan pesan teks tersebut. Pengamanan data sudah menjadi kebutuhan global dari ancaman serangan data termasuk penyadapan SMS, di indonesia jutaan pelanggan telekomunikasi seluler dipantau serta dimata-matai oleh pihak asing dengan teknik tertentu [3]. Maka dari itu, layanan SMS memerlukan sebuah fitur yang dapat meningkatkan keamanan pesan, salah satunya adalah dengan cara dienkripsi.

Enkripsi adalah proses mengamankan suatu informasi dengan membuat informasi tersebut tidak dapat dibaca tanpa bantuan pengetahuan dan atau alat khusus. Cara yang digunakan untuk melakukan enkripsi ialah dengan cara melakukan perubahan sebuah kode dari yang bisa dimengerti menjadi sebuah kode yang tidak bisa dimengerti dengan menggunakan kunci dan algoritma tertentu [4], sedangkan untuk dapat merubah data ke bentuk asli dinamakan proses deskripsi. Salah satu kunci yang dapat digunakan adalah algoritma kunci simetris, yaitu kunci yang digunakan untuk proses enkripsi sama dengan kunci yang digunakan untuk proses deskripsi. Contoh dari algoritma simetris adalah *Data Encryption Standart* (DES) dan RC6.

Beberapa penelitian terkait dengan pembuatan karya ilmiah ini salah satunya, penelitian oleh Rudy Hendrayanto [5] yang mengembangkan aplikasi keamanan pesan SMS dengan menggunakan algoritma DES, DES sangat populer dan telah menjadi standar algoritma ekripsi sejak lama. Defni [6] yang mengembangkan sistem keamanan pesan SMS dengan menggunakan algoritma RC6. Pada dua penelitian tersebut, masing-masing penulis menggunakan satu metode untuk proses enkripsi SMS dengan menggunakan metode algoritma DES dan RC6.

Pada penelitian ini penulis mengembangkan dari penelitian sebelumnya dengan cara mengimplementasikan dua algoritma DES dan RC6 untuk proses enkripsi dan deskripsi pesan SMS. Dengan menggabungkan dua algoritma DES dan RC6, penulis berharap bisa meminimalisir kekurangan-kekurangan dua algoritma tersebut. Dengan menggunakan dua algoritma tersebut, proses enkripsi dan deskripsi akan melalui dua tahapan. Pertama pesan asli *(plaintexs)* di enkripsi menggunakan algoritma DES dengan kunci *(key)* tertentu dan menghasilkan pesan sandi *(ciphertexs)*. Tahapan kedua, *ciphertexs* tadi dijadikan *plaintexs* dan di enkripsikan menggunakan algoritma RC6 dengan *key* yang sama dan menghasilkan *ciphertexs*.

2. TINJAUAN PUSTAKA

2.1 Android

Android adalah sistem operasi berbasis Linux yang digunakan untuk telepon seluler (mobile) seperti telepon pintar (smartphone) dan komputer tablet (PDA). Android menyediakan platform terbuka bagi para pengembang peranti

bergerak. Android kini telah menjelma menjadi sistem operasi mobile terpopuler di dunia.

2.2 SMS(*Short Message Service*)

SMS adalah salah satu fasilitas dari teknologi GSM yang memungkinkan mengirim dan menerima pesan-pesan singkat berupa text dengan kapasitas maksimal 160 karakter dari Mobile Station (MS). Kapasitas maksimal ini tergantung dari alphabet yang digunakan, untuk alphabet Latin maksimal 160 karakter, dan untuk non-Latin misalnya alphabet Arab atau China maksimal 70 karakter [7].

2.3 Kriptografi

Kriptografi berasal dari bahasa Yunani, menurut bahasa dibagi menjadi dua, yaitu kripto dan graphia, kripto berarti *secret* (rahasia) dan *graphia* berarti writing (tulisan). Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ketempat lain. Orang yang melakukan ini disebut "*Cryptographer*"[9]. Kriptografi merupakan bagian dari suatu cabang ilmu matematika yang disebut *Cryptology*. Kriptografi bertujuan menjaga kerahasiaan informasi yang terkandung dalam data sehingga informasi tersebut tidak dapat diketahui oleh pihak yang tidak sah.

Dalam menjaga kerahasiaan data, kriptografi mentransformasikan data jelas (*plaintext*) ke dalam bentuk data sandi (*ciphertext*) yang tidak dapat dikenali. Ciphertext inilah yang kemudian dikirimkan oleh pengirim (*sender*) kepada penerima (*receiver*). Setelah sampai di penerima, *ciphertext* tersebut ditranformasikan kembali ke dalam bentuk *plaintext* agar dapat dikenali.

2.4 Algoritma DES

Data Encrytion Standar (*DES*) adalah algoritma cipher blok yang popular karena pernah dijadikan standar algoritma enkripsi kunci-simetri. Sebenarnya *DES* adalah nama standar enkripsi simetri, nama algoritma enkripsinya sendiri adalah *DEA* (*Data Encryption Algorithm*),namun nama *DES* lebih popular dari pada *DEA*.

Algoritma Deskripsi *DES* dikembangkan di IBM dibawah kepemimpinan W.L. Tuchman pada Feistel. Algoritma ini telah disetujuin oleh *National Bureau of standar* (*NBS*) Amerika Serikat. *DES* termasuk ke dalam *system* kriptografi simetri dan tergolong jenis *cipher* blok. *DES* peroperasi pada ukuran blok 64 bit. *DES* mengenkripsikan 64 bit plainteks menjadi 64 bit chipherteks dengan menggunkan 56 kunci internal atau upa-kunci. Kunci internal di bangkitkan dari kunci eksternal yang panjangnya 64 bit [10].

2.5 Algoritma RC6

Algoritma RC6 adalah suatu algoritma kriptografi block cipher yang dirancang oleh Ronald L. Rivest, Matt J.B. Robshaw, Ray Sidney, dan Yuqin Lisa Yin dari RSA Laboratories. Algoritma ini pada mulanya dirancang untuk menjadi AES (Advance Encryption Standard). Algoritma RC6 ini berhasil menjadi finalis dan menjadi kandidat kuat untuk menjadi AES walaupun pada akhirnya algoritma ini tidak terpilih menjadi AES melainkan algoritma rinjdael. Versi 1.1 dari RC6 mulai dipublikasikan pada tahun 1998. Dasar desain dari algoritma RC6 ini didasarkan pada pendahulunya yaitu algoritma RC5 [11].

Algoritma RC6 dilengkapi dengan beberapa parameter, sehingga dituliskan sebagai RC6-w/r/b. Parameter w merupakan ukuran kata dalam satuan bit, parameter merupakan bilangan bukan negatif yang menunjukan banyaknya iterasi selama proses enkripsi dan parameter b menunjukan ukuran kunci enkripsi dalam byte. Setelah algoritma ini masuk dalam kandidat AES, maka

ditetapkan bahwa nilai w = 32, r=20 dan b bervariasi antara 16, 24 dan 32 byte.

3. METODE

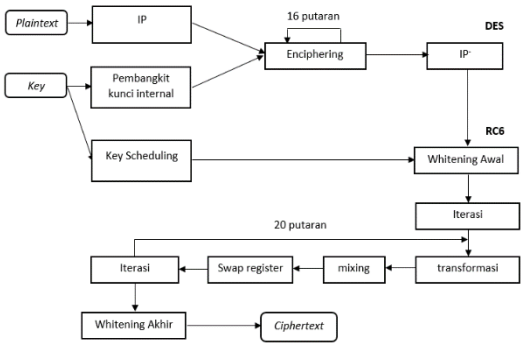
Dalam melakukan penelitian diperlukan metode penelitian, dalam metode tersebut dilakukan beberapa tahapan untuk mendapatkan hasil yang baik. Sehingga penelitian ini dapat berjalan dengan lancar.

3.1 Pengumpulan Data

Proses pengumpulan data yaitu proses atau cara yang dilakukan oleh penulis untuk mendapatkan data-data yang dibutuhkan. Peneliti menggunakan data berupa pesan SMS yang masuk dan keluar dari *smartphone* penulis .

3.2 Enkripsi

Enkripsi berguna sebagai proses untuk mengubah pesan asli menjadi pesan yang tersandikan. Enkripsi ini menggunakan metode DES dan RC6.



Gambar 1 Enkripsi

3.2.1 Pembangkit Kunci Internal
digunakan untuk mendekripsikan pesan *plaintext* dan mendekripsikan *ciphertext.* Kunci akan dipermutasikan dengan tabel PC-1 (*permutation Compression*) sehingga membuat 1 bit masing-masing blok kunci dari 64 bit menjadi 56 bit.

3.2.2 Initial Permutation (IP)
Pada tahap *initial permutation*, pesan asli dipermutasikan menggunakan tabel permutasi IP sehingga menghasilkan *L0* dan *R0* yang berguna untuk proses enciphering.

3.2.3 Enciphering
Pada langkah ini kita akan meng-ekspansi data Ri-1 32 bit menjadi Ri 48 bit menggunakan tabel Ekspansi (Tabel 2.5) sebanyak 16 kali putaran. Setiap putaran merupakan jaringan fiestel.

3.2.4 Inverse Initial Permutation (IP^{-})
Permutasi terakhir dilakukan setelah 16 kali putaran terhadap gabungan blok kiri dan blok kanan. Proses permutasi menggunakan matriks permutasi awal balikan (*inverse initial permutation* atau IP^{-1}) yang akhirnya menghasilkan *ciphertext* dari algoritma DES yang nantinya digunakan sebagai *plaintext* untuk enkripsi RC6.

3.2.5 Key Scheduling
Key scheduling adalah tahapan yang dilakukan sebelum melakukan proses enkripsi dan dekripsi RC6. Algoritma *key scheduling* RC6 terdiri dari 3 tahap utama, yaitu:

a. Penempatan kunci yang di-*input* pengguna kedalam *array L*
b. Inisialisasi kunci yang ditempatkan dalam *array* S
c. Kombinasi *L* dan *S*

3.2.6 Whitening Awal
Pada tahap *whitening awal*, langkah pertama yang dilakukan adalah menambahkan kunci ronde pertama dengan register *B* dan kunci ronde kedua dengan register *D*. Tujuan *whitening awal* adalah untuk menyamarkan input sebelum *iterasi* pertama.

3.2.7 Iterasi
Pada tahapan *iterasi* dilakukan sebanyak 20 iterasi. dan setiap iterasi terdiri dari tiga tiga proses, yaitu:

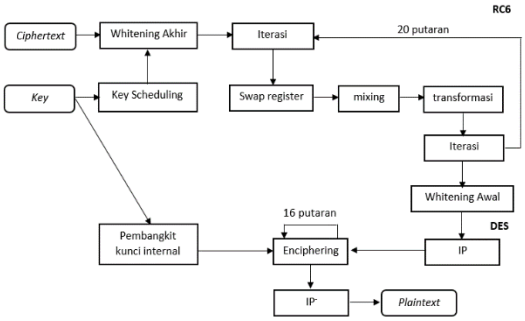
a. Transformasi
b. Mixing
c. Swap register

3.2.8 Whitening Akhir
Pada tahap *whitening akhir*, kunci ronde ke 42 ditambahkan dengan register *A* dan kunci ronde ke 43 dengan register *C*. *Whitening akhir* bertujuan untuk menyamarkan *output* pada iterasi

terakhir. Sehingga menghasilkan *ciphertext* terakhir.

3.3 Dekripsi

Pada proses ini berfungsi untuk mengubah pesan yang tersandikan(*ciphertext*) menjadi pesan alsi(*plaintext*). Proses dekripsi menggunakan metode RC6 dan DES.



Gambar 2 Dekripsi

3.3.1 Key Scheduling

Key scheduling yang dipakai untuk proses dekripsi sama dengan yang dipakai pada saat enkripsi.

3.3.2 Whitening Akhir

Yakni mengembalikan proses *whitening akhir* pada proses enkrpsi dengan mengurangi register *A* dan *C* dengan kunci yang bersesuaian (sama dengan yang dipakai pada saat proses *whitening akhir* enkripsi)

3.3.3 Iterasi

Iterasi sama dengan proses enkripsi, tapi dilakukan dengan urutan pertama yaitu *swap register*, yaitu mengembalikan *proses swap register* yang dilakukan pada saat enkripsi dari *(B,C,D,A)* kembali menjadi *(A,B,C,D).*

3.3.4 Whitening Awal

Whitening Awal adalah langkah terakhir pada proses dekripsi algoritma RC6. Mengembalikan proses *whitening Awal* pada enkripsi dengan mengurangi register *B* dan *D* dengan kunci yang bersesuaian (sama yang dipakai saat proses *whitening Awal* enkripsi).

3.3.5 Pembangkit Kunci Internal

Proses pembangkit kunci internal pada dekripsi sama dengan pada proses enkripsi.

3.3.6 Initial Permutation (IP)

Pada tahap *initial permutation*, pesan sandi (*ciphertext*) dipermutasi dengan menggunakan tabel permutasi IP.

3.3.7 Enciphering

Proses *enciphering* dilakukan sebanyak 16 putaran. Proses *encipering* pada dekripsi sama dengan proses enkripsi.

3.3.8 Inverse Initial Permutation (IP^{-})

Pada proses *inverse initial permutation* dekripsi, sama dengan proses enkripsi. Dipermutasi dengan tabel IP^{-} sehingga menghasilkan *plaintext*.

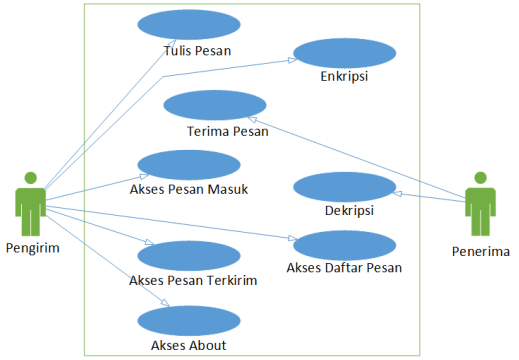
4. HASIL DAN PEMBAHASAN

4.1 Gambaran Umum Sistem

Sistem yang dibangun dalam penelitian ini adalah enkripsi sms pada smartphone berbasis android dengan menggunakan metode DES dan RC6. Gabungan kedua metode tersebut digunakan sebagai algoritma enkripsi dan dekripsi pesan, sehingga dapat meningkatkan keamanan pesan SMS.

4.2 Perancangan Sistem

Rancangan sistem untuk penerapan algoritma DES dan RC6 pada aplikasi enkripsi SMS berbasis android dibuat dengan pemodelan UML yang meliputi *use case diagram*, *activity diagram*, *class diagram* dan *sequence diagram*.

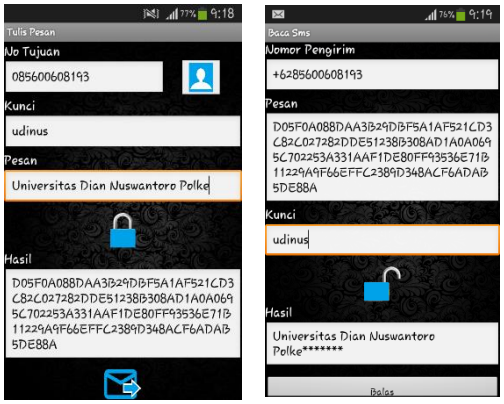


Gambar 3 *Use Case Diagram*

5. IMPLEMENTASI PERANGKAT KERAS

5.1 Hasil Tampilan

Gambar 4 menunjukkan tampilan form tulis pesan dan form baca pesan.



Gambar 4 Halaman Tulis Pesan dan Baca Pesan

5.2 Pengujian

5.2.1 Pengujian Validasi

Pengujian Validasi dilakukan untuk mengetahui bahwa aplikasi dapat memenuhi kebutuhan fungsional untuk melakukan enkripsi *plaintext* menjadi *ciphertext* dan mendekripsikan *ciphertext* menjadi *plaintext* kembali. Pesan yang di ujikan adalah data pesan yang dikumpulkan penulis. Sedangkan, Kunci yang digunakan pada semua pesan yang akan diujikan adalah sama, yaitu "udinus". Pada proses pengiriman ke nomer tujuan dilakukan dengan bantuan provider agar sampai ke tempat nomer tujuan. Daftar pesan yang dienkripsi ditunjukkan tabel sebagai berikut :

Tabel 1 Pengujian Validasi

No	Pesan Sms	Key	Enkripsi	dekripsi
1	Setelah dhuhur	udinus	5E6C3650BDB2CDE606174CCE149B518E941FFEFAC997E10C36A0AECAF6B2DD05	Setelah dhuhur
2	Dikampus gedung H	udinus	0FDDD9DB5EC750CB9CB524F65AE26E81B0A2E36EE2B03B523E91DE293F628AEBCA1D6B37F317A8C37031F0EFF2C48E2F	Dikampus gedung H
3	Nanti kita kumpul di gazebo jam 2	udinus	338C3FF590CDD7A293ED5ED8AECEEA38E56977EAAD9F22560BEF361011DF87CDB9A1ED0D17D7310D0203698B9151F5F6D9F25FB543B9DB72EA5A2F0C3403CDCD	Nanti kita kumpul di gazebo jam 2
4	Aku nanti sidang jam 2, datang yaa	udinus	5E373A633FB67BC4E5BC393CD52D3EB0C58C5470452034F997686B8AE3F3544FEB43293AF4F4D4B4B865BC5F8E810DCB98003C87E21EB33834D27B28B6F49112	Aku nanti sidang jam 2, datang yaa
5	Nanti kalo udah selesai tak traktir	udinus	D1B5030D41100E8042A7C66F8091C73A089281D3B1945393E8465A27344F5807AB8E55DC43BF64FF6A767F04EC5E9B3DF6049AC2EF3B189D192E372388BD11F9	Nanti kalo udah selesai tak traktir

5.2.2 Pengujuan Kecepatan Proses

Pengujian kecepatan proses dilakukan untuk mengetahui proses enkripsi dan dekripsi sebagai acuan analisis terhadap kecepatan proses. Pengujian dengan menggunakan dua smartphone android yaitu Samsung ACE 3 dengan Ram 1Gb dan Lenovo A369i dengan Ram 500 Mb.

Tabel 2 Pengujian Kecepatan Proses Enkripsi

Panjang Pesan (karakter)	Panjang kunci (karakter)	Waktu (ms)	Waktu (ms)	Waktu (ms)	Rata-rata (ms)	Hardware
26	6	239	275	221	245	Samsung ACE 3 Ram 1Gb
37	6	322	353	386	353,7	
58	6	406	427	450	427,7	
26	10	266	284	286	278,7	
37	10	372	379	368	373	
58	10	477	451	424	440,6	
26	6	258	317	647	407,3	Lenovo A369 i Ram 500 Mb
37	6	460	452	720	604	
58	6	471	966	1152	863	
26	10	359	464	598	473,7	
37	10	452	808	1050	770	
58	6	529	735	1235	833	

Tabel 3 Pengujian Kecepatan Proses Dekripsi

Panjang Pesan (karakter)	Panjang kunci (karakter)	Waktu (ms)	Waktu (ms)	Waktu (ms)	Rata-rata (ms)	Hardware
26	6	1005	645	689	779,7	Samsung ACE 3 Ram 1Gb
37	6	813	925	626	788	
58	6	904	822	852	859	
26	10	1081	832	630	847	
37	10	781	962	976	885	
58	10	1069	788	963	940	
26	6	524	678	850	684	Lenovo A369 i Ram 500 Mb
37	6	626	680	840	715,3	
58	6	621	648	917	728,7	
26	10	548	594	725	622,3	
37	10	640	957	962	853	
58	10	961	1109	1141	1070	

Berdasarkan pengujian kecepatan proses enkripsi dan dekripsi, didapatkan hasil bahwa Samsung ACE 3 dengan Ram 1 Gb lebih cepat daripada Lenovo A369i dengan Ram 500 Mb.

6. KESIMPULAN DAN SARAN

6.1 Kesimpulan

Berdasarkan eksperimen dengan mengimplementasikan algoritma DES dan RC6, maka dapat disimpulankan bahwa Semakin panjang *plaintext*, *ciphertext* dan *key* maka semakin lama proses enkripsi dan dekripsinya. Dan ukuran Ram smartphone android mempengarusi kecepatan proses enkripsi dan dekripsi.

6.2 Saran

Peneliti memberikan saran untuk pengembangan selanjutnya menggunakan algoritma DES dan RC6 untuk mengenkripsi pesan gambar dan suara.

DAFTAR PUSTAKA

[1] Kompas, "2015, Pengguna mobile Lampaui Jumlah Penduduk Dunia," 4 Juni 2014. [Online]. Available : http://tekno.kompas.com/read/2014/06/04/1025003/2015.Pengguna.Mobile.Lampaui.Jumlah.Penduduk.Dunia. [Diakses pada 5 Februari 2015].

[2] Republik, "Pengguna Smartphone Indonesia Peringkat Lima Dunia," 2 November 2014. [Online] Available : http://trendtek.republika.co.id/berita/trendtek/gadget/14/11/02/neehfh-pengguna-smartphone-indonesia-peringkat-kelima-dunia. [Diakses pada 5 Februari 2015].

[3] Tajuk, "Layanan SMS-Guard Anti Sadap Hadir di Luar Negeri," 15 April 2014. [Online]. Available : http://tajuk.co/news/layanan-sms-guard-anti-sadap-hadir-di-luar-negeri. [Diakses pada 5 Februari 2015].

[4] Busran and P.Mandarani, "Analisa Komputasi Enkripsi Dan Dekripsi Data Gambar, Teks Dan Audio Dengan Menggunakan Algoritma Rc4 Berbasis Visual Basic 6.0," *ISSN Jurnal Teknologi Informasi & Pendidikan,* vol.5 no.1, pp. 2086-4981, Maret 2012.

[5] R. Hendrayanto and A.R. Nilawati, "Program Aplikasi Enkripsi dan Dekripsi Sms pada Ponsel Berbasis Android dengan Algoritma Des," *ISSN Prosiding Kommit 2012*, vol.7, pp. 2302-3740, September 2012.

[6] Defni and I. Rahmayun, "Enkripsi Sms (Short Message Service) pada Telepon Selular Berbasis Android dengan Metode Rc6," *ISSN Jurnal Momentum,* vol.16 no 1, pp. 1693-752x, Februari 2014.

[7] A. Dwinanto, "Penerapan Algoritma AES (Advance Encryption Standard) 128 dan Vigenere Cipher pada Aplikasi Enkripsi Pesan Singkat Berbasis Android," Skripsi Sistem Informatika Universitas Negeri Gorontalo, Gorontalo, 2014.

[8] A. Dwinanto, "Penerapan Algoritma AES (Advance Encryption Standard) 128 dan Vigenere Cipher pada Aplikasi Enkripsi Pesan Singkat Berbasis Android," Skripsi Sistem Informatika Universitas Negeri Gorontalo, Gorontalo, 2014.

[9] T. R. Rahayu, Yakub, and I. Limiady, ”Aplikasi Enkripsi Pesan Teks (SMS) pada Perangkat *Handphone* dengan Algoritma *Caesar Cipher*,” *ISSN Sentika 2012*, pp. 2089-9815, Maret 2012.

[10] Febriansyah, “Analisis dan Perancangan Keamanan Data menggunakan Algoritma Kriptografi *Des (Data Encyption Standard)*,” Skripsi Fakultas Ilmu Komputer Universitas Bina Darma, Palembang, 2012.

[11] I. Wibisono, “Aplikasi Penerapan Algoritma Rc6 Pada Gambar Berbasis Android,” Skripsi Fakultas Sains Dan Teknologi Universitas Islam Negeri Sultan Syarif Kasim Riau, Pekanbaru 2014.

[12] Etunas, “Pengembangan Software dengan Metode Waterfall,” 24 Maret 2013. [Online] Available : http://www.etunas.com/web/pengembangan-software-dengan-metode-waterfall.htm. [Diakses pada 20 Juni 2015].