APLIKASI PENGAMANAN SMS (SHORT MESSAGE SERVICE) DENGAN MENGGUNAKAN ALGORITMA AES-128 BERBASIS ANDROID PADA KANTOR NOTARIS RINA ADRIANI S.H

Anita Fauziah[1)], Dewi Kusumaningsih[2)]
Program Studi Anda, Fakultas Teknologi Informasi, Universitas Budi Luhur
Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260
Telp. (021) 5853753, Fax. (021) 5866369
E-mail : anitafauziah.fauziah@gmail.com, Dewi.kusumaningsih@budiluhur.ac.id[2)]

ABSTRAK

Perkembangan teknologi masa kini mengubah cara masyarakat dalam berkomunikasi. Telepon Seluler yang dulu hanya dapat melakukan telepon dan mengirim pesan kini dapat digunakan dalam berbagai hal. Munculnya handphone pintar (smartphone) merupakan handphone atau telepon seluler yang saat ini sangat berkembang yang memiliki sistem operasi kompleks layaknya komputer dan memiliki banyak fitur lengkap tetapi fitur lama seperti fitur SMS masih banyak digunakan oleh pengguna handphone pintar (smartphone) untuk bertukar informasi dengan mudah dan cepat dalam melakukan pengiriman pesan dan terkadang membuat pengguna kurang memperhatikan ancaman yang mengintai seperti masalah keamanan, kerahasiaan dan keontetikan pesan. Oleh karena itu, diperlukan suatu aplikasi pengamanan pesan SMS yang bertujuan untuk meningkatkan keamanan pesan, melindungi suatu pesan agar tidak di baca oleh pihak dan mencegah pihak yang tidak berwenang untuk menyisipkan, menghapus, ataupun merubah pesan. Kriptografi merupakan salah satu solusi yang dapat dimanfaatkan dan dikembangkan dalam menyelesaikan masalah keamanan pesan SMS. Pada penelitian ini dibuatlah aplikasi pengamanan pesan SMS dengan menerapkan algoritma kriptografi Advanced Encryption Standard (AES)-128. Pesan SMS yang dapat dikirimkan melalui aplikasi ini maksimal sepnjang 160 karakter pesan enkripsi. Pesan SMS akan dienkripsi atau diacak sebelum dikirim dan penerima dapat mendekripsi atau membalikkan pesan SMS seperti semula. Hasil dari penelitian ini akan diimplementasikan dalam sebuah program aplikasi pesan berbasis Android yang dapat memberikan kemudahan untuk mengamankan pesan penting.

Kata kunci : SMS, Kriptografi, Advanced Encryption Standard (AES)-128, enkripsi, dekripsi

1. PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi telekomunikasi saat ini sudah sangat berkembang. Salah satu dari teknologi telekomunikasi, munculnya ponsel cerdas (*smartphones*) yang dikenal dengan sebutan Android yang memiliki sistem operasi kompleks layaknya komputer. Android ini memiliki berbagai fungsi seperti multimedia, multiplayer, games, transfer data, video streaming, dan lain-lain. Meskipun Android memiliki fitur yang lengkap, namun fitur lama seperti layanan pesan singkat atau yang lebih diketahui dengan SMS masih banyak yang menggunakannya. SMS (*Short Message Service*) adalah suatu fasilitas untuk mengirim dan menerima pesan singkat berupa teks dari sebuah handphone (telepon seluler) ke handphone lainnya.

Kantor Notaris Rina Adriani S.H., merupakan kantor Notaris dan PPAT yang mengurus pembuatan akta-akta otentik, mengesahkan surat-surat dibawah tangan, mendaftarkan surat-surat dibawah tangan, memberikan nasihat hukum, penjelasan mengenai undang-undang kepada pihak-pihak yang bersangkutan, dan membuat akta tanah. Demi mempercepat pembuatan dokumen dan pertukaran informasi dengan klien, notaris menggunakan SMS untuk menginformasikan hal-hal yang harus dipersiapkan dan berkas-berkas apa saja yang dibutuhkan. SMS memegang peranan penting bagi penggunanya dalam bertukar informasi. Mengingat pesan yang terkandung dalam SMS membuat orang yang tidak bertanggung jawab ingin mengambil keuntungan dengan memanfaatkan kelemahan SMS. Sehingga diperlukan pengamanan SMS untuk menjaga pesan SMS agar tidak dapat diakses oleh pihak yang tidak bertanggung jawab. Demi menjaga pesan SMS maka pada penelitian ini maka penulis membuat perancangan aplikasi pengamanan SMS (*Short Message Service*) berbasis android dengan metode AES-128 untuk mengamankan isi pesan dari

notaris untuk klien agar tidak dapat diakses oleh pihak yang tidak berkepentingan dan tidak bertanggung jawab. Pesan SMS akan dienkripsi atau diacak sebelum dikirim dan penerima dapat mendekripsi atau mengembalikan pesan seperti semula. Sehingga notaris dan klien dapat melakukan pertukaran informasi melalui SMS lebih aman dan nyaman.

Agar tidak keluar dari materi pembahasan maka akan diberikan beberapa batasan masalah sebagai berikut: a. Algoritma yang dipakai dalam pembuatan aplikasi yaitu *Advanced Encryption Standard (*AES*)* – 128; b. Bahasa pemrograman yang digunakan adalah java; c. Enkripsi yang dilakukan hanya berupa pesan teks SMS; d. Media yang digunakan untuk implementasi adalah ponsel cerdas (smartphones) dengan sistem operasi android versi 5.0 *Lollipop*. Aplikasi ini dibuat untuk mengamankan isi pesan SMS agar tidak mudah dibaca oleh pihak yang tidak berkepentingan.

Dalam penulisan skripsi ini, digunakan metode Waterfall berupa pengumpulan data dan informasi untuk mempermudah analisa dan perancangann aplikasi

2. LANDASAN TEORI

2.1 Android

Android merupakan sistem operasi untuk perangkat *mobile* berbasis linux yang mencakup sistem operasi, middleware dan aplikasi. [1]

2.2 *Short Message Service* (SMS)

SMS merupakan suatu fasilitas untuk mengirim dan menerima suatu pesan singkat berupa teks melalui perangkat nirkabel, yaitu perangkat nirkabel yang digunakan adalah telepon selular. Yang memiliki panjang isi pesan maksimal 160 karakter, dimana setiap karakter memiliki panjang 7 bit. Pada umumnya karakter sepanjang 8 bit dan 7 bit digunakan untuk menampilkan data seperti gambar dan simbol. pesan yang lebih dari 160 karakter maka dipecah menjadi beberapa buah SMS. [2]

2.3 Kriptografi

Kriptografi menurut terminologi adalah merupakan ilmu dan seni yang bertujuan untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat yang lain. [3]

Bentuk pesan yang tersandikan disebut *chipertext*. *Chipertext* adalah pesan acak yang harus dikembalikan ke bentuk awal atau dikembalikan menjadi *plaintext* semula agar pesan dapat dibaca oleh orang yang seharusnya menerima pesan. Ada empat tujuan mendasar dari ilmu kriptografi ini yang juga merupakan aspek keamanan informasi yaitu:

1. Kerahasiaan rahasia merupakan untuk menjaga isi informasi dari orang yang tidak berhak.
2. Integritas data adalah untuk menjaga integritas data agar orang yang tidak berhak tidak dapat menyisipkan, menghapus, pensubtitusian data lain kedalam data yang asli.
3. Autentikasi merupakan identifikasi atau pengenalan informasi yang dikirimkan harus diautentikasi keaslian, isi datanya, waktu pengiriman, dan lain-lain..
4. Non-repudiasi merupakan usaha untuk mencegah terjadinya penyangkalan terhadap pengiriman/ terciptanya suatu informasi oleh yang mengirimkan atau membuat.

2.4 Advanced Encryption Standard (AES)

AES algorithm dipublikasikan oleh NIST *(National Institute of Standard and Technology)* pada tahun 2001 yang digunakan untuk menggantikan algoritma DES. [4]

Algoritma AES merupakan algoritma kunci simetrik yang dapat mengenkripsi dan dekripsi suatu informasi atau pesan. Kunci Kriptografi pada Algoritma AES adalah 128, 192, dan 256 bit untuk mengenkripsi dan dekripsi data pada blok 128 bit. [5]

Perbedaan panjang kunci akan sangat mempengaruhi jumlah *round/putaran* yang akan diimplementasikan pada algoritma AES ini. Berikut ini adalah tabel yang memperlihatkan jumlah *round*/putaran (Nr) yang akan diimplementasikan pada masing-masing panjang kunci**.**

Tabel 1: Tabel Perbandingan Panjang Kunci AES

	Jumlah Key (Nk)	Ukuran Block (Nb)	Jumlah Putaran (Nr)
AES – 128	4	4	10
AES – 192	6	4	12
AES – 256	8	4	14

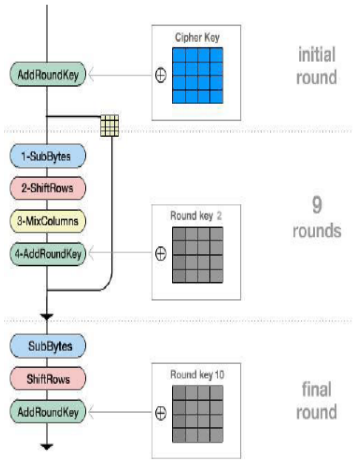
2.5 Proses Enkripsi AES-128

Proses putaran pada saat mengenkripsi pesan menggunakan AES-128 dikerjakan sebanyak 10 kali (a=10). [6] yaitu :

1) *Addroundkey* : melakukan XOR antara state awal (*plainteks*) dengan
2) Putaran sebanyak Nr-1 kali, proses yang dilakukan pada setiap putaran adalah :
   a) *SubBytes* adalah subtitusi byte dengan menggunakan tabel subtitusi (S-box)
   b) *ShiftRow* adalah pergeseran baris-baris array state secara wrapping.
   c) *MixColumns* adalah mengacak data di masing-masing kolom array state.

d) *AddRoundKey* adalah melakukan XOR antara state sekarang round key.
e) *Final Round* adalah proses putaran untuk putaran terakhir yang meliputi *SubBytes,*

Ilustrasi proses enkripsi AES-128 dapat dilihat dari gambar dibawah ini:

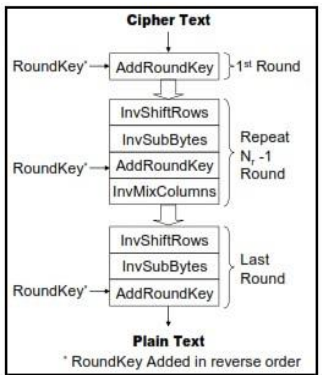


Gambar 1: Ilustrasi proses enkripsi AES-128

2.6 Proses Dekripsi AES-128

Proses dekripsi pada algoritma AES menggunakan transformasi yang berlawanan dari proses enkripsi. Transformasi yang berlawanan tersebut digunakan untuk menghasilkan *inverse cipher* sehingga *ciphertext* yang dikembalikan menjadi plaintext. Penjelasan lebih mendalam mengenai transformasi *InvShiftRows*, *InvSubBytes*, *InvMixColumns*, dan *AddRoundKey* . [7]

Ilustrasi proses dekripsi AES-128 dapat dilihat dari gambar dibawah ini:



Gambar 2: Diagram Alur Proses Dekripsi AES-128

3. RANCANGAN SISTEM DAN APLIKASI

3.1 Rancangan Layar Aplikasi

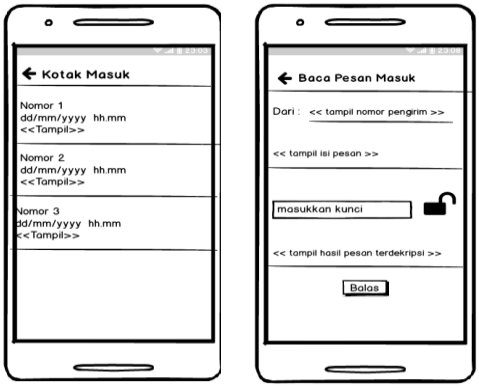
Pada aplikasi ini terdiri dari lima menu, yaitu Menu utama, pesan baru, kotak masuk, bantuan, tentang dan keluar. Aplikasi ini dimulai dari menu utama kemudian kita dapat memilih menu pesan baru untuk memulai membuat pesan baru kemudian menu kotak masuk untuk melihat pesan-pesan yang masuk lalu menu bantuan berisikan panduan untuk mengoperasikan aplikasi ini dan menu tentang yang berisi informasi dari aplikasi ini. Dalam menu pesan baru harus menginput no tujuan, langkah selanjutnya menginput pesan yang akan dikirim, kemudian masukkan kunci enkripsi lalu mengklik button gambar *lock*, ketika sudah akan menampilkan hasil klik *button* kirim pesan untuk melakukan pengiriman pesan yang telah berhasil dienkripsi. Menu kotak masuk adalah sederetan pesan masuk yang sudah berbentuk pesan enkripsi, lalu pilih salah satu pesan enkripsi untuk didekripsi dengan mengklik salah satu pesan lalu akan menampilkan menu baca pesan yang berisi nomor pengirim, pesan,kunci, *button* gambar *unlock*, untuk mengembalikan pesan seperti semula perlu memasukkan kunci yang sama pada saat mengenkripsi pesan setelah itu klik button gambar *unlock* maka hasil akan ditampilkan, dan klik button balas maka akan dilempar kemenu tulis pesan.
Gambar 3 berikut ini adalah rancangan layar Menu Utama dimana pengguna dapat memilih menu pada saat memulai aplikasi.

Gambar 3: Rancangan Layar Menu Utama

Gambar 4 merupakan rancangan layar menu pesan baru dimana user dapat menulis dan mengirimkan pesan yang sudah terenkripsi.

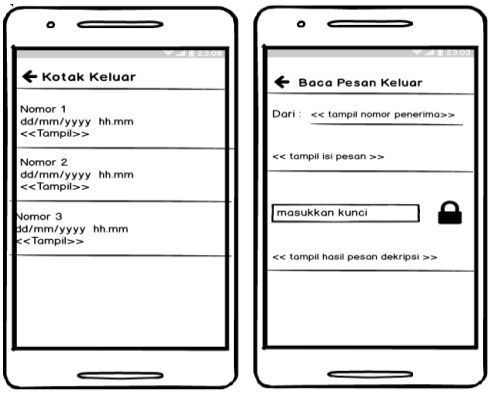
Gambar 4: Rancangan Layar Menu Pesan Baru

Gambar 5 merupakan rancangan layar kotak masuk dimana pengguna dapat melihat sederetan pesan masuk terenkripsi dan dapat membaca pesan terenkripsi dengan memilih salah satu pesan lalu mendekripsi pesan.



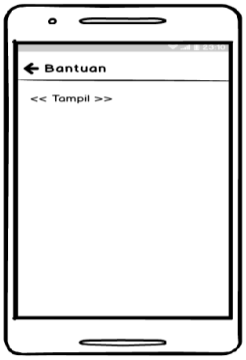
Gambar 5: Rancangan Layar List Kotak Masuk dan Baca Pesan Masuk

Gambar 6 merupakan rancangan layar kotak keluar dimana pengguna dapat melihat sederetan pesan yang berhasil dikirim dan dapat membaca pesan dengan memilih salah satu pesan.



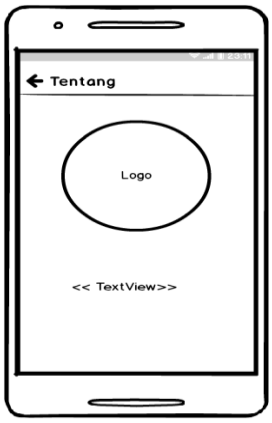
Gambar 6: Rancangan Layar List Kotak Keluar & Baca Pesan Keluar

Gambar 7 merupakan rancangan layar bantuan dimana pengguna dapat melihat panduan untuk mengoperasikan aplikasi ini.



Gambar 7: Rancangan Layar Bantuan

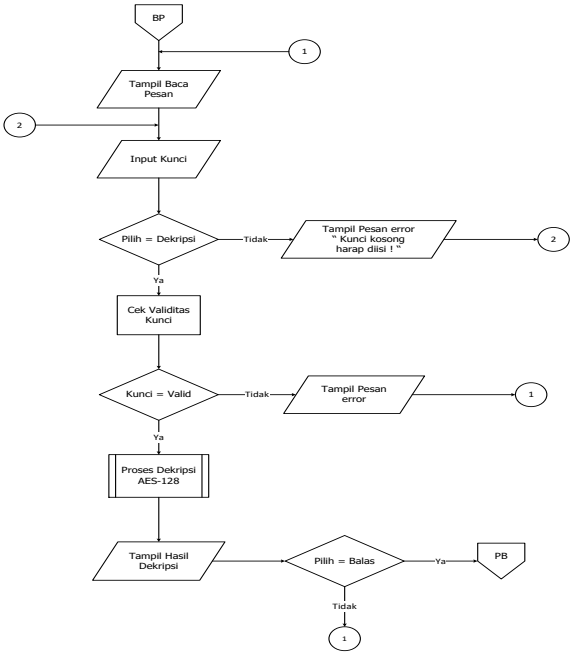
Gambar 8 merupakan rancangan layar tentang dimana pengguna dapat melihat logo dan informasi seputar pembuat aplikasi ini.



Gambar 8: Rancangan Layar Tentang

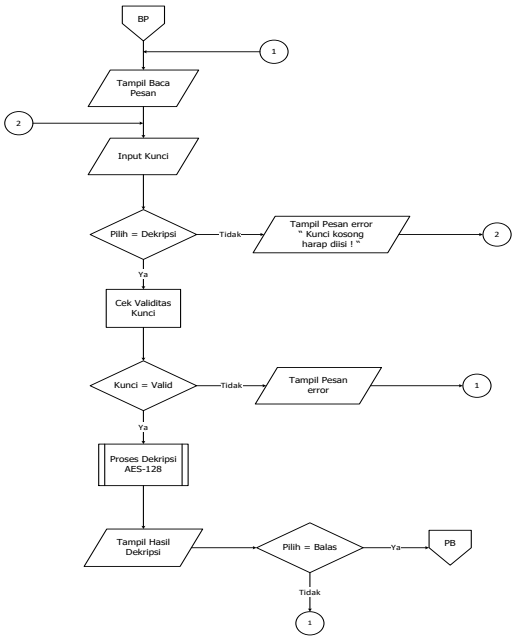
3.2 Flowchart

Pada gambar 9 merupakan flowchart pesan baru yang menggambarkan alur jalannya proses dimana pengguna dapat membuat atau menulis pesan yang akan dienkripsi dan pengguna dapat mengirimkan pesan enkripsi.



Gambar 9: Flowchart Pesan Baru

Gambar 10 merupakan flowchart baca pesan masuk yang menggambarkan alur jalannya membaca pesan dan mendekripsi pesan yang telah dienkripsi.



Gambar 10: Flowchart Baca Pesan Masuk

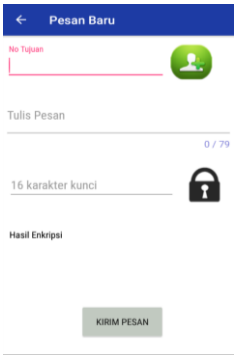
4. HASIL DAN PEMBAHASAN

4.1 Tampilan Layar

Pada Gambar 11 adalah tampilan layar menu utama yang akan tampil pada saat aplikasi dijalankan.

Gambar 11: Tampilan Layar Menu Utama

Gambar 12 adalah tampilan layar pesan baru dimana pengguna dapat menulis dan mengirimkan pesan enkripsi.



Gambar 12: Tampilan Layar Pesan Baru

Gambar 13 adalah tampilan layar kotak masuk dan baca pesan masuk.

Gambar 13: Tampilan Layar Kotak Masuk dan Baca Pesan Masuk

Gambar 14 adalah tampilan layar kotak keluar dan baca pesan keluar.

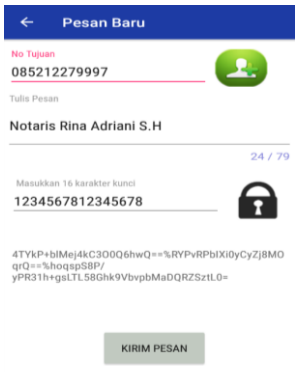
Gambar 14: Tampilan Layar Kotak Keluar dan Baca Pesan Keluar

Gambar 15 adalah tampilan layar bantuan dan tampilan layar tentang.

Gambar 15: Tampilan Layar Bantuan dan Tentang

4.2 Pengujian Aplikasi

Pada Gambar 16 adalah hasil pengujian proses enkripsi pesan sms.



Gambar 16: Proses Enkripsi SMS

Pada Gambar 17 adalah hasil pengujian proses dekripsi pesan SMS.

Gambar 17: Proses Dekripsi Pesan SMS

5. KESIMPULAN

Berdasarkan analisis dan perancangan, pembuatan, serta serangkaian uji coba dalam program dari aplikasi kriptografi, maka dapat disimpulkan sebagai berikut:

a. Pesan dapat diamankan dengan kriptografi algoritma *Advanced Encyrption Standard* (AES)-128.
b. Dengan adanya program aplikasi kriptografi, pengamanan pesan dalam proses penyampaian informasi menjadi lebih aman.
c. Aplikasi SMS dan pesan rahasia dengan sistem keamanan kriptografi algoritma AES-128 hanya dapat mengenkripsi dan mendekripsi pesan pada aplikasi yang dibuat.
d. Proses dekripsi dengan kunci yang sama atau sesuai pada saat mengirim pesan dan akan mengembalikan pesan terenkripsi menjadi pesan semula tanpa mengalami perubahan pada isi.

Adapun beberapa saran yang diperlukan dalam aplikasi ini agar menjadi lebih baik lagi dikemudian hari, berikut ini diantaranya:

a. Menambahkan beberapa fitur yang dapat mempermudah penggunaan aplikasi, seperti fitur hapus pesan untuk menghapus pesan yang sudah tidak ingin dibaca lagi, fitur teruskan pesan untuk meneruskan pesan ketika klien atau notaris ingin meneruskan pesan dan fitur lainnya yang dapat membuat aplikasi menjadi semakin mudah digunakan.
b. Pada fitur balas pesan tidak dapat menginput nomor secara otomatis, diharapkan aplikasi ini dapat menginput nomor secara otomatis ketika ingin membalas pesan sehingga memudahkan notaris atau klien dalam membalas pesan.

DAFTAR PUSTAKA

[1] Intania, 2012. *All About Android*, Jakarta: Kuncikom.

[2] Subhan, S., Amini, S. & Ariyani, P.F., 2017. Implementasi Pengamanan Data Enkripsi SMS Dengan Algoritma RC4 Berbasis Android. *Seminar Nasional Inovasi dan Aplikasi Teknologi di Industri*, pp.1–6.

[3] Ariyus, D., 2008. Pengantar ilmu kriptografi: Teori, Analisis, dan Implementasi., Yogyakarta: Andi.

[4] Abdurachman, H. & Gunandhi, E., 2015. Keamanan Komunikasi Data SMS Pada Android dengan Menggunakan Aplikasi Kriptografi Advanced Encryption Standard (AES). *Jurnal Algoritma*, pp.1–6.

[5] Informatika, J.T., Teknik, F. & Oleo, U.H., 2015. Penyadapan SMS dan GPS Berbasis Android Menggunakan Algoritma Advanced Encyption Standard (AES). *Universitas Halu Oleo*, 1(2), pp.11–22.

[6] Arif, A. et al., 2016. Rekayasa Perangkat Lunak Kriptografi Menggunakan Algoritma Advanced Encryption Standard (AES) 128 BIT Pada Sistem Keamanan Short Message Service (SMS) Berbasis Android. *Jurnal TEKNOIF*, 4(1).

[7] Pabokory, F.N., Astuti, I.F. & Kridalaksana, A.H., 2015. Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, Dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard. *Jurnal Informatika Mulawarman*, 10(1), pp.20–31.