Jurnal Mahajana Informasi. Vol. 6, No. 2, Desember 2021
e-ISSN : 2527-8290

Penerapan Kriptografi Dalam Pengamanan Pesan Text Berbasis Android Dengan Menggunakan Metode Rijndael

Ahmad Teguh Fikri Alhamdi[1*], R. Fanry Siahaan[2]

[1,2]Program Studi Teknik Informatika, STMIK Pelita Nusantara, Jl. Iskandar Muda No.1 Medan, Sumatera Utara, Indonesia, , Phone: +6285359455843, Fax: -

E-mail: atfa1902@gmail.com , rfanry@gmail.com

Abstrak

Kriptografi merupakan teknik penyandian untuk menjaga kerahasian pesan agar tidak mudah di baca/di ketahui oleh orang yang tidak berhak. Dalam kriptografi ada dua buah bagian utama yaitu enkripsi dan dekripsi. Enkripsi adalah proses penyembunyian data pesan, mengubah plaintext menjadi chipertext, sedangkan dekripsi merupakan kebalikan dari enkripsi, bertujuan untuk memahami pesan yang ada. Algoritma Rijndael adalah salah satu algoritma pada kunci simetris yang dapat digunakan untuk melakukan enkripsi data sehingga data asli hanya dapat dibaca oleh seseorang yang memiliki kunci enkripsi tersebut. Penyandian Rijndael menggunakan proses yang berulang yang disebut dengan ronde. Jumlah ronde yang digunakan oleh Rijndael tergantung dengan panjang kunci yang digunakan. Setiap ronde membutuhkan kunci ronde dan masukan dari ronde berikutnya. Sistem operasi untuk perangkat mobile yang menyertakan middleware (virtual machine) dan sejumlah aplikasi utama disebut sebagai. Android sebuah modifikasi dari kernel Linux. Tujuan pembuatan sistem operasi ini sebagai penyedia platform yang terbuka, misalnya dalam penggunaan chating, namun didalam penggunaanya masih terdapat kelemahan sistem. Android juga dirancang untuk memudahkan pengembang membuat aplikasi dengan batasan yang minim sehingga kreativitas pengembang menjadi lebih berkembang. Oleh karena itu di perlukan sebuah keamanan yang dapat mengamankan pesan atau chating agar dapat membantu privasi seseorang dalam melakukan kegiatan sehari-hari.

Kata Kunci : Kriptografi, PDF, RSA.

Abstract

Cryptography is an encoding technique to maintain the confidentiality of messages so that they are not easily read / known by unauthorized people. In cryptography there are two main parts, namely encryption and decryption. Encryption is the process of hiding message data, converting plaintext into ciphertext, while decryption is the opposite of encryption, aiming to understand the message. The Rijndael algorithm is one of the algorithms on symmetric keys that can be used to encrypt data so that the original data can only be read by someone who has the encryption key. Rijndael encoding uses an iterative process called a round. The number of rounds used by Rijndael depends on the length of the key used. Each round requires a round key and input from the next round. An operating system for mobile devices that includes a middleware (virtual machine) and a number of key applications is referred to as. Android is a modification of the Linux kernel (mintoro, 2019). The purpose of making this operating system is as an open platform provider, for example in the use of chat, but in its use there are still system weaknesses. Android is also designed to make it easier for developers to create applications with minimal limitations so that developer creativity can develop more. Therefore we need a security that can secure messages or chats in order to help someone's privacy in carrying out daily activities.

Keywords: *Cryptography, PDF, RSA.*

Pendahuluan

Pada era globalisasi saat ini Keamanan data menjadi hal yang sangat penting dan terus berkembang. Perkembangan ilmu dan teknologi telah mempengaruhi segala aspek kehidupan manusia. Informasi dan data dapat dengan mudah dan cepat untuk dikirim melalui jaringan [1]. Hal ini tentu saja menimbulkan resiko jika informasi dan data yang dikirim bisa diakses oleh pihak yang tidak berhak sehingga mengakibatkan data yang akan dikirim di ketahui oleh pihak lain [2]. Masalah keamanan merupakan salah satu aspek terpenting dari sebuah sistem informasi. Sementara itu masalah keamanan untuk saat ini sering tidak dipedulikan, padahal hal tersebut merupakan hal yang sangat penting dalam pengamanan data/informasi yang bersifat rahasia untuk mengurangi dampak kerugian materil dan nonmateril.

Salah satu model untuk mengamankan data adalah kriptografi. Kriptografi merupakan teknik penyandian untuk menjaga kerahasian pesan agar tidak mudah di baca/di ketahui oleh orang yang tidak berhak. Dalam kriptografi ada dua buah bagian utama yaitu enkripsi dan dekripsi [3]. Enkripsi adalah proses penyembunyian data pesan, mengubah plaintext menjadi chipertext, sedangkan dekripsi merupakan kebalikan dari enkripsi, bertujuan untuk memahami pesan yang ada. Terdapat dua model dalam kriptografi, yaitu kriptografi modern dan kriptografi klasik (konvensional) [2]. Pada kriptografi modern, proses enkripsi menggunakan perhitungan yang rumit dan melibatkan bilangan yang besar, sehingga diperlukan bantuan komputer [4]. Ada dua jenis kriptografi modern yaitu simetris dan asimetris. Algoritma simetris adalah algoritma yang menggunakan kunci yang sama untuk proses enkripsi dan proses dekripsinya. Sedangkan algoritma asimetris membutuhkan dua kunci yang salah satunya digunakan untuk proses enkripsi dan satu lagi untuk proses dekripsi. Kunci untuk enkripsi dan dekripsi sama dengan panjang 12 karakter, input yang digunakan berupa text berbasis pada ASCII (American Standard Code for Information Interchange) dan rubik yang digunakan adalah kubus rubik 4×4×4, yang biasa disebut sebagai kunci simetris[4].

Algoritma Rijndael adalah salah satu algoritma pada kunci simetris yang dapat digunakan untuk melakukan enkripsi data sehingga data asli hanya dapat dibaca oleh seseorang yang memiliki kunci enkripsi tersebut. Menurut [5] Penyandian Rijndael menggunakan proses yang berulang yang disebut dengan ronde. Jumlah ronde yang digunakan oleh Rijndael tergantung dengan panjang kunci yang digunakan. Setiap ronde membutuhkan kunci ronde dan masukan dari ronde berikutnya. Kunci ronde dibangkitkan berdasarkan kunci yang diberikan. Menurut [6] algoritma AES Rijndael memiliki tingkat keamanan yang tinggi berdasarkan variasi panjang kunci yang dimiliki, serta memiliki kompleksitas waktu dan ruang yang baik karena kesederhanaannya.

Android adalah sebuah sistem operasi untuk perangkat mobile yang menyertakan middleware (virtual machine) dan sejumlah aplikasi utama. Android sebuah modifikasi dari kernel Linux [7]. Tujuan pembuatan sistem operasi ini sebagai penyedia platform yang terbuka, misalnya dalam penggunaan chating, namun didalam penggunaanya masih terdapat kelemahan sistem. Android juga dirancang untuk memudahkan pengembang membuat aplikasi dengan batasan yang minim sehingga kreativitas pengembang menjadi lebih berkembang [8]. Oleh karena itu di perlukan sebuah keamanan yang dapat mengamankan pesan atau chating agar dapat membantu privasi seseorang dalam melakukan kegiatan sehari-hari.

Metode

1. *Kriptografi*

Kriptografi berasal dari bahasa Yunani yaitu "*kriptos*" dan "*graphia*". Kriptos dapat diartikan sebagai rahasia, sedangkan *graphia* dapat diartikan sebagai tulisan. Menurut teminologinya kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan Ketika pesan dikirim dari suatu tempat ketempat yang lain[9]. Kriptograf merupakan ilmu yang digunakan untuk mempelajari tulisan rahasia dimana komunikasi dan data dapat dikodekan dan berfungsi mencegah orang yang tidak berwenang untuk memanipulasi informasi

melalui sebuah teknik sehingga hanya pihak berwenang saja yang dapat mengetahui isi informasi tersebut [10].

Ada beberapa proses dalam penyandian dalam kriptografi, berikut adalah proses pada kriptografi tersebut [11]:

a. Proses menyandikan plaintext menjadi ciphertext disebut enkripsi (encryption) atau enciphering
b. Proses mengembalikan ciphertext menjadi plaintext-nya disebut dekripsi (decryption) atau deciphering

2. Algoritma Rijndael

Algoritma AES Rijndael adalah algoritma kriptografi modern yang di publikasi oleh NIST (National Institute of Standard and Technology) tahun 2001 menggunakan mode cipher blok dan menggunakan kunci simetris [12]. Pada tahun 90-an, setelah beberapa tahun standar penyandian simetris Data Encryption Standard (DES) dianggap tidak lagi aman, lembaga standar Amerika Serikat, National Institute of Standards and Technology (NIST) membuat sayembara untuk menggantikan Data Encryption Standard (DES) dengan sebuah sistem penyandian baru pada tanggal 12 September 1997 [13].

Hasil

Rijndael bisa memiliki ukuran mariks lebih dari itu dengan menambahkan berapa banyak kolom yang diperlukan. Berikut ini merupakan Contoh kasus mengubah *plaintext* dengan rijndael-128 Bit :

Plaintext = PELITA NUSANTARA
Key = 2021000000000000

a. Masukan (128-Bit Pesan Dan Kunci)

Mengubah *plaintext* dan *key* tersebut menjadi bentuk bilangan HEXADESIMAL dengan melihat tabel ASCII (*American Standard Code for Information Interchange*) atau Kode Standar Amerika untuk Pertukaran Informasi yang ada pada tabel 2.1 atau pada Lampiran, berikut adalah hasilnya.

Tabel 1 Contoh *Plaintext*

P	**E**	**L**	**I**	**T**	**A**		**N**	**U**	**S**	**A**	**N**	**T**	**A**	**R**	**A**
5	4	4	4	5	4	2	4	5	5	4	4	5	4	5	4
0	5	C	A	4	1	0	E	5	3	1	E	4	1	2	1

Sehingga Plaintext (*Hex*) adalah: 50 45 4c 4a 54 41 20 4e 55 53 41 4e 54 41 52 41

Tabel 2 Contoh *Key*

2	**0**	**2**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**
3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
2	0	2	1	0	0	0	0	0	0	0	0	0	0	0	0

Sehingga Key (*Hex*) adalah: 32 30 32 31 30 30 30 30 30 30 30 30 30 30 30 30

b. Initial Round

Membagi menjadi 4 blok dan XOR tiap barisnya, pada kotak pertama adalah plaintext yaitu PELITA NUSANTARA yang sudah dalam bentuk Hexadesimal. Dibagi menjadi 4 bagian sehingga tersusun manjadi seperti berikut, setelah itu di Xor kan dengan kunci yang sudah disusun juga seperti plaintext. Berikut adalah initial round tersebut:

$$\begin{bmatrix}50 & 45 & 4C & 4A\\ 54 & 41 & 20 & 4E\\ 55 & 53 & 41 & 4E\\ 54 & 41 & 52 & 41\end{bmatrix} \text{ XOR } \begin{bmatrix}32 & 30 & 32 & 31\\ 30 & 30 & 30 & 30\\ 30 & 30 & 30 & 30\\ 30 & 30 & 30 & 30\end{bmatrix} = \begin{bmatrix}62 & 75 & 7E & 7B\\ 64 & 71 & 10 & 7E\\ 65 & 63 & 71 & 7E\\ 64 & 71 & 62 & 71\end{bmatrix}$$

c. Proses *Sub-bytes*

Mengubah hasil tiap baris dengan melihat *S-Box*, pada tahapan ini adalah mengubah hasil yang didapat sebelumnya dengan melihat *S-Box* pada gambar 4.4. beriku adalah hasil dari perubahan hasil atau *Sub-Bytes* :

$$\begin{bmatrix}62 & 75 & 7E & 7B\\ 64 & 71 & 10 & 7E\\ 65 & 63 & 71 & 7E\\ 64 & 71 & 62 & 71\end{bmatrix} \rightarrow \begin{bmatrix}AA & 9D & F3 & 21\\ 43 & A3 & CA & F3\\ 4D & FB & A3 & F3\\ 43 & A3 & AA & A3\end{bmatrix}$$

d. Proses *ShiftRows*

Proses memindahkan elemen pada kolom depan ke kolom paling belakang, untuk baris pertama tidak ada pemindahan, baris ke 2 pemindahan 1 kolom, baris ke 3 pemindahan 2 kolom, sedangkan baris ke 4 pemindahan 3 kolom dari proses data sebelumnya.

$$\begin{bmatrix}AA & 9D & F3 & 21\\ 43 & A3 & CA & F3\\ 4D & FB & A3 & F3\\ 43 & A3 & AA & A3\end{bmatrix} \rightarrow \begin{bmatrix}AA & 9D & F3 & 21\\ 43 & A3 & CA & F3\\ 4D & FB & A3 & F3\\ 43 & A3 & AA & A3\end{bmatrix}$$

$$\begin{bmatrix}AA & 9D & F3 & 21\\ 43 & A3 & CA & F3\\ 4D & FB & A3 & F3\\ 43 & A3 & AA & A3\end{bmatrix} \rightarrow \begin{bmatrix}AA & 9D & F3 & 21\\ A3 & CA & F3 & 43\\ 4D & FB & A3 & F3\\ 43 & A3 & AA & A3\end{bmatrix}$$

$$\begin{bmatrix} AA & 9D & F3 & 21 \\ 43 & A3 & CA & F3 \\ 4D & FB & A3 & F3 \\ 43 & A3 & AA & A3 \end{bmatrix} \rightarrow \begin{bmatrix} AA & 9D & F3 & 21 \\ 43 & A3 & CA & F3 \\ A3 & F3 & 4D & FB \\ 43 & A3 & AA & A3 \end{bmatrix}$$

$$\begin{bmatrix} AA & 9D & F3 & 21 \\ 43 & A3 & CA & F3 \\ 4D & FB & A3 & F3 \\ 43 & A3 & AA & A3 \end{bmatrix} \rightarrow \begin{bmatrix} AA & 9D & F3 & 21 \\ 43 & A3 & CA & F3 \\ 4D & FB & A3 & F3 \\ A3 & 43 & A3 & AA \end{bmatrix}$$

e. Proses *MixColumn*

Proses perkalian matriks dengan cara mengubah bentuk data hexadecimal ke dalam bentuk biner menggunakan operasi Xor dengan matriks yang sudah ditetapkan. Dibawah ini adalah matrik ketetapan pada metode rijndael. Nilai ini nantinya akan dikalikan dengan hasil akhir dari proses *shiftrows* sebelumnya.

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix}$$

Proses perhitungannya dengan mengambil kolom data pada proses sebelumnya dikalikan dengan matriks ketetapan pada tiap barisnya.

Hitung hasil dari semua kolom pada data yang telah dilakukan proses *MixColumn*, Dan seterusnya masing-masing baris dan juga kolom sampai semua dihitung. Sehingga didapatlah untuk hasil dari perhitungan tersebut sebagai berikut:

$$\begin{bmatrix} 1E & 44 & FD & 11 \\ 68 & D2 & 32 & E2 \\ BD & 32 & 43 & AA \\ C6 & 32 & DA & 2A \end{bmatrix}$$

Pada proses AddRoundKey() maka 128 bit dari hasil state akan di-XOR-kan dengan Kunci Ronde, yaitu kunci hasil dari proses Expand Key. Pada tahap awal enkripsi, 128 bit plaintext akan di-XOR-kan dengan kunci 128 bit yang asli. Kemudian 128 bit plaintext akan mengalami proses-proses SubBytes(), ShiftRows() dan MixColumns().

Pembahasan

Pada tahapan Implementasi sistem yang akan dibahas tentang tahapan-tahapan saat menjalankan sistem yang dibangun.

a. *Tampilan* Form Enkripsi Pesan

Pada tampilan form enkripsi pesan dirancang pertama untuk memilih kontak yang akan dituju kemudian membuat kunci yang akan dipakai dalam mengamankan pesan sebanyak 16 carakter dan selanjutnya menambahkan sebuah pesan sebanyak 160 karakter dan terakhir kirim ke nomor tujuan. Tampilan form enkripsi pesan dapat dilihat pada gambar di bawah ini:

Gambar 1 Tampilan form enkripsi pesan

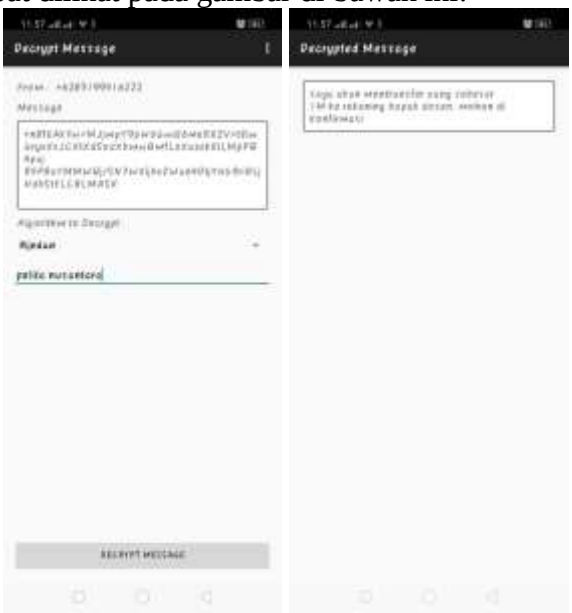
b. Tampilan *Inbox*

Pada tampilan inbox akan menampilkan sebuah pesan yang masuk dengan cara mengklik titik tiga [⋮] dan pilih inbox messege kemudian klik untuk melihat pesan yang sudah masuk. Berikut tampilan inbox pada gambar di bawah ini:

Gambar 2 Tampilan Inbox

c. Tampilan Form Dekripsi Pesan

Pada menu ini bertujuan untuk membuka pesan yang telah di kirim pada inbox sebelumnya dan kemudian memasukan kunci yang sama pada saat melakukan penguncian pesan. Berikut tampilan form dekripsi pesan dapat dilihat pada gambar di bawah ini:



Gambar 5.3 Tampilan Dekripsi Pesan

Kesimpulan

Adapun kesimpulan pada peneitian ini yaitu sebagai berikut :

Dalam merancang sebuah sistem dalam mengamankan data digital (dokumen) dibuat dengan menggunakan aplikasi Visual Studio 2019 dengan database yang digunakan adalah microsoft access dengan format (*.accdb) sebagai media penyimpanan user login dan kunci. Dengan menggunakan UML sebagai perancangan sistem juga design untuk perancangan antarmuka.

Pengamanan data digital dengan menerapkan algoritma RSA (Rivest Shamir Adleman) adalah sebagai suatu cara dalam mengamankan data, dikarena metode RSA yang memakai 2 (dua) buah kunci yaitu public key dan private key akan lebih dapat mengamankan data tersebut.

Kata pengantar

Dalam kesempatan ini penulis juga ingin menyampaikan terimakasih kepada Kedua Orang Tua saya atas kasih sayang yang diberikan kepada penulis serta doa, semangat, dukungan dan dorongan moril dan material sehingga skripsi ini dapat terselesaikan dengan baik. Dengan terselesaikan penyusunan skripsi ini dengan baik juga berkat dukungan dari banyak pihak, penulis mengucapkan terimakasih kepada berbagai pihak yang turut membantu dalam menyelesaikan skripsi ini baik secara langsung maupun secara tidak langsung.

Referensi

[1] E. H. Rachmawanto, C. A. Sari, and K. Kunci, “Keamanan File Menggunakan Teknik Kriptografi Shift Cipher,” *Jl. Nakula Semarang*, vol. 14, no. 50131024, pp. 329–335, 2015.

[2] Y. Prasetio and B. Triandi, “Perancangan Aplikasi Pengamanan File Teks dengan Skema Hybrid Menggunakan Algoritma Enigma dan Algoritma RSA Designing Application for Safeguarding Text Files with Hybrid Schemes Using Enigma Algorithms and RSA Algorithms,” *46. IT J.*, vol. 6, no. 1, pp. 2252–746, 2018.

[3] R. Siringoringo, “Analisis dan Implementasi Algoritma Rijndael (AES) dan Kriptografi RSA pada Pengamanan File,” *KAKIFIKOM Kumpul. Artik. Karya Ilm. Fak. ...*, vol. 02, no. 01, pp. 31–42, 2020, [Online]. Available: https://core.ac.uk/download/pdf/327176749.pdf.

[4] T. H. Saputro, N. H. Hidayati, and E. I. H. Ujianto, “Survei Tentang Algoritma Kriptografi Asimetris,” *J. Inform. Polinema*, vol. 6, no. 2, pp. 67–72, 2020, doi: 10.33795/jip.v6i2.345.

[5] K. D. R. Sianipar, S. W. Siahaan, M. Siregar, and I. Gunawan, “Pengamanan File Suara Menggunakan Kriptografi Algoritma Rijndael Dengan Proses Enkripsi Dan Dekripsi,” *TECHSI - J. Tek. Inform.*, vol. 11, no. 3, p. 431, 2019, doi: 10.29103/techsi.v11i3.1967.

[6] M. D. Irawan, “Implementasi Kriptografi Vigenere Cipher Dengan Php,” *J. Teknol. Inf.*, vol. 1, no. 1, p. 11, 2017, doi: 10.36294/jurti.v1i1.21.

[7] A. Utama and R. F. Siahaan, “Penerapan Kriptografi untuk Pengamanan Data

Transaksi Deposito pada Easy Tronik dengan Metode RC-5," *J. Ilmu Komput. dan Sist. ...*, vol. 3, no. 3, pp. 29–39, 2021, [Online]. Available: http://ejournal.sisfokomtek.org/index.php/jikom/article/view/86.

[8] A. Prayitno and N. Nurdin, "Analisa Dan Implementasi Kriptografi Pada Pesan Rahasia," *J. Elektron. Sist. Inf. dan Komput.*, vol. 3, no. 1, pp. 1–11, 2017, [Online]. Available: nnurdin69@gmail.com.

[9] S. Bandung, "SISTEM KEAMANAN SHORT MESSAGE SERVICE (SMS) MENGGUNAKAN," vol. 6, no. 2, pp. 5–10, 2017.

[10] I. Gunawan, "Pengamanan Acakan Biss Menggunakan Algoritma RSA," *Jurasik (Jurnal Ris. Sist. Inf. dan Tek. Inform.*, vol. 2, no. 1, p. 58, 2017, doi: 10.30645/jurasik.v2i1.19.