PENGGUNAAN HYBRID CRYPTOSYSTEM UNTUK ENKRIPSI DAN DEKRIPSI PESAN *MESSANGER* MENGGUNAKAN ALGORITMA *RIVEST SHAMIR ADLEMAN* (RSA) DAN *ADVANCED ENCRYPTION STANDARD* (AES) DENGAN FIREBASE PADA ANDROID

Ahmad Pudoli[1], Dewi Kusumaningsih[2]

[1, 2)] Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur
Jl. Raya Ciledug, Petukangan Utara, Pesanggrahan, Jakarta Selatan 12260
Telp. (021) 5853753, Fax. (021) 5853752
[1]ahmad.pudoli45@gmail.com, [2]dewi.kusumaningsih@budiluhur.ac.id

ABSTRAK

Perkembangan Teknologi Informasi membuat seseorang dengan mudah mendapatkan informasi, dan komunikasi juga dapat dilakukan dimanapun dan kapanpun. Dalam perkembangan untuk melakukan komunikasi bukan hanya dengan telpon atau SMS, tetapi juga layanan Messenger. Aplikasi messenger pada awalnya berbasis desktop, namun sekarang sudah bergeser berbasis perangkat bergerak (mobile). Beberapa aplikasi messanger sudah menerapkan pengamanan namun ada juga yang belum menggunakan pengamanan. Jika ada seseorang melakukan serangan contohnya sniffing, maka dapat dengan mudah pesan dapat dibaca. Hal ini dapat merugikan pengguna, terlebih pesan tersebut bersifat rahasia. Untuk mengantisipasi agar pesan tidak mudah dibaca oleh orang yang tidak berhak, maka perlu dibuat sistem pengamanan pada pesan tersebut. Salah satu cara untuk melakukan pengamanan tersebut adalah dengan enkripsi. Banyak teknik kriptografi yang dapat digunakan. Pada penelitian ini, digunakan Hybrid Cryptosystem dengan kombinasi RSA dan AES. Untuk menjaga keabsahan dari pesan yang dikirim perlu ditambahkan teknik error detection yang dalam hal ini menggunakan hash function. Pada penelitian ini menghasilkan aplikasi yang dapat memberikan keamanan pesan dengan memenuhi seluruh aspek keamanan informasi yang meliputi kerahasiaan, integritas, dan otentikasi.

Kata Kunci : Kriptografi, *Hybrid Cryptosystem, RSA, AES*

I. PENDAHULUAN

1.1. Latar Belakang

Dalam perkembangannya untuk melakukan komunikasi bukan hanya dengan telpon atau SMS, tetapi juga layanan *messanger*. Layanan *messanger* ini ada yang dapat digunakan secara gratis maupun berbayar. Pada umumnya layanan *messanger* memerlukan jaringan internet untuk dapat saling terhubung.Kriptografi merupakan salah satu teknik untuk melakukan penyandian pesan sehingga pesan tidak mudah dibaca. Penelitian ini fokus pada pembuatan layanan *messager* berbasi android dengan menggunakan fitur firebase, untuk memberikan solusi keamanan pesan pada *messager,* maka pesan yang dikirim pada layanan tersebut dilakukan pengamanan, sehingga jika dilakukan *snifing* oleh seseorang maka pesan dapat tidak dapat dibaca. Jika tidak dilakukan pengamanan akan sangat merugikan bagi pemilik pesan, terlebih pesan tersebut bersifat rahasia. Teknik yang digunakan untuk melakukan pengamanan pesan dapat dilakukan dengan *Hybrid Cryptosystem*. Alasan penggunaan teknik *Hybrid Cryptosystem* karena keamanan dan efisiensi [1].

1.2. Rumusan Masalah

"Bagaimana menerapkan metode *Hybrid Cyptosystem* untuk memberikan keamanan pesan dengan memenuhi seluruh aspek keamanan informasi yang meliputi kerahasiaan, intergritas data, dan otentikasi pada aplikasi *messenger* dengan prototipe berbasis Android?"

1.3. Tujuan Penelitian

Tujuan penelitian ini adalah sebagai berikut:

a. Membuat prototipe pengamanan pesan pada aplikasi *messenger* pada *mobile device* berbasis Android menggunakan *firebase* dengan menggunakan metode *Hybrid Cryptosystem,* yaitu menggunakan kombinasi RSA dan AES.
b. Membuat *hash* yang digunakan sebagai validasi dan verifikasi untuk memastikan pesan masih asli atau belum pernah diubah oleh orang yang tidak berhak.

II. LANDASAN TEORI

2.1. Kriptografi

Kriptografi merupakan sebuah seni perlindungan keamanan pesan rahasia dengan mengacaukan dan menyandikan pesan rahasia menjadi kode-kode rahasia atau *ciphertext*[2]. Tujuan utama penggunaan teknik kriptografi dalam pengiriman pesan rahasia terbagi menjadi beberapa poin-poin penting, yaitu [3]:

a. *Confidentialy* (Kerahasiaan), merupakan hal paling penting. Dipastikan bahwa pesan yang dikirimkan hanya bisa dimengerti oleh pengirim maupun penerima yang

telah memiliki kunci untuk membuka pesan rahasia. Dalam hal ini dipastikan selain pengirim dan penerima pesan tidak seorangpun dapat mengerti pesan rahasia tersebut.

b. *Authentication* (keaslian), merupakan proses pembuktian identitas yang menjamin keamanan komunikasi dalam pengiriman pesan rahasia. Pengguna dan sistem dapat membuktikan identitas yang mereka miliki berhak untuk membuka pesan rahasia tersebut.
c. *Data integrity* (integritas data), dipastikan bahwa data yang diterima adalah data yang sama dengan data yang dikirimkan dan tidak ada perubahan data.
d. *Non- Repudiation* (anti penyangkalan), mencegah pihak pengirim pesan tidak mengakui bahwa telah mengirimkan sebuah pesan rahasia.
e. *Access Control* (kendali akses), proses yang digunakan untuk pencegahan penggunaan yang tidak sah dari sumber daya.

2.2. RSA (*Rivest-Shamir-Adleman*)

RSA menggunakan variable ukuran enkripsi blok dan ukuran kunci variabel. Dalam penggunaannya untuk otentikasi, server mengimplementasikan *public key* dengan *client* dengan memberikan *signature* pada pesan dengan menggunakan *private key*. Kemudian signature tersebut dikembalikan ke *client* selanjutnya diverifikasi dengan menggunakan *public key* yang diketahui *server*[4].

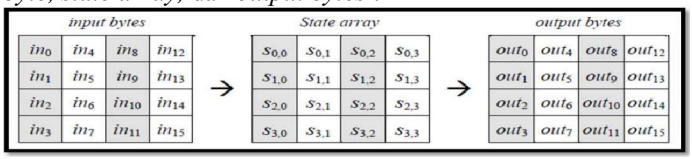
Sebelum melakukan enkripsi dan dekripsi dengan menggunakan RSA, terlebih dahulu membuat *public key* dan *private key*. Berikut algoritma untuk melakukan enkripsi dan dekripsi pada RSA(Samni,2007):

a. Memilih dua buah bilangan prima yang diberi p dan q (disarankan untuk memilih bilangan yang besar)
b. Menghitung nilai n = p . q
c. Kemudian menghitung nilai Φ (n)= (p – 1) . (q – 1), dimana Φ (n) adalah *Euler totient* dari n yaitu bilangan positif kurang dari n dan relatif prima dengan n (gcd Φ (n) dan n sama dengan 1).
d. Cari bilangan e, yang relatif prima terhadap Φ (n) dan harus lebih kecil dari Φ (n).
e. Hitung d dimana d = e^{-1}mod Φ (n) atau e*d mod Φ (n) = 1.
f. Untuk melakukan enkripsiyaitu n dan e dimana C = P^e mod n.
g. Untuk melakukan dekripsi yaitu n dan d dimana P = C^d mod n.

2.3. AES (*Advance Encryption Standard)*

Pada tahun 2001, Algoritma Rijndael, karya peneliti dari universitas di Belgia ditetapkan menjadi AES. Rijndael merupakan algoritma yang dapat menerima masukan data 128 bit dan menghasilkan data 128 bit pula. Urutan data yang sudah terbentuk dalam satu kelompok 128 *bit* tersebut disebut juga sebagai blok data atau dengan panjang 128 *bit,* 192 *bit,* atau 256 *bit.* Perbedaan AES panjang kunci akan mempengaruhi jumlah *around* yang akan diimplementasikan pada algoritma AES ini [6].

Gambar 1 mengilustrasikan proses penyalinan dari *input byte, state array,* dan *output bytes* :



Gambar 1 : Prosees Input Btye, State Array, dan Output Bytes[7]

2.4. *Hybrid Cryptosystem*

Hybrid Cryptograph merupakan teknik kriptografi dengan menggunakan dua atau lebih *cipher* yang berbeda dalam waktu bersamaan. Sedangkan *Hybrid Cryptosystem* dibangun dengan menggunakan dua atau lebih kriptografi yang terpisah. Pada *Hybrid Cryptosystem* untuk melakukan enkripsi atau dekripsi pesan yang panjang akan efisien dengan menggunakan *symetryc-key*. Sedangkan kunci publik hanya digunakan untuk mengenkripsi/mendekripsi kunci simetris yang pendek[1].

2.5. Sistem Operasi Android

Android merupakan sistem operasi berbasi Linux yang digunakan oleh *mobile device* misalnya seperti *smartphone*. Pada sistem operasi *Android* diberi hak penuh untuk menciptakan aplikasi mereka sendiri. Berikut ini merupakan kelebihan sistem operasi *Android*,yaitu:

a. Sistem Operasi bersifat *open source*, jadi sangat memungkinkan penggunanya untuk membuat software sendiri.
b. Banyak aplikasi baik *software* maupun *game* yang bisa kita nikmati mulai dari yang berbayar sampai gratis.
c. Dari segi tampilan, terlihat elegant, sehingga penggunanya tidak akan mudah bosan.
d. Bersifat *Multitasking* yang artinya bisa menjalankan berbagai aplikasi sekaligus

2.6. Tinjauan Studi

Tinjauan studi yang dijadikan acuan dalam melakukan penelitian ini mengacu pada beberapa penelitian terkait yang telah dilakukan sebelumnya yaitu sebagai berikut.

a. Jigar Chauhan, Neekhil Dedhia dan Bhagyashri Kulkarni melakukan penelitian tentang *Hybrid Cryptograph* dengan menggunakan AES-DES. Pada penelitian ini mengusulkan metode pengamanan data dengan merancang konsep gabungan AES dan DES untuk mendapatkan model *hybrid* agar dapat digunakan untuk semua jenis data. Dengan menggunakan model *hybrid* AES-DES didapatkan difusi yang lebih baik. Oleh karena itu dengan menggunakan model ini serangan dapat diminimalisir. Model *hybrid* AES-DES membutuhkan proses yang lebih dibandingkan AES atau DES saja, dengan demikian waktu yang digunakan *hybrid* AES-DES untuk melakukan enkripsi dan dekripsi jauh lebih besar. Namun membutuhkan waktu yang lama oleh kriptanalis untuk memecahkan *cipher*[8].

b. Penelitian tentang pengulangan enkripsi pada RSA yang dilakukan oleh Anjana S. Chandran mengatakan RSA masih menjadi algoritma yang kuat dari*public key cryptosystem*. Namun terjadi sebuah kasus pada saat melakukan enkripsi *plaintext* dengan *key* yang merupakan bilangan kecil secara berulang akan mendapatkan kembali *plaintext*-nya. Oleh karena itu untuk menghindari kasus seperti itu *key* yang digunakan pada RSA harus bilangan bulat yang besar, sehingga sulit mendapatkan *plaintext* kembali jika *ciphertext*di enkripsi secara berulang[9].

c. Anjali Patil dan Rajeshwari Goudar melakukan studi literatur perbandingan antara kriptografi yang berbeda untuk perangkat *wireless*. Pada penelitian ini memberikan rincian tentang algoritma simetris seperti *Vigenere*, DES, 3DES, AES, *Blowfish* dan algoritma asimetris seperti RSA, DH dan lainnya. Hasil evaluasi yang didapat bahwa *memory* yang digunakan oleh algoritma simetris lebih sedikit dibandingkan dengan asimetris. Dan algoritma simetris berjalan lebih cepat daripada algoritma asimetris

d. Mansoor Ebrahim, Shujaat Khan dan Umer Bin Khalid melakukan analisis kinerja algoritma kriptografi simetris yang berbeda. Pada penelitian ini melakukan evaluasi jenis-jenis algoritma kriptografi simetris dengan melakukan penilaian algoritma yang berbeda berdasarkan parameter yang dibutuhkan. Selama analisis ini diamati bahwa AES (Rijndael) adalah yang terbaik diantara semua dalam hal keamanan, Fleksibilitas, penggunaan memori, dan kinerja Enkripsi[10].

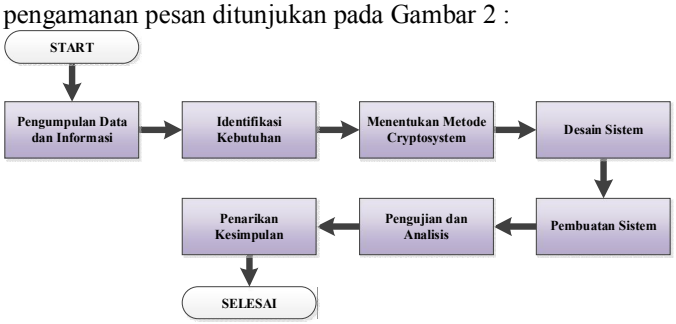
III. ANALISIS DAN RANCANGAN PROGRAM

3.1 *Metode Penelitian*

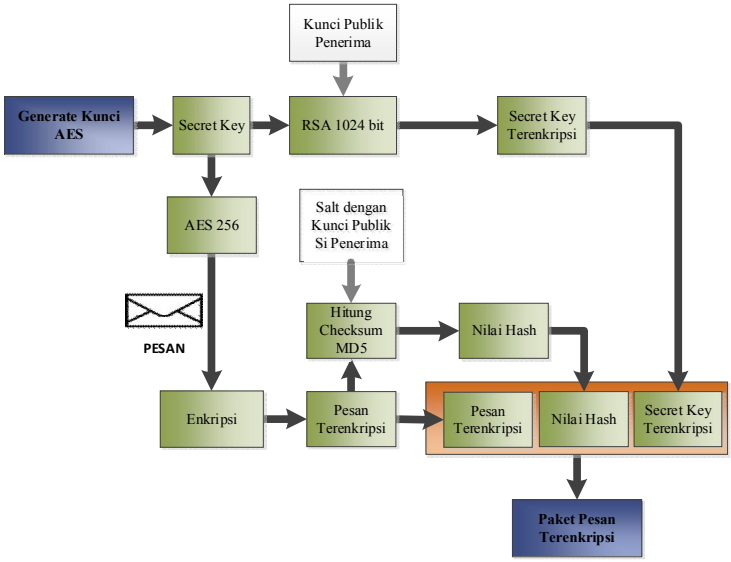
Berdasarkan tujuan tersebut, metode penelitian yang digunakan dalam penelitian ini adalah metode penelitian eksperimen. Penelitian eksperimen merupakan penelitian dimana peneliti dapat melakukan manipulasi kondisi yang ada sesuai dengan keinginan peneliti, dalam kondisi yang telah dimanipulasi ini biasanya dibuat dua kelompok yaitu kelompok kontrol dan kelompok pembanding.

3.2 *Langkah-langkah Penelitian*

Tahapan yang dilakukan dalam rangka melakukan penelitian pengembangan prototipe layanan *chatting* dengan pengamanan pesan ditunjukan pada Gambar 2 :



Gambar 2: Langkah-langkah Penelitian



Gambar 3: Desain Enkripsi dengan Hybrid Cryptosystem Usulan

Gambar 3 merupakan blok diagram proses enkripsi yang dibangun. Dimulai dari *Generate Key* sampai mendapatkan paket pesan yang terenkripsi. Berikut ini algoritma yang menjelaskan alur proses yang terdapat pada Gambar 3:

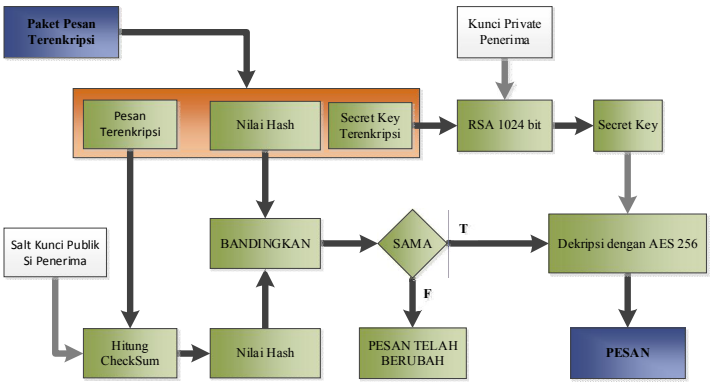
a. Melakukan *Generate Key* untuk mendapatkan kunci AES 256. Kunci tersebut selanjutkan menjadi *Secret Key*.

b. Pesan dienkripsi dengan menggunakan AES 256. Pada proses enkripsi ini menggunakan kunci yang di-*generate* pada tahap sebelumnya *(secret key)*.

c. Setelah pesan dienkripsi maka proses selanjutnya menghitung nilai *checksum*-nya dengan menggunakan *Message Digest 5 (MD5)*. Pada proses ini ditambahkan *salt* dengan menggunakan kunci publik penerima.

d. Enkripsi *Secret Key* (kunci AES 256) dengan Algoritma RSA, dimana dengan menggunakan kunci publik penerima pesan.

e. Membuat paket pesan terenkripsi dengan menggabungkan *hash,* kunci terenkripsi dan pesan yang terenkripsi.



Gambar 4 : Desain Dekripsi dengan Hybrid ryptosystem Usulan

Pada Gambar 4 merupakan blok diagram proses dekripsi yang dibangun. Dimulai dari memisahkan pesan yang

terenkripsi sampai mendapatkan pesan asli. Berikut ini algoritma yang menjelaskan alur proses yang terdapat pada Gambar 4:

a. Memisahkan paket pesan terenkripsi sehingga masing-masing menjadi *hash*, kunci terenkripsi dan pesan terenkripsi.
b. Hitung nilai *hash* pesan terenkripsi menggunakan *Checksum* MD5. Pada proses ini ditambahkan *salt* dengan menggunakan kunci publik penerima, kemudian bandingkan dengan nilai *hash* yang disimpan.
c. Jika nilai *hash* sama, maka *secret key* yang dienkripsi dengan RSA didekripsi dengan menggunakan *private key* si penerima. Nanti akan mendapatkan *Secret Key* (kunci AES 256) untuk melakukan dekripsi *AES 256*.
d. Setelah mendapatkan kunci AES 256, maka dekripsi pesan dengan menggunakan AES 256

IV. HASIL DAN UJI COBA

4.1 *Kebutuhan Sistem*

Berikut spesifikasi perangkat pendukung yang penulis gunakan untuk membuat program ini :

A. Perangkat Keras *(Hardware)*

Pada saat aplikasi ini dibuat, penulis menggunakan *Handphone* Xiaomi Redmi 3 Pro sebagai demo aplikasi. Di bawah ini merupakan spesifikasi *Handphone* Xiaomi Redmi 3 Pro yang digunakan dalam demo aplikasi:

1) *Processor* Snapdragon 616 dengan Octa-core (4x1,5 GHz Cortex-A53 dan 4x1,2 GHz Cortex-A53)
2) RAM 3 GB
3) Memori Internal 32 GB

Di bawah ini merupakan spesifikasi komputer yang digunakan penulis dalam membangun dan pengujian aplikasi ini sehingga dapat berjalan dengan baik:

1) *Processor* AMD A10-5745M APU
2) RAM 8 GB
3) *Harddisk* 500 GB

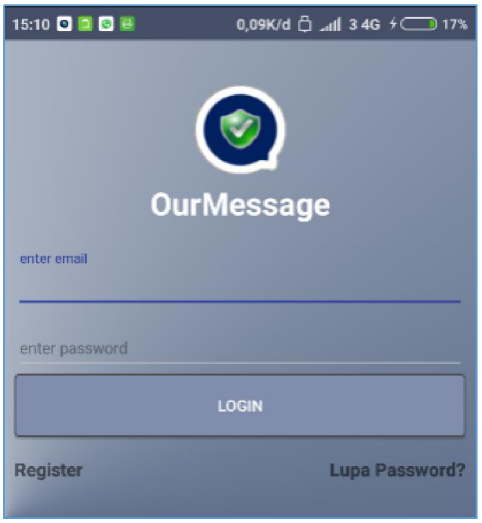
B. Perangkat Lunak *(Software)*

Dibawah ini merupakan spesifikasi *software* yang ter-*install* pada *handphone* yang penulis gunakan untuk menjalankan dan pengujian aplikasi ini sehingga aplikasi dapat berjalan dengan baik.

1) Android *Lollipop* Versi 5.1
2) ROM atau *Operating System* MIUI Global 8.5 Stabil 8.5.1.0 (LAIMIED)
3) Vysor untuk pengujian anti-*screenshoot*

4.2 *Tampilan Layar*

A. Tampilan Layar Menu *Login*

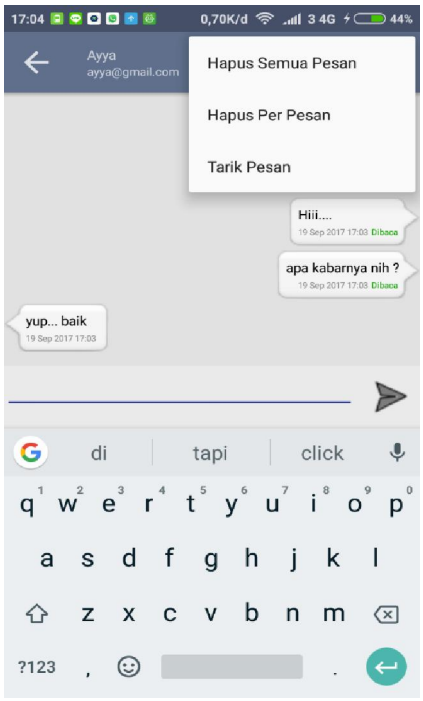


Gambar 5 : Tampilan Layar Halaman Login

B. Tampilan Layar Menu Utama

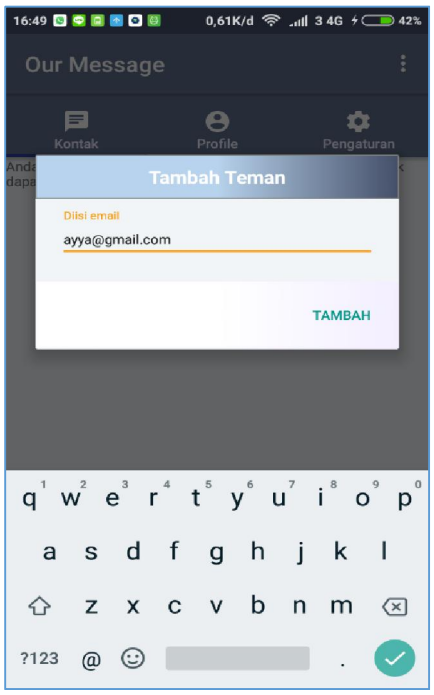
Gambar 6: Tampilan Layar Menu Utama

C. Tampilan Layar Menu *Chat*



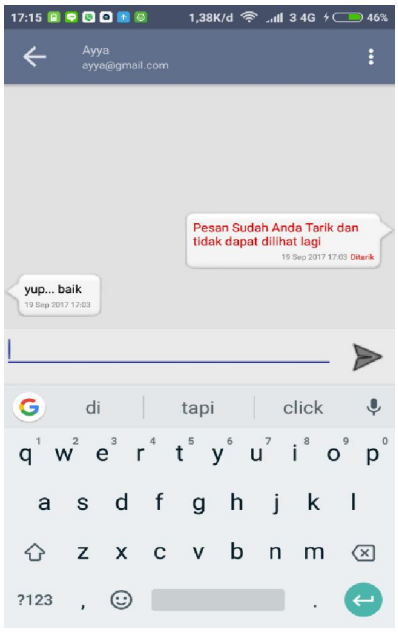
Gambar 7 : Tampilan Layar Menu Chat

D. Tampilan Layar Tambah Teman



Gambar 8 : Tampilan Layar Tambah Teman

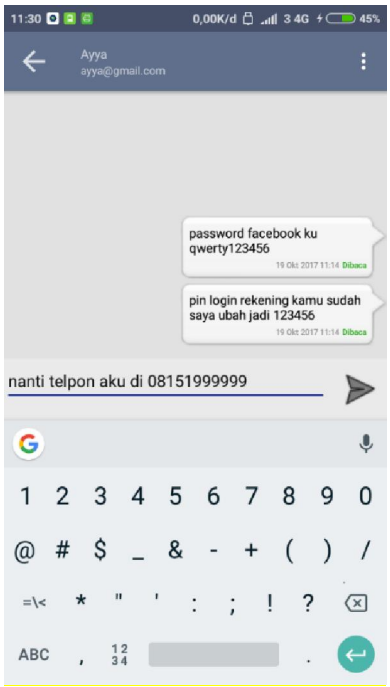
E. Tampilan Layar Tarik Pesan



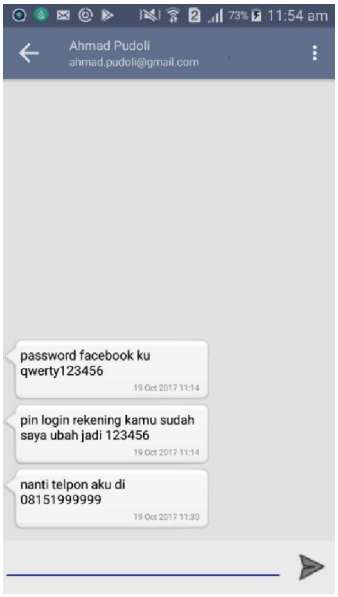
Gambar 9 : Tampilan Layar Tarik Pesan

4.3 *Pengujian Program*

Percobaan dilakukan dengan mengirimkan pesan melalui aplikasi, kemudian pesan yang dikirim dilihat pada *platform firebase*. Tujuan dari pengujian ini adalah untuk membuktikan bahwa metode yang diusulkan tersebut dapat memenuhi semua aspek keamanan informasi. Yaitu kerahasiaan, integritas data, dan otentikasi. Selain itu, pengujian juga dilakukan terhadap fitur anti *screenshot.*



Gambar 10 : Pengujian Mengirim Pesan Ke Teman Pengujian dari Pengirim



Gambar 10 : Pengujian Mengirim Pesan Ke Teman Pengujian dari Penerima

Tabel 1 : Hasil Uji Kerahasiaan Data Pada Pesan

No	Pesan Pada Aplikasi	Pesan Pada Platform Firebase
1	password facebook ku qwerty123456	1p893H+1jCYhvHA098UHSvgjYg6apliheQU5BFN+Ey3DUBmxqJy2OA/kx9FehIgy\
2	pin login rekening kamu diubah jadi 123456	cLIHbDVoBxev1ZNuOZyoBGsmG2UpUFqZEF770jT78pRI1GQacy1kN4sZCwC3UCThtauvyoQRi4zDHot14/kV2g==
3	nanti telpon aku di 08151999999	lPR38zoARLuJL2/tNtzgKc8bHFkKfN2hlvT1wxwD+jM=

Tabel 2 : Informasi Pesan Terenkripsi, Hash, dan Hasil Dekripsi Pesan

No	Pesan Pada Platform Firebase	Message Diggest	Hasil Dekripsi Pesan pada Aplikasi	Keterangan
1	1p893H+1jCYhvHA098UHSvgjYg6apliheQU5BFN+Ey3DUBmxqJy2OA/kx9FehIgy\	2452fe8252b173053b2fa555712c6e5a	Password facebook ku qwerty123456	Data valid
2	cLIHbDVoBxev1ZNuOZyoBGsmG2UpUFqZEF770jT78pRI1GQacy1kN4sZCwC3UCThtauvyoQRi4zDHot14/kV2g==	5ee6e33dc4ab8c6f04168fb4193ddf6d	pin login rekening kamu diubah jadi 123456	Data valid
3	lPR38zoARLuJL2/tNtzgKc8bHFkKfN2hlvT1wxwD+jM=	2c6aafc4adcd89286a2515946ee2aac4	Nanti telpon aku di 081519999999	Data valid

V. PENUTUP

5.1 Kesimpulan

Dari hasil perancangan dan percobaan aplikasi ini. Dapat diambil kesimpulan sebagai berikut:

a. Dengan adanya aplikasi kriptografi, tingkat privasi pesan menjadi lebih aman dari pihak yang tidak bertanggung jawab.
b. Metode *Hybrid Cryptosystem* dengan kombinasi RSA dan AES dapat di implementasikan pada aplikasi pengamanan pesan. Serta dapat digunakan untuk memberikan keamanan data dengan meliputi aspek kerahasiaan, integritas data, dan otentikasi.
c. Aplikasi dapat meminimalisir tingkat kebocoran informasi pesan oleh pihak yang tidak berhak yang disebabkan oleh *human error* yang mengakibatkan kerugian untuk perusahaan.

5.2 Saran

Aplikasi chatting ini masih memiliki beberapa keterbatasan dan kekurangan, sehingga untuk itu penulis menyarankan untuk pengembangan aplikasi selanjutnya agar:

a. Aplikasi dapat berjalan cepat
b. Menyempurnakan beberapa fitur di aplikasi seperti penambahan gambar profil pengguna dan dapat melampirkan file, foto, serta video dan membuat Group chat.

DAFTAR PUSTAKA

[1] Gupta, Ravindra Kumar andParvinder Singh. "A New Way to Design and Implementation of Hybrid Cryptosystem for Security of The Information in Public Network". *International Journal of Emerging Technology and Advanced Engineering,* Vol. 3, Agustus 2013.

[2] Gutub, Adnan Abdul-Aziz. "Pixel Indicator Technique for RGB Image Steganography". *Journal of Emerging Technologies in Web Intelligence,* Vol.2, No.1, Februari 2010.

[3] Abutaha, Mohammed, et.al. "Cryptography is The Science of Information Security",*Communication Theory of Secrecy Systems*, Vol.5, No.3, Juli 2011.

[4] Seth, Shashi Mehrotra and Rajan Mishra. "Comparative Analysis Encryption Algorithms For Data Communication". *International Journal of Computer Science and Technology (IJCST),* Vol. 2, No. 2, Juni 2011.

[5] Lukas, Samuel and Ni Putu Sri Artati. "Analisis Waktu Enkripsi-Dekripsi File Text Menggunakan Metoda One-Time Pada (OTP) dan Rivest, Shamir,

Adleman (RSA)". *Seminar Nasional Sistem dan Informatika,* November 2007.

[6] Hendra and Sukiman. "Aplikasi Pengaman Pertukaran SMS pada Perangkat Android dengan Metode RSA". *Seminar Nasional Teknologi Informasi dan Komunikasi (SNASTIKOM),* 2012.

[7] Didi, Surian, "Algoritma Kriptografi AES Rijndael", *Jurnal Teknik Elektro, TESLA* Vol.8, No.2, 97-101, Oktober 2006.

[8] Jigar, et.al. "Enhancing Data Security by using Hybrid Cryptography Algorithm". *International Journal of Engineering Science and Innovative Technology (IJESIT),* Vol. 2, No. 3, Mei 2013.

[9] Anjana S,Chandran,. "Repeated Encryption on RSA", *International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE),* Vol. 4, No. 4, April 2014.

[10] Mansoor, Ebraheem. et.al. "Symetric Algorithm Survey: A Comparative Analysis". *International Journal of Applications,* Vol. 61, No. 20, Januari 2013.