ALGORITMA RSA DAN 3DES PADA APLIKASI SMS BERBASIS ANDROID PADA KEPOLISIAN *RESORT* KOTA BANDARA SOEKARNO HATTA

Lavriyan Zagita[1)], **Rizky Tahara Shinta, M.Kom**[2)]
[1]Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur
[1,2]Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260
E-mail : lavriyanzagita@gmail.com[1)], rizky.tahara@gmail.com[2)]

Abstrak

Kepolisian Resort Kota Bandara Soekarno Hatta adalah salah satu kantor kepolisian yang bertanggung jawab atas keamanan pengguna jasa angkutan udara di Bandara Internasional Soekarno Hatta. Dalam melaksanakan salah satu kegiatannya, ada informasi rahasia mengenai kronologis, waktu, tempat terjadinya suatu perkara yang harus diinformasikan oleh anggota melalui fasilitas SMS ke kepala Kepolisian Resort Kota Bandara Soekarno Hatta ataupun sebaliknya. SMS yang dikirim dapat diketahui oleh orang yang mempunyai hak akses ke SMSC ataupun pihak yang melakukan penyadapan, untuk melindungi pertukaran pesan rahasia melalui SMS maka dibuatlah aplikasi dengan menerapkan algoritma kriptografi RSA dan 3DES. Aplikasi ini dibangun dengan bahasa pemrograman berbasis mobile android dengan maksimal 160 karakter pesan yang terenkripsi. Aplikasi ini diharapkan mempunyai manfaat mengamankan dan menjaga kerahasiaan informasi pada Kepolisian Resort Kota Bandara Soekarno Hatta dari terjadinya pencurian dan manipulasi data oleh pihak yang tidak berkepentingan karena data yang sudah dienkripsi dapat didekripsi menjadi data semula tanpa ada perubahan. Berdasarkan hasil uji coba yang dilakukan, penggabungan algoritma RSA dan EDES pada proses enkripsi dan dekripsi untuk pengamanan pengiriman SMS menjadi lebih sulit untuk diketahui oleh pihak yang tidak berhak sehingga informasi dalam pesan terjaga kerahasiaan, integritas data, otentikasi dan nirpenyangkalan.

Kata kunci: SMS, Kriptografi, RSA, 3DES

1. PENDAHULUAN

SMS *(Short Message Service)* merupakan salah satu fasilitas dasar yang disediakan telepon seluler untuk bertukar informasi berupa pesan singkat. Saat menggunakan fasilitas SMS *(Short Message Service)* akan pengguna akan mempertanyakan mengenai keamaan informasi yang dikirim.

Kepolisian *Resort* Kota Bandara Soekarno Hatta yang dipimpin oleh Kepala Kepolisian Resort mempunyai tugas sesuai dengan Undang-Undang yaitu menegakkan hukum, memelihara keamanan dan ketertiban masyarakat, memberikan perlindungan, pengayoman dan pelayanan kepada masyarakat diwilayah hukum Kepolisian *Resort* Kota Bandara Soekarno Hatta. Dalam pelaksanaan tugas sehari-hari Kepala Kepolisian Resort dibantu oleh Kepala Satuan Reserse Kriminal untuk menjalankan tugas kepolisian di bidang penegakkan hukum yang mempunyai tugas menyelenggarakan kegiatan penyelidikan atau penyidikan tindak pidana umum dan khusus, , penyelenggaraan pembinaan, koordinasi serta pengawasan terhadap penyidik pegawai negeri sipil baik dibidang operasional maupun administrasi penyidikan sesuai dengan peraturan perundang-undangan. Untuk menunjang efektifitas dalam hal kecepatan dan ketepatan informasi yang akan dikirim dari Kepala Kepolisian *Resort* Kota Bandara Soekarno Hatta dan diterima oleh anggota maupun sebaliknya melalui fasilitas SMS *(Short Message Service)* diperlukan suatu aplikasi pengamanan pengiriman SMS *(Short Message Service)*, agar informasi rahasia sampai ke pihak yang tepat dan mampu memenuhi aspek keamanan yaitu integritas data, otentikasi, dan nirpenyangkalan sehingga tidak mengganggu pelaksanaan kegiatan pada Kepolisian *Resort* Kota Bandara Soekarno Hatta.

Demi menjaga kerahasiaan informasi dalam pesan singkat tersebut maka dibuatlah aplikasi pengamanan SMS *(Short Message Service)* berbasis *Mobile* Android dengan metode algoritma RSA *(Rivest Shamir Adleman)* dan 3DES *(Triple Data Encryption Standard)* yang akan mengamankan teks SMS *(Short Message Service)* yang bersifat rahasia dengan mengenkripsi teks SMS *(Short Message Service)* agar pesan rahasia tersebut tidak dapat dketahui oleh pihak yang tidak berwenang.

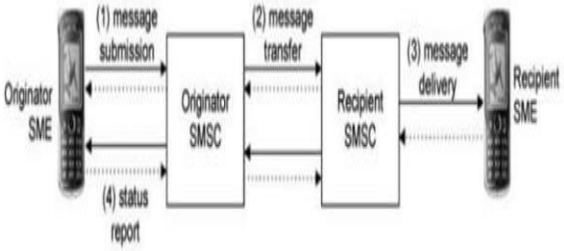
2. LANDASAN TEORI

2.1. SMS *(Short Message Service)*

Layanan SMS *(Short Message Service)*, merupakan salah satu layanan pengiriman pesan. Layanan SMS *(Short Message Service)* menjadikan pengguna dapat mengirimkan pesan berbasis teks dari satu pengguna ke pengguna lain atau dari satu pengguna ke suatu aplikasi. [1]

Panjang isi pesan pada sebuah paket SMS *(Short Message Service)* berisi maksimal 160 karakter, dengan panjang 7 *bit* setiap karakternya. Tidak semua telepon selular yang mendukung karakter sepanjang 8 *bit* (140 karakter) dan 16 bit. [2]

Layanan SMS *(Short Message Service)* awalnya dirancang sebagai bagian dari jaringan GSM *(Global System For Mobile Communication)* namun juga berkembang untuk jaringan CDMA *(Code Division Multiple Access)*. Skema pengiriman SMS *(Short Message Service)* ditunjukkan pada gambar 1 berikut. [3]



Gambar 1. Skema Pengiriman SMS

2.2. RSA

Algoritma RSA adalah enkripsi yang paling umum digunakan dalam algoritma otentikasi. Algoritma RSA melibatkan mengalikan dua bilangan prima besar, setelah kunci telah dibuat, bilangan prima asli tidak lagi penting dan dapat dibuang. Baik kunci publik dan kunci privat dibutuhkan untuk enkripsi dan dekripsi. Pada algoritma RSA, kunci privat tidak pernah perlu dikirim. Kunci privat digunakan untuk mendekripsi teks yang telah dienkripsi dengan kunci publik. [4]

Keamanan algoritma RSA terdapat pada susahnya mendapatkan faktor-faktor bilangan prima untuk memperoleh kunci privat. Semakin besar bilangan maka pemfaktoran menjadi bilangan prima semakin sulit sehingga keamanan algoritma RSA terjamin. Algoritma RSA memiliki besaran seperti berikut [5]:

a. p dan q bilangan prima (rahasia)
b. n = p.q (tidak rahasia)
c. $\Phi(n) = (p-1)(q-1)$ (rahasia)
d. e = kunci enkripsi (tidak rahasia)
e. d = kunci dekripsi (rahasia)
f. m = *plaintext* (rahasia)
g. c = *chipertext* (tidak rahasia)

a. Pembangkitan Kunci RSA

Berikut adalah cara-cara dalam membangkitkan dua kunci algoritma RSA *(Rivest Shamir Adleman)*.

1) Tentukan dua bilangan prima p dan q
2) Hitung n = p*q (dengan ketentuan p≠q. Jika nilai p=q maka n=p2 maka nilai p diperoleh dengan numeric akar pangkat dua dari n)
3) Hitung $\Phi(n) = (p-1) * (q-1)$
4) Ambil kunci public e, yang relatif prima terhadap nilai $\Phi(n)$
5) Hitung kunci private dengan menggunakan persamaan $d= (1+k\ \Phi(n))\ /e$.

b. Algoritma Enkripsi

Langkah melakukan proses enkripsi adalah sebagai berikut :

1) Ambil modulus n dan kunci publik penerima pesan e.
2) Plainteks diubah menjadi blok-blok m1, m2, m3, …… hingga setiap blok menjadi nilai di selang [0,n – 1].
3) Enkripsi setiap blok mi menjadi blok ci dengan persamaan

$$i = mi^{e} \bmod n$$

c. Algoritma Dekripsi

Langkah melakukan proses dekripsi adalah sebagai berikut :

1) Dekripsi setiap blok chiperteks Ci kembali menjadi blok mi dengan persamaan

$$mi = ci^{d} \bmod n$$

2) Blok-blok m1, m2, m3, …… diubah menjadi bentuk huruf dengan kode ASCII.

2.3. 3DES

3DES *(Triple Data Encryption Standard)* adalah salah satu algoritma simetris pada kriptografi yang dilakukan dalam penyandian data melalui proses enkripsi dan dekripsi. Algoritma 3DES merupakan pengembangan dari algoritma DES *(Data Encryption Standard)* dengan perbedaan pada 3DES menggunakan tiga kunci yang saling bebas (K1≠K2≠K3) dan satu kunci yang sama dengan kunci awal (K1≠K2 dan K3=K1) dengan panjang 168 bit sehingga algoritma 3DES lebih aman dari algoritma DES karena panjang kunci yang digunakan. [6]

a. Pemilihan Kunci 3DES

Pertama plainteks dienkripsi menggunakan algoritma DES dengan kunci K1. Selanjutnya hasil enkripsi dilakukan enkripsi atau dekripsi (tergantung cara pengenkripsian yang digunakan) menggunakan algoritma DES dengan kunci K2. Kemudian dilakukan enkripsi kembali menggunakan algoritma DES dengan kunci K3 sehingga menghasilkan *ciphertext* (C).

Ada dua pilihan untuk pemilihan kunci pada algoritma 3DES, yaitu:

1) K1, K2, dan K3 merupakan kunci yang saling bebas
   K1 ≠ K2 ≠ K3 ≠ K1
2) K1 dan K2 adalah kunci yang saling bebas, dan kunci K3 sama dengan kunci K1
   K1 ≠ K2 dan K3 = K1

b. Proses Enkripsi & Dekripsi 3DES

1) Proses Enkripsi 3DES

   Proses enkripsi 3DES dapat dicapai dengan menggunakan tiga kunci :
   Enkripsi:C=EK3(DK2(EK1(P)))

   Penjelasan : enkripsi pesan P dengan kunci K1 lalu dengan kunci K2, kemudian dengan kunci K3 sehingga hasil enkripsi menjadi chipherteks. [6]
2) Proses Dekripsi 3DES

Proses dekripsi 3DES dapat dicapai dengan menggunakan tiga kunci :
Dekripsi:P=DK1(EK2(DK3(C))

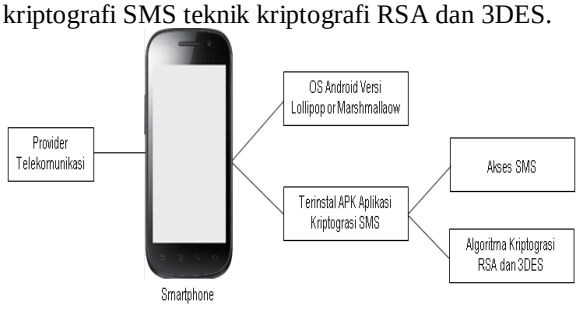
Penjelasan : Kunci K3 digunakan untuk mendekripsi Cipherteks, lalu Cipherteks dienkripsi dengan kunci K2, kemudian didekripsi dengan kunci K1 sehingga menghasilkan pesan semula (P). [6]

3. PERANCANGAN PROGRAM

Program yang akan dibuat dapat menjaga kerahasiaan dari proses pertukaran informasi melalui fitur SMS. Aplikasi tersebut nantinya dapat mengubah sebuah *plaintext* SMS menjadi *chipertext* yang isinya tidak dapat dibaca oleh pihak lain yang tidak berhak sehingga pertukaran infomasi tersebut terjaga kerahasiaannya. Kemudian mengubah kembali seperti semula. Dan dari berbagai mcam jenis algoritma yang ada program ini dikembangkan menggunakan algoritma RSA *(Rivest Shamir Adleman)* dan 3DES (*Triple Data Encryption Standard*) berbasis android dengan menggunakan bahasa pemrograman *Java*. Dengan adanya aplikasi ini diharapkan pesan SMS yang telah di-enkripsi tidak dapat dimanipulasi oleh pihak yang tidak bertanggung jawab

3.1. Arsitektur Sistem

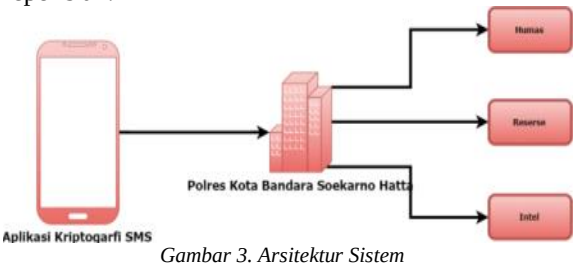
Pada arsitektur sistem aplikasi ini dapat dijalankan dengan menggunakan *smartphone* dengan sistem operasi android versi *lollipop* dan *marshmallow* yang sudah terinstal aplikasi kriptografi SMS teknik kriptografi RSA dan 3DES.



Gambar 2. Arsitektur Sistem

3.2. Arsitektur Pengguna

Implementasi pengamanan SMS *(Short Message Service)* ini melibatkan unit / bagian sistem kepolisian.



Gambar 3. Arsitektur Sistem

3.3. Rancangan Sistem

Gambar 4. Rancangan Layar Menu Utama

Rancangan layar menu utama berguna pengguna memilih layar pesan baru, layar kotak masuk, layar kotak keluar, layar tentang pembuat.

Gambar 5. Rancangan Layar Pesan Baru

Rancangan layar pesan baru berguna membuat pesan baru dengan mengisi nomor tujuan pesan secara manual atau memilih kontak tujuan yang tersimpan didalam kontak telepon.

Gambar 6. Rancangan Layar Kotak Masuk

Rancangan layar otak masuk berguna untuk menampilkan *list* kotak masuk serta mengenkrip isi pesan serta terdapat fitur balas pesan dan meneruskan pesan.

Gambar 7. Rancangan Layar Kotak Keluar

Rancangan layar menu kotak keluar berguna menampilkan *list* kotak keluar, mendekripsi isi pesan yang telah dienkripsi serta terdapat fitur meneruskan pesan

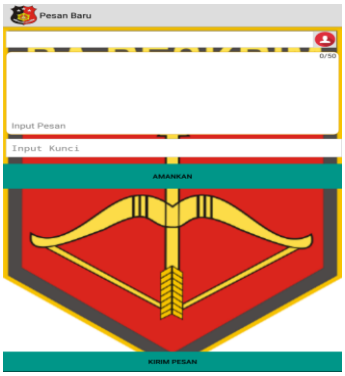
Gambar 8. Rancangan Layar Tentang Pembuat

Rancangan layar tentang pembuat berisi tentang pembuat aplikasi kriptografi SMS *(Short Message Service)*.

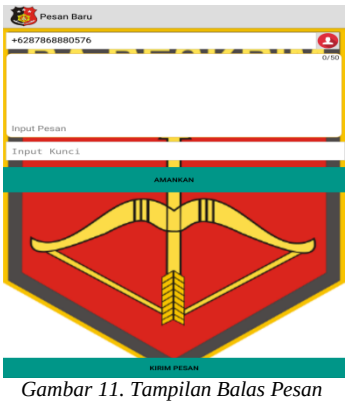
4. HASIL DAN PEMBAHASAN

Pada saat program dijalankan akan muncul menu utama seperti pada gambar 8 ini. *User* memiliki 4 pilihan menu yakni pesan baru, kotak masuk, kotak keluar dan tentang pembuat.

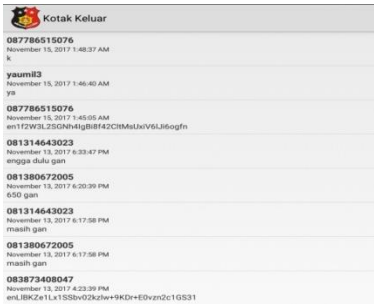
Gambar 9. Tampilan Awal Aplikasi



Gambar 10. Menu Pesan Baru



Gambar 11. Tampilan Balas Pesan

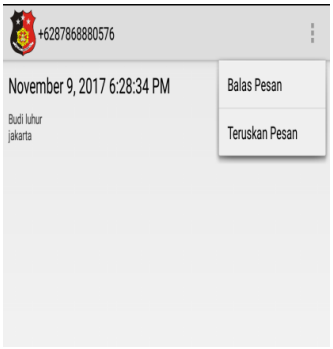


Gambar 12. Menu Kotak Keluar

Gambar 13. Menu Baca Kotak Keluar

Gambar 14. Menu Kotak Masuk

Gambar 15. Menu Baca Kotak Masuk



Gambar 16. Menu Baca Kotak Masuk

Gambar 17. Menu Baca Kotak Masuk

Dibawah ini adalah table pengujian yang telah dilakukan dalam bentuk file yang telah terenkrip dan terdekrip.

Tabel 1. Hasil Pengujian File Yang Terenkrip

No	*SMS*	*Plaintext*	*Ciphertext*	**Hasil Pengujian**
1	Isi pesan	Universitas Budi luhur Jakarta	en+JykA+op6S3ApHKOgnFU07gD14klffh1gEdte6DXAqlQK2try5HFYw81NDwlT1ohitj7+pjamWwfvNqSEAhp07v6frtCVLMtttdwovvUv8JmtollPsH9lg	Berhasil
	Jumlah Karakter	30 karakter	120 karakter	
2	Isi pesan	Penangkapan di terminal 3 ultimate	enTHf8ADIGNVN/E6EvxAXtRRDtTaTpLevwKbqBRwgu627ip+Yir6Gxw+d15mF3XbDUXIwMfqwml2ejX5LO+RdgefBAtL/Vofwz8nclaYmWBpeba6LKXWwwTsD7XID1wCG	Berhasil
	Jumlah Karakter	42 karakter	129 karakter	
3	Isi pesan	Butir melaksanakan giat buddy system di VVIP Room	enWamthJ8yw1SPS950zhMrKsV4iK1c0EUiE8KfkyPiul6ZpBdCOeeTPz5qpSaL4rvja06JdUpims9f6ybIRey0fN0hS8QOkrQBhjJHHb7cuPSzzWNfPrjL0R8sTzUNOVIsjVTPVn3oW0WQN35Ofc3Yog	Berhasil
	Jumlah Karakter	49 karakter	154 karakter	

Table 2. Hasil Pengujian File Yang Terenkrip

No	*SMS*	*Ciphertext*	*Plaintext*	**Hasil Pengujian**
1	Isi pesan	en+JykA+op6S3ApHKOgnFU07gD14klffh1gEdte6DXAqlQK2try5HFYw81NDwlT1ohitj7+pjamWwfvNqSEAhp07v6frtCVLMtttdwovvUv8JmtollPsH9lg	Universitas Budi luhur Jakarta	Berhasil
	Jumlah Karakter	120 karakter	30 karakter	
2	Isi pesan	enTHf8ADIGNVN/E6EvxAXtRRDtTaTpLevwKbqBRwgu627ip+Yir6Gxw+d15mF3XbDUXIwMfqwml2ejX5LO+RdgefBAtL/Vofwz8nclaYmWBpeba6LKXWwwTsD7XID1wCG	Penangkapan di terminal 3 ultimate	Berhasil
	Jumlah Karakter	129 karakter	42 karakter	
3	Isi pesan	enWamthJ8yw1SPS950zhMrKsV4iK1c0EUiE8KfkyPiul6ZpBdCOeeTPz5qpSaL4rvja06JdUpims9f6ybIRey0fN0hS8QOkrQBhjJHHb7cuPSzzWNfPrjL0R8sTzUNOVIsjVTPVn3oW0WQN35Ofc3Yog	Butir melaksanakan giat buddy system di VVIP Room	Berhasil
	Jumlah Karakter	154 karakter	49 karakter	

5. KESIMPULAN

Setelah dilakukan pengujian terhadap aplikasi yang dikembangkan dapat ditarik beberapa kesimpulan, antara lain :

a. Pesan terjaga kerahasiannya pesan dengan tidak ada perubahan pesan asli pada saat pesan yang dienkripsi dikembalikan dengan menggunakan algoritma RSA *(Rivest Shamir Adleman)* dan 3DES *(Triple Data Encryption Standard).*
b. Di Kepolisian *Resort* Kota Bandara Soekarno Hatta dapat meminimalisir kebocoran informasi saat menggunakan aplikasi yang dikembangkan.

6. DAFTAR PUSTAKA

[1]Ayuningtyas N., 2008, *Implementasi kode Huffman dalam aplikasi kompresi teks pada layanan SMS*, Bandung, Institut Teknologi Bandung.

[2]Zain, A.R., 2015, Analisa Kinerja Teknik dan Algoritma Keamanan SMS, Institut Teknologi Bandung.

[3]Bodic, G., 2003, *Mobile Messaging Technologies and Services*, John Wiley & Sons Ltd, West Sussex, England.

[4]Gupta, R.K., and Singh, P., 2013, A New Way to Design and Implementation of Hybrid Crypto System for Security of the Information in Public Network, International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459.

[5]Stinson, D.R., 2006, Cryptography, Theory and Practice, 3rd Edition, Chapman and Hall, London.

[6]Hidayat, A., 2009, *Enkripsi Dan Dekripsi Data Dengan Algoritma 3DS (Triple Data Encryption Standard)*, Jurnal Matematika Universitas Padjajaran.