IMPLEMENTASI ALGORITMA DES (DATA ENCRYPTION STANDARD) PADA *ENKRIPSI* DAN *DESKRIPSI* SMS BERBASIS *ANDROID*

Deny Adhar

Universitas Potensi Utama
Jl. Kol. Yos Sudarso Km 6.5 No 3A Tanjung Mulia Medan, Sumatera Utara
E-mail :adhar_7@yahoo.com

ABSTRACT

The development of technology makes the birth of a tool that is the forerunner to the formation of Short Messaging Service (SMS), namely pagers. However, with the community's need to send messages quickly, accurately and safely make technology experts create a device that is a cellphone. Cellphone or mobile was first created already equipped with SMS feature. When a message or data becomes important and is privacy, it is necessary to protect the data. Therefore experts created an algorithm method to secure data. This method is called the encryption and decryption method to secure highly confidential messages or information from irresponsible and unauthorized people. There are various kinds of encryption algorithms with each characteristic that can be used, one of which is the DES (Data Enryption Standard) algorithm. DES is a symmetric encryption algorithm, where the process of encrypting and decrypting messages uses the same key. So even though a cryptografe understands the algorithm used to encode the message, but if you don't know the key used, it won't be able to decrypt the message so that the SMS message is really safe.

Keywords: SMS, Cryptography, Enkripsi, Dekripsi, DES Algorithm

ABSTRAK

Perkembangan teknologi membuat lahirnya sebuah alat yang merupakan cikal bakal terbentuknya *Short Messaging Service* (SMS) yaitu *pager*. Namun, dengan kebutuhan masyarakat akan pengiriman pesan dengan cepat, akurat dan aman membuat para ahli teknologi menciptakan sebuah alat yaitu ponsel. Ponsel atau mobile pertama kali diciptakan sudah dilengkapi dengan fitur SMS. Saat sebuah pesan atau data menjadi penting dan bersifat privasi maka perlu diadakan perlindungan terhadap data tersebut. Oleh karena itu para pakar menciptakan sebuah metode algoritma untuk mengamankan data. Metode ini disebut metode enkripsi dan dekripsi untuk mengamankan pesan atau informasi yang sangat rahasia dari orang-orang yang tidak bertanggungjawab dan tidak berkepentingan. Ada berbagai macam algoritma enkripsi dengan karakteristik masing-masing yang bisa digunakan salah satunya adalah algoritma DES (Data Enryption Standard). DES merupakan algoritma penyandian simetris, dimana untuk proses enkripsi dan dekripsi pesan menggunakan kunci yang sama. Jadi walaupun seorang kriptografe rmengerti dengan baik algoritma yang digunakan untuk menyandikan pesan tersebut, tapi kalau tidak tahu kunci yang digunakan, maka tidak akan dapat mendekripsi pesan tersebut sehingga pesan sms benar - benar aman.

Kata kunci: SMS,Kriptografi, Enkripsi,Dekripsi,Algoritma DES

I. PENDAHULUAN

Kebutuhan masyarakat untuk berkomunikasi secara tidak langsung membuat terciptanya metode pengiriman pesan pada zaman tradisional yaitu dengan surat. Tetapi dengan surat, pengiriman pesan dapat sampai dalam waktu yang lama. Namun, dengan kebutuhan masyarakat akan pengiriman pesan dengan cepat, akurat dan aman membuat para ahli teknologi menciptakan sebuah alat yaitu ponsel. Ponsel atau mobile pertama kali diciptakan sudah dilengkapi dengan fitur SMS. Teknologi SMS dikembangkan pertama kali oleh Friedhelm Hillebrand, Bernard

Ghillebaert, dan Oculy. Kemudian munculah organisasi-organisasi yang menciptakan standar teknologi SMS sehingga membuat teknologi SMS bisa digunakan di seluruh dunia. Dikembangkannya standarisasi SMS dimulai tahun 1985 oleh upaya kerja sama antara Perancis dan Jerman. Saat sebuah pesan atau data menjadi penting dan bersifat privasi maka perlu diadakan perlindungan terhadap data tersebut. Oleh karena itu para pakar menciptakan sebuah metode algoritma untuk mengamankan data. Metode ini disebut metode enkripsi dan dekripsi (Rudy Hendrayanto;2012). Dengan adanya kemungkinan penyadapan data, maka aspek keamanan dalam pertukaran informasi menjadi sangat penting karena suatu komunikasi data jarak jauh belum tentu memiliki jalur transmisi yang aman dari penyadapan sehingga keamanan informasi menjadi bagian penting dalam dunia informasi itu sendiri. Saat ini perlindungan informasi menjadi lebih perlu diperhatikan. Sangat sulit untuk mengamankan pesan atau informasi yang sangat rahasia dari orang-orang yang tidak bertanggungjawab dan tidak berkepentingan. Ada berbagai macam algoritma enkripsi dengan karakteristik masing-masing yang bisa digunakan salah satunya adalah algoritma DES. DES (Data Enryption Standard) merupakan algoritma enkripsi yang paling banyak dipakai dunia, yang diadopsi oleh NIST (National Institute of Standards and Technology) sebagai standar pengolahan informasi federal A.

2. METODOLOGI

Dari penelitian yang dilakukan oleh Andi Riski Alvianto dan Darmaji dari Institut Teknologi Sepuluh Nopemberdengan judul "Pengaman Pengiriman Pesan Via SMS dengan Algoritma RSA Berbasis Android" dan penelitian yang dilakukan oleh Nina Anindyawati dan Nina Anindyawati dari Unversitas Sebelas Maret dengan judul "Pembangunan Aplikasi Penyembunyian Pesan Menggunakan Metode End Of File (EOF) ke dalam Citra Digital Terhadap Pesan yang Terenkripsi Dengan Algoritma RSA" perbandingannya dapat dilihat pada tabel I.1 dibawah ini :

Tabel I.1 Perbandingan Sistem Lama dan Yang Akan Dirancang

No	Jenis Luaran	Indikator Capaian
1	ISSN :2337-3520 (2301-928X Print)	JURNAL SAINS DAN SENI ITS Vol. 4, No.1, (2015)
Penelitian pertama : Pengaman Pengiriman Pesan Via SMS dengan Algoritma RSA Berbasis Android		
1.	Target	Merancang perangkat lunak pengamanan Pesan Via SMS
2.	Solusi	Solusi didapat dengan metode RSA
3.	Bahasa pemrograman	*java*
Penelitian kedua : Pembangunan Aplikasi Penyembunyian Pesan Menggunakan Metode *End Of File* (EOF) ke dalam Citra Digital Terhadap Pesan yang Terenkripsi Dengan Algoritma RSA		
2	ISSN : 2301–7201	JURNAL ITSMART Vol 1. No 1. Juni 2012
1.	Target	Merancang aplikasi penggabungan steganografi dan enkripsi data pesan
2.	Solusi	Solusi didapat dengan metode EOF dan RSA
3.	Bahasa pemrograman	*Visual Basic* 6.0
Penelitian yang akan dibuat : **Perancangan Aplikasi *Enkripsi* Dan *Deskripsi* SMS Menggunakan Metode DES Berbasis *Android***		
1.	Target	aplikasi keamanan SMS
2.	Solusi	Solusi didapat

		dengan metode Des
3.	Bahasa pemrograman	*Java*

2.1 Pengertian Kriptografi

Kriptografi adalah ilmu yang mempelajari teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, otentikasi entitas, dan otentikasi asal data [2]. Kriptografi bertujuan agar informasi yang bersifat rahasia dan dikirim melalui suatu jaringan, seperti LAN atau internet, tidak dapat diketahui dan dimanfaatkan oleh orang lain atau pihak yang tidak berkepentingan. (Ashari Arief;46: 2016)

2.2 SMS (Short Message Service)

SMS merupakan sebuah layanan yang bersifat nonereal time dimana sebuah short message dapat di submit ke suatu tujuan, tidak peduli apakah tujuan tersebut aktif atau tidak. Bila dideteksi bahwa tujuan tidak aktif, maka sistem akan menunda pengiriman ke tujuan hingga tujuan aktif kembali. Pada dasarnya sistem SMS akan menjamin delivery dari suatu short message hingga sampai tujuan. Kegagalan pengiriman yang bersifat sementara seperti tujuan tidak aktif akan selalu teridentifikasi sehingga pengiriman ulang short message akan selalu dilakukan kecuali apabila diberlakukuan aturan bahwa short message yang telah melampaui batas waktu tertentu harus dihapus dan dinyatakan gagal kirim. Layanan SMS dibangun dari berbagai entitas yang saling terkait dan mempunyai fungsi dan tugas masing-masing. Tidak ada satupun dalam sistem SMS yang dapat bekerja secara parsial. Entitas dalam jaringan SMS ini disebut juga elemen SMS(Raisul Azhar;106;2016).

2.3 DES (Data Encryption Standart)

Penggunaan data sandi yang paling banyak didasarkan pada standard-standard data sandi (DES) yang diambil pada tahun 1977 oleh Standard-Standard Nasional Bureau, yang sekarang Institut Nasional Standard dan Tekhnologi (NIST), sebagai Standard Proses Informasi Umum. Untuk DES, data disandikan ke dalam 64 balok bit menggunakan 56 bit kunci. Transformasi algoritma 64 bitinput ke dalam satu serilangkah-langkah ke dalam 64 bitoutput. Langkah yang sama dengan kunci yang sama, digunakan untuk cadangan persandian. (Dadang Priyanto; 2016;69).

2.4 Android

Android adalah aplikasi sistem operasi untuk telepon seluler yang berbasis Linux.Android menyediakan platform terbuka bagi para pengembang untuk menciptakan aplikasi mereka sendiri untuk digunakan oleh bermacam piranti bergerak.

Berikut penulis membahas kelebihan Android yaitu:

a. Switching dan multitasking yang lebih baik Android sangat mendukung multitasking aplikasi, kini hal tersebut kembali ditingkatkan. Dalam Honeycomb penggguna dapat dengan mudah berpindah aplikasi hanya dengan menyentuh sebuah icon pada systembar.

b. Kapasitas yang lebih baik untuk beragam Widgetkapabilitas terhadap beragam Widget dijanjikan bakal makin memanjakan para penggunanya. Contohnya Widget untukGmail yang dipamerkan Google, pengguna tidak perlu membuka aplikasi Gmail untuk melihat isi di dalamnya.

c. Peningkatan kemampuan copypastebeberapa seri Android terdahulu memang sudah bisa melakukan copypaste, namun beberapa pengguna masalah pemilihan teks yang agak sulit. Kini hal tersebut coba diselesaikan, selain copypasteGoogle juga. (Sulihati;2016;19)

3. HASIL DAN PEMBAHASAN

Langkah-langkah pembangkitan kunci DES adalah sebagai berikut:

Misal plainteks = Ajie2018
Kunci 1 = 3C 63 47 9B 85 5A 4E 2F
Kunci 2 = A9 19 64 48 22 C5 9F 66
Ubah plainteks kedalam biner
A =65=01010010
j =106=10010111
i =105=01101000
e =101=01100001
2 =50= 10010110
0 =48= 01101001
1=49= 01010010
8 =56= 01001000

1. Masukkan plainteks yang panjangnya 64 bit atau 8 karakter kedalam Inisial Permutasi (IP).

IP=11101101 01010011 00010010 00101010 00010010 00101100 10100100 01010011

Pecah IP menjadi 2 bagian L_oR_o sehingga menghasilkan output
L_o=11101101 01010011 00010010 00101010
R_o=00010010 00101100 10100100 01010011

2. Setelah dipecah menjadi 2 bagian maka kunci 1 akan diubah menjadi biner dan kemudian di initial Permutasi (IP) .
Kunci 1 = 3C 63 47 9B 85 5A 4E 2F

3C =60 =00111100	→	01100110
63 =99 =01100011	→	00101001
47 =71 =01000111	→	11010101
9B =155=10011011	→	10011110
85 =133=10000101	→	00011000
5A =90 =01011010	→	10000011
4E =78 =01001110	→	11101001
2F =47 =00101111	→	11101110

Setelah Kunci 1 sudah di permutasi awal maka selanjutnya dengan menggunakan matriks permutation PC-1 sehingga panjang kunci yang 64 bit dikompresi menjadi 56 bit.
Maka hasil PC-1= 0001100 0011001 1010000 0110010 1110111 0110101 0111101 0011001
Hasil PC-1 dibagi 2 bagian menjadi C_oD_o sebagai berikut
C_o=0001100 0011001 1010000 0110010
D_o=1110111 0110101 0111101 0011001

3. Cara permutasi sama dengan permutasi plainteks 56 bit dari 64 bit kunci eksternal. Setelah didapat hasil dari permutasi maka hasil dibagi dua yaitu bagian kiri dan kanan (C_oD_o) masing-masing 28 bit. Kemudia digeser ke kiri (*Left Shift)* sepanjang satu atau dua bit tergantung pada setiap putaran yang ditentukan. Operasi pergeseran bernilai *Wrapping* atau *Round- Shift.*

C_1=0011000 0110011 0100000 1100100
D_1=1101110 1101010 1111010 0110011

C_2=0110000 1100110 1000001 1001000
D_2=1011101 1010101 1110100 1100111

C_3=1000011 0011010 0000110 0100001
D_3=1110110 1010111 1010011 0011110

C_4=0001100 1101000 0011001 0000110
D_4=1011010 1011110 1001100 1111011

C_5=0110011 0100000 1100100 0011000
D_5=1101010 1111010 0110011 1101110

C_6=1001101 0000011 0010000 1100001
D_6=0101011 1101001 1001111 0111011

C_7=0110100 0001100 1000011 0000110
D_7=0101111 0100110 0111101 1101101

C_8=1010000 0110010 0001100 0011001
D_8=0111101 0011001 1110111 0110101

C_9=0100000 1100100 0011000 0110011
D_9=1111010 0110011 1101110 1101010

C_{10}=0000011 0010000 1100001 1001101
D_{10}=1101001 1001111 0111011 0101011

C_{11} =0001100 1000011 0000110 0110100
D_{11}=0100110 0111101 1101101 0101111

C_{12}=0110010 0001100 0011001 1010000
D_{12}=0011001 1110111 0110101 0111101

C_{13}=1001000 0110000 1100110 1000001
D_{13}=1100111 1011101 1010101 1110100

C_{14}=0100001 1000011 0011010 0000110
D_{14}=0011110 1110110 1010111 1010011

C_{15}=0000110 0001100 1101000 0011001
D_{15}=1111011 1011010 1011110 1001100

C_{16}=0001100 0011001 1010000 0110010
D_{16}=1110111 0110101 0111101 0011001

$C_{16}D_{16}$ gabung kembali menjadi C_iD_i=0001100 0011001 1010000 0110010 1110111 0110101 0111101 0011001

4. Pada langkah ini, akan dilakukan ekspansi data R_{i-1} 32 bit menjadi R_i 48 bit sebanyak 16 kali putaran dengan nilai perputaran 1<=i<=16 menggunakan tabel Ekspansi (E). Tahap ini merupakan perluasan dari invers permutasi yang terdiri dari 48 bit.

Hasil E (R_{i-1}) kemudian di XOR dengan K_i dan menghasilkan Vektor Matriks A_i. Pada tahap sebelumnya telah diketahui L_oR_o.
L_o=11101101 01010011 00010010 00101010
R_o=00010010 00101100 10100100 01010011
Berikut hasil outputnya:
Iterasi 1
E(R_o) =100010 100100 000101 011001 010100 001000 001010 100110

K1 =100000 100001 000110 100010 110001 101111 101110 100111

——————————————————XOR

A1 =000010 000101 000011 111011 100101 100111 100100 000001

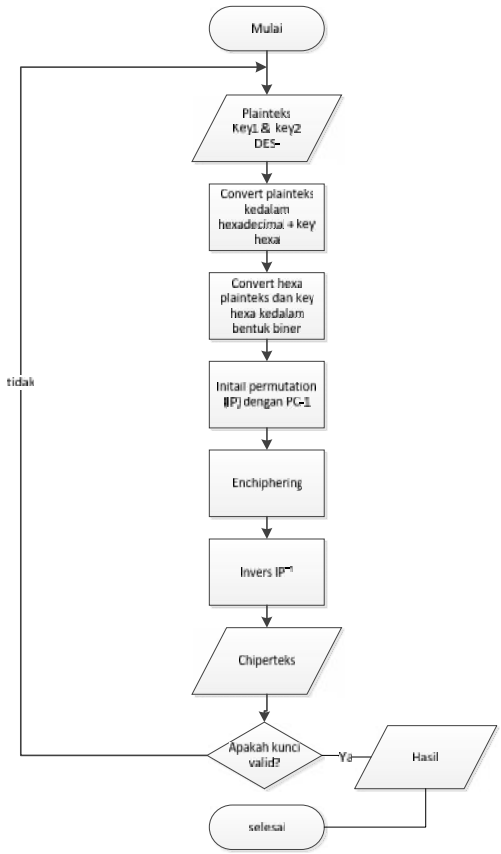
5. Langkah terakhir adalah menggabungkan R_{16} dengan L_{16} kemudian dipermutasikan untuk terakhir kalinya dengan tabel Invers Initial Permutasi (IP^{-1}).

Tabel 1 Tabel (IP^{-1})

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

Hasil permutasinya adalah sebagai berikut:
IP^{-1}= 01000010 00111101 10001100 00110110 11010010 10110010 11111111 11000011
ubah biner ke hexa maka chipertext = 42 3D 8C 36 D2 B2 FF C3

proses kerja implementasi Algoritma DES pada enkripsi dan dekripsi sms ini dapat digambarkan melalui sebuah flowchart berikut :

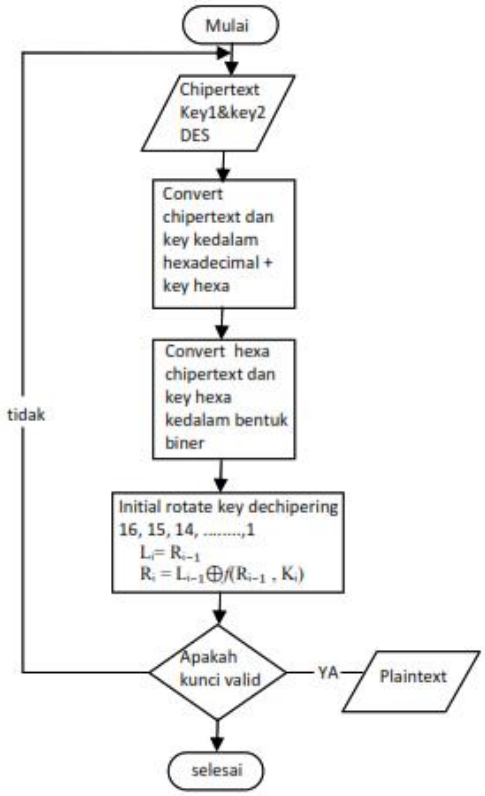


Gambar 1. *Flowchart* Enkripsi SMS

Proses kerja *Flowchart* enkripsi SMS sebagai berikut:

1. Mulai
2. Tentukan pesan asli dan kunci 1, dan kunci 2
3. Convert plainteks ke dalam bentuk hexadecimal dan key hexadecimal
4. Convert hexadecimal plainteks dan key hexadecimal dalam bentuk biner
5. Lakukan Inital Permutation (IP) dengan Permutation Kompresi PC-1
6. Proses *Enchiphering* sebanyak 16 putaran terhadap blok plainteks yang dilakukan setelah permutasi awal.
7. Lakukan Invers Inital Permutation (IP^{-1})
8. Cipherteks
9. Jika kunci valid maka akan muncul hasil dan jika tidak akan di ulang menginput plainteks dan kunci 1 sampai dengan kunci 2 DES
10. Jika semua tahap berjalan dengan lancar maka akan mendapatkan hasil enkripsi yang diinginkan.
11. Selesai

Proses kerja dekrispsi dapat dilihat pada gambar berikut :



Gambar 2. *Flowchart* Dekripsi SMS

Proses kerja *Flowchart* dekripsi SMS sebagai berikut:

1. DES menggunakan algoritma yang sama untuk proses dekripsi.
2. Pada proses dekripsi urutan kunci yag digunakan adalah K_{16}, K_{15}, K_{14}, K_{13},....., K_1.
3. Untuk tiap putaran 16, 15, 14, ...,1, keluaran pada setiap putaran *deciphering* adalah :

$$L_i = R_{i-1}$$
$$R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$$

3.1. Hasil Implementasi

tampilan hasil dari implementasi algoritma DES pada enkripsi dan dekripsi SMS Berbasis *Android* dapat dilihat pada halaman tampilan menu utama berikut

Gambar 3. **Tampilan halaman utama**

dengan menekan menu tulis pesan kita akan melakukan enkripsi pesan sms seperti terlihat pada gambar berikut

Gambar 4. **Tampilan hasil enkripsi pesan SMS**

Pada tampilan tulis pesan disini digunakan untuk pengguna yang melakukan pengiriman pesan .

Langkah penggunaan :

1. Masukkan nomor yang dikirim
2. Masukkan isi pesan
3. Masukkan kunci, kunci ini berguna untuk proses enkripsi
4. Klik gambar gembok
5. Lalu akan keluar kode berupa angka pada kolom hasil setelah dienkripsi
6. Lalu tekan tombol surat jika ingin mengirim pesan
7. Jika ingin kembali kemenu utama tekan tombol cancel

Pesan SMS yang telah di enkrisi kemudian dikirim ke no tujuan, dan si penerima SMS

bisa mendekripsikan pesan melalui menu baca pesan seperti ter;ihat pada gambar berikut

Gambar 5. Tampilan hasil dekripsi pesan SMS

4. KESIMPULAN

Setelah dilakukan analisa dan implementasi pembahasan maka penelitian ini menyimpulkan beberapan yaitu :

1. Implementasi algoritma DES dapat digunakan untuk mengirim pesan SMS yang sifatnya rahasia dengan menekan tombol enkripsi terlebih dahulu sebelum mengirim pesan SMS.
2. DES merupakan algoritma penyandian simetris, dimana untuk proses enkripsi dan dekripsi pesan menggunakan kunci yang sama. Jadi, walaupun seorang criptanalis rmengerti dengan baik algoritma yang digunakan untuk menyandikan pesan tersebut, tapi kalau tidak tahu kunci yang digunakan, maka tidak akan dapat mendekripsi pesan SMS tersebut.

5. SARAN

Untuk menyempurnakan sistem yang telah dibuat ini diberikan saran :

1. Perlu dilakukan penelitian lebih lanjut untuk pengamanan pesan SMS mengggunakan Algoritma kriptografi yang lain.
2. Diharapkan hasil implementasi algoritma DES pada aplikasi ini nantinya dapat digunakan untuk mengirimkan file gambar yang dapat dienkripsi, dekripsikan dan dapat digunakan pada system operasi lainnya selain android.
3. Untuk pengembangan aplikasi ini, akan lebih efektif dan efiesien dibuat *auto refresh* untuk mengetahui pesan-pesan yang baru masuk.
4. Sistem ini diperlukan pengembangan lebih lanjut yaitu memperbaiki tampilan desain *interface*.

DAFTAR PUSTAKA

[1] Didik Prasetyo, 2006. Keamanan SQLite Database pada RDBMS, Jakarta, PT. Elex Media Komputindo.

[2] Dony Ariyus 2008, Pengantar Ilmu kriptografi Teori Analisa dan Implementasi, Yogyakarta, ANDI.

[3] Anandia Zelvina, Syahril Efendi, Dedy Arisandi, 2012. Journal Perancangan Aplikasi Pembelajaran Kriptografi Kunci Public Elgamal Untuk Mahasiswa, Medan.

[4] M. Taufiq Tamam, Wakhyu Dwiono, Tri Hartono, 2010. Journal Penerepan Algoritma Kriptografi Elgamal Untuk Pengaman File Citra, Yogyakarta.

[5] Danang Tri Massandy, 2009. Journal Algoritma Elgamal Dalam Pengaman Pesan Rahasia, Bandung.

[6] Mukhammad Ifanto, 2009. Journal Metode Enkripsi Dan Dekripsi Menggunakan Algoritma Elgamal

[7]. SugiartiYuni S.T.M.Kom. 2013 *Analisa Dan Perancangan UML (Unified Modeling Language).* Penerbit Graha Ilmu. Yogyakarta

[8]. Fauzi Achmad dan Maulita Yani , *Analisis Hybrid Cryptosystem Algoritma Elgamal Dan Algoritma Triple Des, 2016*

[9] Sulihati dan Andriyani, Aplikasi Akademik Online Berbasis Mobile Android. 15. Jurnal Sains dan Teknologi Utama, Volume XI, Nomor 1, April 2016.

[10] Priyanto, D., & Azhar, R. (2016). SISTEM APLIKASI UNTUK KEAMANAN DATA DENGAN ALGORITMA 'DES' (Data Encryption Standard). MATRIK : Jurnal Manajemen, Teknik Informatika Dan Rekayasa Komputer, 16(1), 67-76.

[11] Azhar, R., & Kurniawan, K. (2016). APLIKASI KEAMANAN SMS MENGGUNAKAN ALGORITMA RIJNDAEL. MATRIK : Jurnal

Manajemen, Teknik Informatika Dan Rekayasa Komputer, 16(1), 105-112.

[12] Ashari Arief & Ragli Saputra, 2016. Implementasi Kriptografi Kunci Publik denganmAlgoritma RSA-CRT pada Aplikasi Instant Messaging, Scientific Journal of Informatics Vol. 3, No. 1, Mei 2016