IMPLEMENTASI KRIPTOGRAFI RSA PADA APLIKASI CHAT BERBASIS ANDROID

Anisa Reski Pratiwi,[1)], Farniwati Fattah[2)], Dedy Atmajaya[3)]
[1)] *Mahasiswa Jurusan Teknik Informatika Universitas Muslim Indonesia, Makassar*
[2.3)] *Dosen Jurusan Teknik Informatika Universitas Muslin Indonesia, Makassar*

ABSTRACT

Technological advances have allowed millions of people to communicate with various hardware and software technologies. One of the development of software which is currently a massive means of communication used by the public is a messaging application. However, of the many messaging applications used in the community, not all of them apply cryptography security. The purpose of this study is to implement the RSA (revest shamir adleman method) method to secure text, and the AES (Advanced Encryption Standard) method for file and document message types by changing the extension in the messaging application. The process of implementing the RSA and AES methods, data that is sent first is encrypted by the sender and results in encrypted data which will then be sent to the recipient. When the recipient wants to access the message, the recipient must first enter a key to access the message. The result of this research is a SecretChat application that can be used to secure messages and has successfully implemented the RSA and AES methods.
Keywords: *Kriptografi, Rivest Shamir Adleman, Advanced Encryption Standard, Android*

1. PENDAHULUAN

Kemajuan di bidang komunikasi data dan jaringan komputer telah memungkinkan ribuan orang untuk melakukan komunikasi dengan beragam teknologi perangkat keras dan perangkat lunak. Disisi lain terdapat ancaman yang membayangi kemajuan tersebut, yaitu aspek keamanan data dan informasi. Sistem keamanan data diperlukan untuk melindungi data dan informasi yang ditransmisikan melalui jaringan komunikasi. Salah satu mekanisme untuk menyediakan layanan keamanan data adalah teknik kriptografi [1].

Kriptografi merupakan ilmu yang mempelajari teknik-teknik matematis yang berhubungan dengan aspek keamanan informasi seperti keabsahan, integritas serta autentifikasi data. Dimana pengirim akan mengirimkan pesan kepada si penerima, tetapi sebelum pesan tersebut dikirimkan ke server, pesan tersebut akan dienkripsikan menjadi sandi terlebih dahulu, kemudian sandi tersebut akan diteruskan ke penerima, dan terakhir penerima akan mendekripsikan sandi tersebut kembali menjadi pesan yang mengandung informasi [2].

Kriptografi memiliki banyak metode dalam mengenkripsi data diantaranya adalah Algoritma *Rivest Shamir Adleman* (RSA) yaitu algoritma yang mempunyai dua kunci yaitu kunci publik dan kunci pribadi. Kunci publik diketahui oleh siapa saja dan digunakan untuk enkripsi. Sedangkan kunci pribadi hanya pihak-pihak tertentu saja yang boleh mengetahuinya dan digunakan untuk dekripsi [3].

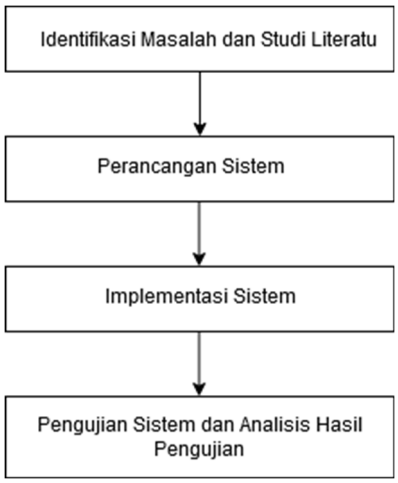
Android merupakan sistem operasi ponsel yang paling populer dan paling banyak digunakan saat ini. Sehingga keamanan ponsel android perlu ditingkatkan khususnya pada aplikasi *chatting* salah satu cara pertukaran informasi yang paling digemari adalah dengan melakukan *chatting* melalui ponsel. Selain praktis, *chatting* juga memungkinkan pengguna berkirim pesan di manapun dan kapanpun tanpa ada batasan wilayah dengan biaya yang relatif murah [4].

2. METODE PENELITIAN

Metode yang digunakan dalam penelitian ini adalah metode deskriptif yang menggunakan metode kepustakaan. Metode Kepustakaan ini dilakukan dengan cara mempelajari jurnal jurnal dan buku buku sebagai referensi sebagai sumber pembahasan mengenai enkripsi, aplikasi chatting, dan hal lain yang dibutuhkan [6].

Penelitian yang dilakukan, diselesaikan melalui tahapan penelitian yang terbagi dalam empat tahapan, yaitu: Identifikasi masalah dan studi literatur, Perancangan sistem, Implementasi sistem yaitu Perancangan aplikasi/program, dan Pengujian sistem serta analisis hasil pengujian.

[1]Korespondensi penulis: Anisa Reski Pratiwi, Telp 082291950783, anisareskipratiwi@gmail.com



Gambar 1. Tahapan penelitian

1. Identifikasi masalah dan studi literatur
   Mengidentifikasi masalah dan pengumpulan data, pada tahap ini dilakukan analisis tentang masalah yang terjadi pada layanan internet messaging, yaitu data percakapan yang dikirim dan diterima, dan melakukan pengumpulan data serta literatur mengenai chatting, kriptografi, proses enkripsi dan dekripsi data.
2. Perancangan sistem
   Merancang sistem yaitu proses yang terjadi di dalam sistem, serta rancangan antarmuka aplikasi yang digunakan oleh user.
3. Implementasi sistem
   Implementasi sistem, yaitu membuat aplikasi sesuai perancangan proses pada tahap kedua.
4. Pengujian sistem dan analisis hasil pengujian
   adalah melakukan pengujian sistem dan kemudian melakukan analisis terhadap hasil pengujian tersebut

RSA dibidang kriptografi merupakan algoritma kriptografi asimetris yang pengaplikasiannya menggunakan *public key* dan *privat key*. RSA masih digunakan secara luas oleh peneliti-peneliti lainnya, dan dipercaya dalam mengamankan dengan menggunakan kunci. Algoritma RSA menggunakan bilangan prima untuk mencari pembangkit kunci, dan dipilih secara acak [5].
Atribut-atribut penting pada algoritma RSA adalah sebagai berikut:

1. p dan q bilangan prima (rahasia)
2. $n = p \cdot q$ (tidak rahasia)
3. $\phi(n) = (p-1)(q-1)$ (rahasia)
4. e (kunci enkripsi) (tidak rahasia)
   Syarat: PBB(e, $\phi(n)$) = 1
5. d (kunci dekripsi) (rahasia)
   d dihitung dari $d \equiv e^{-1} \bmod (\phi(n))$
6. m (plainteks) (rahasia)
7. c (cipherteks) (tidak rahasia)

2.1 Algoritma RSA

1. Menentukan 2 bilangan prima, dengan nama p dan q. Misal nilai p = 47 dan q =71…….. (1)
2. Menghitung nilai modulus (n) : …….. (2)
   n = p×q
   n = 47 × 71
   n = 3.337
3. Menghitung nilai totient n :
   (n) = (p-1) × (q-1)……... (3)
   (n) = (47-1) × (71-1)
   (n) = (46 ×70)

(n) = 3.220

4. Menentukan nilai e dengan syarat e = bilangan prima
   Pilih kunci publik e adalah 79
5. Mencari nilai deciphering exponent (d), maka :..... (4)
   d = (1 + (k x (n)) / e)
   d = (1 + (k x 200)) / 79
   d = (1 + (22 x 3.220)) / 79
   d =1.019
   Nilai k merupakan sembarang angka untuk pencarian hingga dihasilkan suatu nilai integer atau bulat. Dengan mencoba nilai k = 1,2,..., hingga diperoleh nilai d yang bulat, yaitu d = . 1.019
6. Dari langkah-langkah yang sudah diuraikan sebelumnya, maka nilai n, e, dan d telah didapatkan sehingga pasangan kunci telah terbentuk.
   Pasangan kunci publik (n, e) = (3.337, 79)
   Pasangan kunci rahasia (n, d) = (3.337, 1.019)

Plaintext: Alhamdulillah kalau begitu

A=65	d=100	l=108	a=97	b=98	u=117
l=108	u=117	a=97	l=108	e=101	
h=104	l=108	h=104	a=97	g=103	
a=97	i=105	sp=32	u=117	i=105	
m=109	l=108	k=107	sp=32	t=1	

Enkripsi RSA

A = 65^{79} mod 3.337 = 541

l = 108^{79} mod 3.337 = 1795

h = 104^{79} mod 3.337 = 2893

a = 97^{79} mod 3.337 = 957

m = 109^{79} mod 3.337 = 1864

d = 100^{79} mod 3.337 = 1287

u = 117^{79} mod 3.337 = 2289

l = 108^{79} mod 3.337 = 1795

i = 105^{79} mod 3.337 = 193

l = 108^{79} mod 3.337 = 1795

l = 108^{79} mod 3.337 = 1795

a = 97^{79} mod 3.337 = 957

h = 104^{79} mod 3.337 = 2893

sp = 32^{79} mod 3.337 = 1379

k = 107^{79} mod 3.337 = 374

a = 97^{79} mod 3.337 = 957

l = 108^{79} mod 3.337 = 1719

a = 97^{79} mod 3.337 = 957

u = 117^{79} mod 3.337 = 2289

sp = 32^{79} mod 3.337 = 1379

b = 98^{79} mod 3.337 = 617

e = 101^{79} mod 3.337 = 1113

g = 103^{79} mod 3.337 = 101

i = 105^{79} mod 3.337 = 193

t = 116^{79} mod 3.337 = 1031

u = 117^{79} mod 3.337 = 2289

Dekripsi RSA

541^{1019} mod 3.337 = 65

1795^{1019} mod 3.337 = 108

2893^{1019} mod 3.337 = 104

957^{1019} mod 3.337 = 97

1864^{1019} mod 3.337 = 109

1287^{1019} mod 3.337 = 100

2289^{1019} mod 3.337 = 117

1795^{1019} mod 3.337 = 108

193^{1019} mod 3.337 = 105

1795^{1019} mod 3.337 = 108

1795^{1019} mod 3.337 = 108

957^{1019} mod 3.337 = 97

2893^{1019} mod 3.337 = 104

1379^{1019} mod 3.337 = 32

374^{1019} mod 3.337 = 107

957^{1019} mod 3.337 = 97

1719^{1019} mod 3.337 = 108

957^{1019} mod 3.337 = 97

2289^{1019} mod 3.337 =117

1379^{1019} mod 3.337 = 32

617^{1019} mod 3.337 = 98

1113^{1019} mod 3.337 = 101

101^{1019} mod 3.337 = 103

193^{1019} mod 3.337 = 105

1031^{1019} mod 3.337 = 116

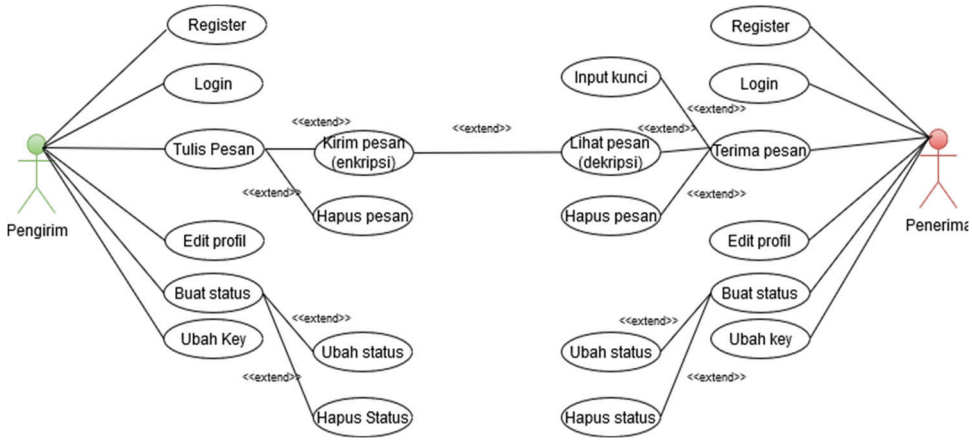
2289^{1019} mod 3.337 = 117

Jadi
541.1795.2893.957.1864.1287.2289.1795.193.1795.1795.957.2893.1379.374.957.1719.957.2289.1379.617.1113.101.193.1031.2289

jika dilihat pada tabel asci akan menghasilkan kata **"Alhamdullilah kalau begitu"**.

3. HASIL DAN PEMBAHASAN

Berdasarkan identifikasi aktor dan identifikasi diagram use case maka aktornya terdiri dari pengirim dan penerima. Adapun use case mengambarkan interaksi anatara aktor dengan sistem dapat dilihat pada gambar 1.



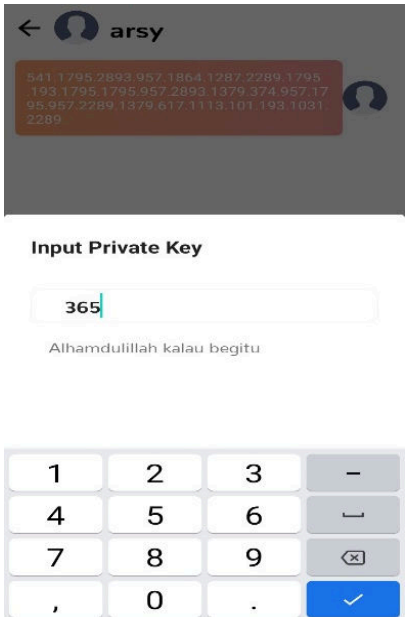
Gambar 2. Use Case SmartChat

Pengujian pada implementasi kriptografi RSA pada aplikasi chat berbasis android akan mengamankan teks, dokumen dan gambar. Jenis dokumen yang akan di enkripsi ialah .doc; .docx; .pdf; .ppt; dan .xls. Sedangkan jenis gambar yang akan di enkripsi adalah JPG, GIF, PNG. Pengujian sistem dilakukan untuk mengetahui apakah penelitian ini telah memenuhi tujuan untuk mengamankan teks, dokumen dan gambar menggunakan metode RSA. Pengujian sistem secara menyeluruh yaitu pengujian sistem pada aplikasi yang akan digunakan oleh admin dari segi tampilan dan segi proses yang terjadi di setiap halaman dan selanjutnya

melakukan proses enkripsi dan dekripsi pesan dengan menerapkan kunci pengirim (e, d) = (29, 365) dan kunci penerima (e, d) = (2=79, 1015).

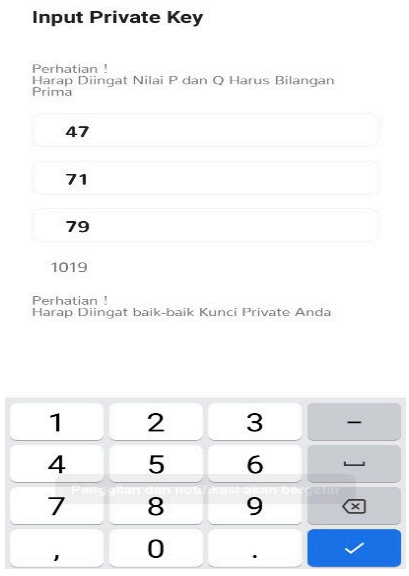
Pengirim

Gambar 3. Kunci Pengirim

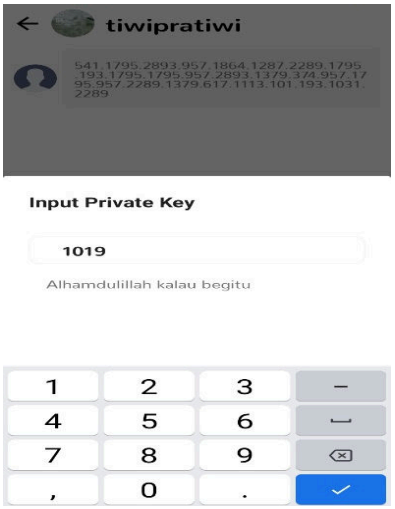


Gambar 4. Pesan Pengirim

Penerima



Gambar 5. Kunci Penerima



Gambar 6. Pesan yang di terima

Pengujian Kecepatan Enkripsi dan dekripsi

Tabel 1. Kecepatan enkripsi dan dekripsi

Jumlah (karakter)	Waktu (milisekon)	
	Enkripsi	Dekripsi
40	12	77
1280	97	3483
20250	623	9351
40710	1962	15794

4. KESIMPULAN

1. Penelitian ini berhasil merancang aplikasi *SecretChat* berbasis android yang dapat dijadikan suatu sistem untuk mengamankan pesan. Pesannya berupa pesan teks, dokumen dan gambar.
2. Penelitian ini berhasil mengimplementasikan *kriptografi* menggunakan algoritma RSA (*Rhavist Shamir Adleman*) untuk menciptakan suatu aplikasi atau sistem keamanan pada pesan berbasis android.
3. Untuk mengenkripsi dan dekripsi pesan teks metode algoritma yang digunakan adalah RSA, didapatkan hasil pegujian waktu yang dibutuhkan untuk proses dekripsi lebih lama daripada proses enkripsi. Sedangkan untuk mengenkripsi dokumen dan gambar menggunakan pengabungan 2 metode yaitu algoritma RSA dan AES dengan cara mengubah esktensinya.

5. DAFTAR PUSTAKA

[1] Agustina, a. n., Aryanti, & Nasron, "pengamanan dokumen menggunakan metode rsa (rivest shamir adleman) berbasis web", UNISBANK, vol.SU-3, pp.14–19, (2017).

[2] Utara, u. s, "playfair cipher dan algoritma kompresi run length encoding dalam pengamanan dan kompresi data teks" (2016).

[3] Kurniawan, s. t. c., dedih, d., & supriyadi, s.. "implementasi kriptografi algoritma rivest shamir adleman dengan playfair cipher pada pesan teks berbasis android". jurnal online informatika, vol.2, no.2, pp.102-109, Desember (2017).

[4] Patra Abdala, 2017." implementasi algoritma kriptografi vernam cipher dan algoritma des (data encryption standard) pada aplikasi chatting berbasis android". skripsi. FIKOM, Universitas Sumatera Utara, Medan.

[5] Amin, m. m.. "komunikasi berbasis teks". jurnal pseudocode, vol.iii, no.2, pp.129–136 (september) (2016).

[6] Fadhlurrahman," Aplikasi Chatting Notaris Berbasis Android Dengan", SKANIKA, vol 1, no.1, pp. 656-661, Mei 2018.

6. UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Fakultas Ilmu Komputer Universitas Muslim Indonesia serta bapak Dedy Atmajaya,S Kom.,M.Eng dan ibu Farniwati Fattah, S.T.,M.T atas dukungan dan bimbingannya sehingga dapat menyelesaikan penelitiaan ini dengan baik.