PENINGKATAN KEAMANAN GRUP *CHAT* MENGGUNAKAN KOMBINASI METODE RSA, *ELGAMAL* DAN *VIGINERE CIPHER*

SKRIPSI

Oleh :

DWI RISKY SETIAWAN
NIM. 15650009

JURUSAN TEKNIK INFORMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM MALANG

2019

PENINGKARAN KEAMANAN GRUP *CHAT* MENGGUNAKAN KOMBINASI METODE RSA, *ELGAMAL* DAN *VIGINERE CIPHER*

SKRIPSI

Diajukan kepada:
Universitas Islam Negeri (UIN) Maulana Malik Ibrahim Malang
Untuk Memenuhi Salah Satu Persyaratan Dalam
Memperoleh Gelar Sarjana Komputer (S.Kom)

Oleh:

DWI RISKY SETIAWAN
NIM. 15650009

JURUSAN TEKNIK INFORMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM MALANG
2019

LEMBER PERSETUJUAN

PENINGKATAN KEAMANAN GRUP CHAT MENGGUNAKAN KOMBINASI METODE RSA, *ELGAMAL* DAN *VIGINERE CIPHER*

SKRIPSI

Oleh :

DWI RISKY SETIAWAN
NIM. 15650009

Telah Diperiksa dan Disetujui untuk Diuji

Tanggal : 6 Desember 2019

Dosen Pembimbing I	Dosen Pembimbing II
Dr. Cahyo Cysdian	Ajib Hanani, MT
NIP. 19740424 200901 1 008	NIDT. 19840731 2016081 1 076

Mengetahui,
Ketua Jurusan Teknik Informatika
Fakultas Sains dan Teknologi
Universitas Islam Negeri Maulana Malik Ibrahim Malang

Dr. Cahyo Crysdian
NIP. 19740424 200901 1 008

LEMBAR PENGESAHAN

PENINGKARAN KEAMANAN GRUP CHAT MENGGUNAKAN KOMBINASI METODE RSA, *ELGAMAL* DAN *VIGINERE CIPHER*

SKRIPSI

Oleh:
DWI RISKY SETIAWAN
NIM. 15650009

Telah Dipertahankan di Depan Dewan Penguji
dan Dinyatakan Diterima Sebagai Salah Satu Persyaratan
untuk Memperoleh Gelar Sarjana Komputer (S.Kom)
Pada Tanggal 6 Desember 2019

Susunan Dewan Penguji			**Tanda tangan**
1. Penguji Utama	:	Khadijah F.H. Holle, M. Kom NIDT. 19900626 20160801 2 077	( )
2. Ketua Penguji	:	Irwan Budi Santoso, M.Kom NIP. 19770103 201101 1 004	( )
3. Sekretaris Penguji	:	Dr. Cahyo Crysdian NIP. 19740424 200901 1 008	( )
4. Anggota Penguji	:	Ajib Hanani, MT NIDT. 19840731 20160801 1 076	( )

Mengetahui,
Ketua Jurusan Teknik Informatika
Fakultas Sains dan Teknologi
Universitas Islam Negeri Maulana Malik Ibrahim Malang

Dr. Cahyo Crysdian
NIP. 19740424 200901 1 008

PERNYATAAN KEASLIAN TULISAN

Saya yang bertanda tangan dibawah ini:

Nama : Dwi Risky Setiawan
NIM : 15650009
Fakultas/Jurusan : *Sains dan Teknologi/Teknik Infomatika*
Judul Skripsi : Peningkaran Keamanan Grup *Chat* Menggunakan Kombinasi Metode RSA, *Elgamal* dan *Viginere Cipher*

Menyatakan dengan sebenarnya bahwa Skripsi yang saya tulis ini benar-benar merupakan hasil karya sendiri, bukan merupakan pengambilalihan data, tulisan atau pikiran orang lain yang saya akui sebagai hasil tulisan atau pikiran saya sendiri, kecuali dengan mencantumkan sumber cuplikan pada daftar pustaka.

Apabila dikemudian hari terbukti atau dapat dibuktikan Skripsi ini hasil jiplakan, maka saya bersedia menerima sanksi atas perbuatan tersebut.

Malang, 6 Desember 2019
Yang membuat pernyataan,

Dwi Risky Setiawan
NIM. 15650009

HALAMAN MOTTO

"*Jalani saja.*
bahkan jika gagal kamu sudah satu langka kedepan"

HALAMAN PERSEMBAHAN

الْحَمْدُ لِلَّهِ رَبِّ الْعَالَمِينَ

Puji syukur kehadirat Allah, shalawat dan salam bagi Rasul-Nya

Penulis persembahkan sebuah karya ini kepada:

Kedua orang tua penulis tercinta, Bapak Samusir dan Ibu Sumilah yang selalu memberikan suntikan motivasi yang tak terhingga

Dosen pembimbing penulis Bapak Dr. Cahyo Crydian dan Bapak Ajib Hananı, MT yang telah dengan sabar membimbing jalannya penelitian skripsi ini dan selalu memberikan stimulus positif untuk tetap semangat menjalani setiap tahap ujian skripsi

Seluruh dosen Teknik Informatika UIN Maulana Malik Ibrahim Malang, dan seluruh guru-guru penulis yang telah membimbing dan memberikan ilmunya yang sangat bermanfaat

Sahabat-sahabat seperjuangan mulai pertama kali penulis menginjakkan kaki di UIN Maulana Malik Ibrahim Malang. Sahabat yang selalu mendukung dan selalu semangat untuk belajar bersama tanpa menjatuhkan. Ribuan kalimat bahagia dan syukur yang tak akan cukup penulis tulis disini teruntuk mereka

Keluarga Teknik Informatika kelas A 2015 dan keluarga Interface (Teknik Informatika angkatan 2015) yang telah memberikan semangat dan doanya

Orang-orang yang penulis penulisngi, yang tak bisa penulis sebutkan satu per satu yang selalu memberikan semangat dan motivasinya kepada penulis untuk menyelesaikan skripsi ini.

Penulis ucapkan terimakasih yang luar biasa. Semoga ukhwah kita tetap terjaga dan selalu diridhoi Allah SWT. Allahumma Aamiin.

KATA PENGANTAR

بِسْمِ اللهِ الرَّحْمٰنِ الرَّحِيْمِ

Puji dan syukur penulis panjatkan ke hadirat Allah subhanahu wa ta'ala yang telah melimpahkan rahmat dan hidayahNya kepada kita, sehingga penulis bisa menyelesaikan skripsi dengan tepat waktu, yang kami beri judul "Peningkatan Keamanan Grup Chat Menggunakan Kombinasi Metode RSA, *Elgamal* dan *Viginere Cipher*". Tujuan dari penyusunan skripsi ini guna memenuhi salah satu syarat untuk bisa menempuh ujian sarjana komputer pada Fakultas Sains dan Teknologi (FSAINTEK) Program Studi Teknik Informatika di Universitas Islam Negeri (UIN) Maulana Malik Ibrahim Malang. Didalam pengerjaan skripsi ini telah melibatkan banyak pihak yang sangat membantu dalam banyak hal. Oleh sebab itu, disini penulis sampaikan rasa terima kasih sedalam-dalamnya kepada:

1. Prof. Dr. Abdul Haris, M.Ag selaku Rektor Universitas Islam Negeri (UIN) Maulana Malik Ibrahim Malang.
2. Dr. Sri Harini,M.Si, selaku Dekan Fakultas Sains dan Teknologi Universitas Islam Negeri (UIN) Maulana Malik Ibrahim Malang.
3. Dr. Cahyo Crysdian, selaku Dosen Pembimbing I yang telah membimbing dalam penyusunan skripsi ini hingga selesai.
4. Ajib Hanani, M.T, selaku Dosen Pembimbing II yang telah membimbing dalam penyusunan skripsi ini hingga selesai.
5. Para staff laboran Fakultas Sains dan Teknologi yang telah bersedia memberikan data.
6. Orang tua tercinta yang telah banyak memberikan doa dan dukungan kepada penulis secara moril maupun materil hingga skripsi ini dapat terselesaikan.

7. Sahabat-sahabat seperjuangan yang tiada henti memberi dukungan dan motivasi kepada penulis serta target bersama untuk lulus skripsi dan wisuda bersama
8. Rekan-rekan interface yang selalu memberikan semangat dan doa kepada penulis.
9. Semua pihak yang telah banyak membantu dalam penyusunan skripsi ini yang tidak bisa penulis sebutkan semuanya.

Penulis menyadari bahwa dalam penyusunan skripsi ini masih terdapat kekurangan dan penulis berharap semoga skripsi ini bisa memberikan manfaat kepada para pembaca khususnya bagi penulis secara pribadi.

Malang, 6 Desember 2019

Penulis

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

ABSTRAK

Risky, Dwi. 2019. ***Peningkatan Keamanan Grup Chat Menggunakan Kombinasi Metode RSA, Elgamal, dan Viginere Cipher.*** Skripsi. Jurusan Teknik Informatika Fakultas Sains Dan Teknologi Universitas Islam Negeri Maulana Malik Ibrahim Malang. Pembimbing : (I) Dr. Cahyo Crydian. (II) Ajib Hanani, M. T.

Kata Kunci : Kiptografi, Elgamal, RSA, Viginere Cippher.

Seiring dengan perkembangan teknologi telepon seluler yang pesat dan banyaknya penggunaan layanan *mobile messenger*, maka aspek keamanan menjadi sangat penting untuk dipertimbangkan. Keamanan merupakan masalah terbesar bagi pengguna *mobile messenger* pada perusahaan atau enterprise. Maka dibutuhkan aplikasi *mobile messenger* dengan sistem enkripsi menggunakan kombinasi metode RSA, *Elgamal*, dan *Viginere Cipher* yang lebih sulit untuk dipecahkan dari pada menggunakan single metode. Penggunaan kombinasi metode akan meningkatkan konsumsi waktu sebanyak 45%, tingkat keberhasilan dideskripsikan kembali menurun sebanyak 46,2%, dan peningkatan size pesan sebanyak 80% namun aspek keamanan jauh lebih penting. Dengan menggunakan kombinasi metode akan meningkatkan usaha perulangan *brute force* sebesar 73.496.518,7%.

ABSTRACT

Risky, Dwi. 2019. ***Improved Chat Group Safety Using a Combination of the RSA, Elgamal and Viginere Cipher Methods.*** Essay. Department of In*form*atics Engineering, Faculty of Science and Technology, Islamic State University of Maulana Malik Ibrahim of Malang. Counselor: (I) Dr. Cahyo Crydian. (II) Ajib Hanani, M. T.

Keywords: Kiptography, Elgamal, RSA, Viginere Cippher.

Along with the development of mobile messenger technology and the many uses of mobile messenger services, the security aspect is very important to consider. Security is the biggest problem for mobile messenger users in a company or enterprise. So we need a mobile messenger application with an encryption system using a combination of RSA, Elgamal, and Viginere Cipher methods that are more difficult to get cracked than using a single method. Using a combination of methods will increase time consumption by 45%, decryption success rate decreases by 46.2%, and message size increases by 80% but security aspects are far more important. Using a combination of methods will increase the brute force looping effort by 73,496,518.7%.

الملخص

رسكي، دوي. ٢٠١٩. و RSA تحسين أمان الدردشة الجماعية باستخدام مزيج من أساليب التشفير Viginere و Elgamal. قسم هندسة المعلوماتية لكلية العلوم والتكنولوجيا في جامعة مولانا مالك إبراهيم الإسلامية الحكومية بمالانق. المشرف : (١)جهي جرسديان، الماجستير. (٢)جهي جرسديان، الماجستير.

الكلمات الرئيسية : Viginere ، RSA ، Elgamal ، Kiptography.

جنبا إلى جنب مع التطور السريع لتكنولوجيا الهاتف الخلوي والعديد من الاستخدامات لخدمات الرسائل المحمولة ، الجانب الأمني مهم جدا للنظر .الأمن هو أكبر مشكلة بالنسبة لمستخدمي برامج مراسلة الجوال في شركة أو مؤسسة .لذلك نحن Viginere Cipher و Elgamal و RSA بحاجة إلى تطبيق مراسلة محمول مع نظام تشفير يستخدم مجموعة من أساليب التي يصعب حلها أكثر من استخدام طريقة واحدة .سيؤدي استخدام مجموعة من الطرق إلى زيادة استهلاك الوقت بنسبة 45٪ ، كما انخفض معدل النجاح الموصوف مرة أخرى بنسبة 46.2٪ ، وزيادة في حجم الرسالة بنسبة 80٪ ولكن الجانب الأمني كان أكثر أهمية .باستخدام مجموعة من الأساليب سيزيد من جهد حلقة القوة الغاشمة بنسبة 73،496،518.7٪..

BAB 1

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi dan komunikasi sangat pesat yaitu menciptakan berbagai aplikasi yang memudahkan pengguna khususnya untuk layanan pengiriman yang memanfaatkan jaringan data internet untuk saling berbagi informasi. Konsep awal pengiriman pesan mengginakan media internet adalah konsep *one-to-one* yang menggunakan e-mail, yang mana e-mail dinilai terlalu formal dan kaku sebagai alat komunikasi, dan e-mail dinilai terlalu lama dalam merespons. Pada tahun 2003 sosial media mulai populer sejak dirilisnya MySpace, dan Facebook. Kedua sosial media ini merubah konsep *instan messager* yang dahulu hanya dapat mengirim pesan dengan konsep *one-to-one* menjadi *one-to-many*, Sejak tahun 2007 perkembangan smartphone sudah semakin popular, sehingga mendorong model komunikasi baru, yaitu berupa komunikasi grup chat. Komunikasi ini dirancang untuk memungkinkan respons langsung dalam waktu yang singkat dengan pengirim pesan instan.

Dengan terungkapnya kegiatan pengawasan massal oleh badan intelijen, saat ini aplikasi IM(*Instant Messager*) menggabungkan enkripsi *end-to-end* pada aplikasinya, aplikasi IM menambahkan protokol enkripsi untuk melindungi komunikasi menuju server pengiriman pesan. Karenanya menganalisis, menyelidiki protokol-protokol ini, juga termasuk serangan berbasis server. Hal ini bertujuan untuk melindungi konten pesan tunggal dan kekuatan protokol untuk memastikan bahwa pengguna yang tidak termasuk ke grup harus tidak dapat

menambahkan diri ke grup atau menerima pesan dari grup tanpa anggota izin (Moran, 2017).

Masalah keamanan mencakup banyak aspek, seperti *physical layer*, *network layer, system layer* dan *application layer*. Karena memiliki sifat yang berbeda, tindakan pencegahan keamanan yang digunakan juga berbeda, seperti teknologi firewall di lapisan jaringan dan antivirus di lapisan sistem. Pencegahan keamanan pada lapisan jaringan dan lapisan sistem tidak cukup untuk menjamin keamanan data, data bersifat sensitif dan hanya boleh dibaca oleh pengirim dan penerima pesan saja, bahkan pengembang aplikasi tidak berhak untuk membaca data tersebut, untuk itu dibutuhkan keamanan tambahan pada lapisan aplikasi, untuk itu diperlukan. pengamanan yang berupa penyandian pesan sehingga pesan yang dikirimkan merupakan pesan yang telah disandikan (Bing, Dkk, 2014).

Aplikasi chatting adalah aplikasi yang digunakan percakapan dua orang atau lebih melalui jaringan internet. Percakapan yang dilakukan dapat berupa pesan teks langsung yang sudah berada di list kontak yang dimiliki. tidak hanya itu pengiriman yang dilakukan dapat mengirimkan file gambar, dokumen, dan audio. Pesan informasi yang dibagikan bersifat sensitif dan rahasia yang menjadi privasi pengguna. Oleh karena itu keamanan pesan merupakan hal yang sangat penting dalam pengiriman data untuk menjaga kerahasiannya.

Dalam menjaga kerahasian data diperlukan ilmu kriptografi, yang mentransformasikan data jelas *(plaintext)* ke dalam bentuk data sandi *(ciphertext)* yang tidak dapat dikenali. Dengan adanya algoritma kirptografi dapat mencegah terjadinya kebocoran informasi dari pesan yang dikirim dengan membuat pesan

agar ter-enskripsi dengan baik dan data pesan pengguna dapat terlindungi sehingga mendapatkan hak privasinya.

Berkaitan dengan keamanan dalam al-Qur'an dalam surah Al-Ahzab ayat 72 dijelaskan bahwa:

وَحَمَلَهَا مِنْهَا وَأَشْفَقْنَ يَحْمِلْنَهَا أَنْ فَأَبَيْنَ وَالْجِبَالِ وَالْأَرْضِ السَّمَاوَاتِ عَلَى الْأَمَانَةَ عَرَضْنَا إِنَّا
جَهُولًا ظَلُومًا كَانَ إِنَّهُ الْإِنْسَانُ

Artinya: "Sesungguhnya Kami telah mengemukakan amanat kepada langit, bumi dan gunung-gunung, maka semuanya enggan untuk memikul amanat itu dan mereka khawatir akan mengkhianatinya, dan dipikullah amanat itu oleh manusia. Sesungguhnya manusia itu amat zalim dan amat bodoh".

Menurut Tafsir Al-Muyassar (Kementerian Agama Saudi Arabia) menjelaskan Sesungguhnya Kami telah menawarkan beban syariat dan apa yang harus dijaga dari harta dan rahasia kepada langit, bumi dan gunung-gunung, namun mereka semua enggan untuk menerima amanah ini dan takut dari akibatnya, lalu manusia menerimanya, sesungguhnya manusia itu amat zalim terhadap dirinya sendiri dan tidak mengetahui sama sekali akibat dari menerima amanah ini.

Sesuai dengan pengiriman pesan melalui aplikasi *chat*. Dimana orang menggunakan layanan tersebut memiliki hak untuk mendapatkan pesan sesuai yang telah dikirimkan. Jika seseorang tidak menerima pesan sesuai dengan apa yang dikirimkan, maka akan menjauhkan dari sifat amanat yang diberikan oleh Allah SWT. Adapun kisah lain pada masalah keamanan informasi secara tersirat yaitu kisah Nabi Sulaiman. Kisah tersebut terdapat pada al-Qur'an surah An-Naml

ayat 21-30. Ayat tersebut menjelaskan bahwa burung hud-hud menyampaikan berita tentang adanya sebuah negeri. Negeri tersebut memiliki kekayaan yang melimpah tetapi seluruh penduduk negeri tersebut menyembah matahari. Negeri tersebut bernama Saba yang dipimpin oleh Ratu Bilqis. Mendengar informasi tersebut Nabi Sulaiman tidak mempercayainya. Kemudian Nabi Sulaiman melakukan *checking* dengan mengirimkan surat. Pada dasarnya surat merupakan uji validitas terhadap burung hud-hud. Hal ini dilakukan burung hud-hud untuk menjaga kerahasian informasi yang ada didalam surat tersebut. kisah ini menunjukan sejak zaman Nabi Sulaiman AS, konsep keamanan telah diterapkan.

Keamanan merupakan karunia Allah yang diberikan kepada manusia untuk wajib disyukuri. Dengan adanya sistem keamanan data pesan yang dimiliki pengguna akan aman. Oleh karena itu pada penelitian peningkatan keamanan menggunakan metode Elgamal, RSA, dan Vigenere Chipper sebagai manajemen keamanan chat berbasis android.

1.2 Pernyataan Masalah

Masalah dalam penelitian ini adalah

1. Seberapa tinggi tingkat keberhasilan enskripsi-dekripsi menggunakan kombinasi metode RSA, Elgamal dan Viginere Cipher
2. Seberapa besar peningkatan size pesan yang dihasilkan oleh proses enskripsi-dekripsi menggunakan kombinasi metode RSA, Elgamal, dan Viginere Cipher
3. Seberapa banyak waktu yang diperlukan pada proses enskripsi-dekripsi menggunakan kombinasi metode RSA, Elgamal, dan Viginere Cipher
4. Mengukur pprobabilitas dipecahkannya skema chipper text menggunakan kombinasi metode RSA, Elgamal, dan Viginere Cipher

1.3 Tujuan Penelitian

Adapun tujuan dilakukannya penelitian ini adalah

1. Mengukur tingkat keberhasilan enskripsi-dekripsi menggunakan kombinasi metode RSA, *Elgamal*, dan *Viginere Cipher*.
2. Mengukur size pesan yang dihasilkan oleh proses enskripsi-dekripsi menggunakan kombinasi metode RSA, *Elgamal*, dan *Viginere Cipher*.
3. Mengukur waktu yang diperlukan pada proses enskripsi-dekripsi menggunakan kombinasi metode RSA, *Elgamal*, dan *Viginere Cipher*.
4. Mengukur probabilitas dipecahkannya skema chipper text.

1.4 Batasan Penelitian

Pembahasan pada penelitian ini dibatasi oleh beberapa hal berikut:

Grup chat yang dijadikan objek penelitihan memiliki spesifikasi sebagai berikut:

- Informasi yang dikirim hanya berupa text
- Aplikasi harus terhubung dengan jaringan Internet
- Berjalan diplatform android

1.5 Manfaat Penelitian

Adapun manfaat yang dapat diperoleh dari penelitian ini ditunjukan kepada pakar keamanan data, perusahaan-perusahaan yang memiliki data-data sensitif untuk menjaga kerahasiaan data mereka.

1.6 Sistematika Penulisan

Uraian dalam laporan skripsi penulis menyusun dengan sistematika penulisan sebagai berikut :

BAB I : PENDAHULUAN

Pendahuluan berisi tentang latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan.

BAB II : TINJAUAN PUSTAKA

Tinjauan pustaka berisikan tentang teori yang berhubungan dengan permasalahan penelitian dari keamanan *chat* menggunakan algoritma elgamal, yang selanjutnya digunakan dalam bagian pembahasan dan sebagai dasar dalam pembuatan sistem.

BAB III :METODOLOGI PENELITIAN

Metodologi penelitian berisikan tentang pembuatan analisis dan perancangan program aplikasi enkripsi aplikasi *chat* menggunakan algoritma *elgamal* berbasis android.

BAB IV : HASIL DAN PEMBAHASAN

Analisa dan perancangan berisikan tentang analisa sistem aplikasi dan perancangannya

BAB V : PENUTUPAN

Pada bab terakhir berisi kesimpulan dan saran berdasarkan hasil yang telah dicapai dari pembahasan.

BAB 2

STUDI PUSTAKA

2.1 Penelitian Terkait

Bing Han (2014) menjelaskan bahwa tingkat keamanan pada netword layer seperti firewall dan antivirus tidak cukup dalam mengamankan data maka pada tingkat aplikasi dibutuhkan keamanan tambahan yaitu berupa eksripsi. Pada sistem group based enskripsi hanya dibutuhkan satu kali kemudian dekripsi dilakukan secara tersendiri.

(2013) menjelaskan bahwa penyerangan ketahanan Algoritma RSA terhadap penyerangan *Brute Force* jika ada waktu untuk melakukannya, semakin besar kunci yang digunakan semakin lama pula waktu yang diperlukan, untuk kunci sebesar 56 bit, maka dibutuhkan waktu 1142 tahun untuk memecahkan pesan yang dienskripsinya.

Gilang (2013) menjelaskan bahwa hasil enskripsi dari Vigenere Cipher dapat dibobol menggunkan metode analisist frekuensi, gagal didekripsi jika menggukanan kunci berkarakter non alphabet.

Danang (2013) dalam peneitihannya berjudul "Algoritma Elgamal Dalam Pengamanan Pesan Rahasia" menjelaskan metode ElGAmal mempunyai kemamuan yang baik dalam pendistribusian kunci, ini dikarenakan saat pembentukan kunci sang penerima pesan membuat 2 kunci yaitu kunci public dan kunci private, kunci public akan diserahkan ke orang lain yang akan digunakan untuk mengamankan pesan yang akan dikirim sedangkan kunci private tetap di pengang oleh pembuat kunci saja, algoritma ini mempunyai kelebihan yaitu pada

proses enskripsi akan menghasilkan chipper yang berbeda-beda, namun pada proses dekripsi akan menghasilakan plaint text yang sama.

2.2 Grup Chat Komunikasi

Evolusi teknologi terutama teknologi internet membuat teknologi pengiriman pesan semakin berkembang, selama dua dekade terakhir teknologi pengiriman pesan berkembang pesat, dimulai dari tahun 1990an teknologi pengiriman pesan instan lahir dengan konsep komunikasi one-to-one dimana setiap pengguna dapat mengirim suatu pesan ke pengguna lain secara instan melalui jalur internet konsep ini dinamakan dengan instant messengers (Seufert, Dkk. 2016).

Pada tahun 1996 salah satu aplikasi instant messengers ICQ dirilis, aplikasi ini merupakan alternatif pengiriman pesan yang menggantikan E-Mail, yang mana E-Mail dinilai terlalu formal dan kaku sebagai alat komunikasi, dan E-Mail dinilai terlalu lama dalam merespon. Instant messenger semakin populer dikarenkan karekteristiknya yang mana dapat mengirim pesan dengan kalimat yang pendek dan memiliki respon yang cepat.

Pada tahun 2003 dan 2004, dua dari sosial media populerr dirilis, yaitu MySpace, dan Facebook. Kedua sosial media ini merubah konsep instan messager yang dahulu hanya dapat mengirim pesan dengan konsep *one-to-one* menjadi *one-to-many*.

Sejak tahun 2007 perkembangan smartphone sudah semakin popular, sehingga mendorong model komunikasi baru, yaitu berupa komunikasi grup chat.

Komunikasi ini dirancang untuk memungkinkan respons langsung dalam waktu yang singkat dengan pengirim pesan instan.

2.3 Kiptografi

Kriptografi (*cryptography*) berasal dari bahasa Yunani. Kriptografi terdiri dari 2 kata yaitu kripto artinya menyembunyikan, sedangkan graphia artinya tulisan. Kriptografi adalah teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasian data, integritas data, serta autentikasi data.

Kebalikan dari kriptografi adalah kriptonalisis (*cryptanalysis*) adalah ilmu untuk memecahkan mekanisme kriptografi dengan mendapatkan kunci dari *ciphertext* yang akan digunakan mendapatkan *plaintext*. Kemudian ilmu yang mencakup dari kriptografi dan kriptonalisis yaitu kriptologi (*cryptology*).

Kriptografi dapat diartikan ilmu untuk menjaga pesan. Ketika pesan dikirim dari suatu tempat ketempat yang lain. Pada isi pesan tersebut harus dijaga. Untuk menjaga suatu pesan tersebut yaitu dapat diubah menjadi sebuah kode dan tidak dapat dimengerti oleh orang lain.

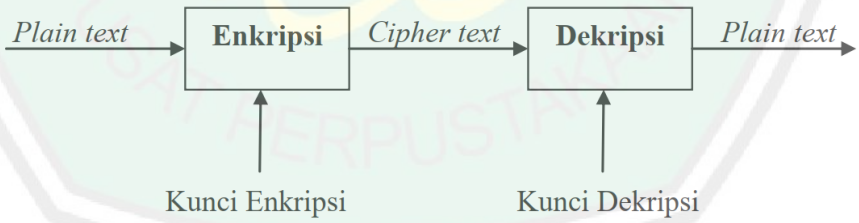
Kriptografi memiliki empat tujuan yaitu dari segi aspek keamanan:

1. *Confidentiality* yaitu untuk menjaga informasi dari orang yang ingin mengakses data pribadi.
2. *Integrity* yaitu untuk menjaga data yang tidak dapat diubah oleh orang tidak berwenang.
3. *Authentication* yaitu untuk mengetahui keaslian informasi.
4. *Availability* yaitu ketersedian dari sistem dan data ketika dibutuhkan.

Pada dasarnya komponen kriptografi terdiri dari beberapa komponen, seperti:

1. Enkripsi: merupakan proses pengamanan informasi yang dikirimkan dengan cara membuat informasi tersebut tidak dapat dibaca sehingga terjaga kerahasiaannya.
2. Dekripsi: merupakan kebalikan dan enkripsi. Yaitu proses mengkonversi pesan yang telah di enkripsi dikembalikan ke bentuk asalnya.
3. Kunci: adalah kunci yang dipakai untuk melakukan enkripsi dan deskripsi. Kunci terbagi menjadi dua bagian. yaitu kunci publik dan kunci privat
4. Ciphertext: merupakan suatu informasi yang telah melalui proses enkripsi. Informasi ini tidak bisa dibaca karena berupa karakter-karakter yang tidak tidak dapat dibaca.
5. Plaintext: merupakan informasi yang dapat dibaca. Plainteks inilah yang diproses menggunakan algoritma kritografi untuk menjadi cipher text (teks-kode). mengenkripsi dan mendekripsi data.

Proses pada kriptografi terdiri dari dua yaitu proses enkripsi dan dekripsi. Adapun diagram secara umum berikut gambar 2.1.



Gambar 2.1 Diagram Proses Enkripsi dan Dekripsi

Suatu pesan yang tidak disandikan disebut dengan *plaintext* atau *cleartext.* Proses enkripsi dikenal dari proses transformasi dari *plaintext* ke *ciphertext.* Sedangkan proses dekripsi dikenal dari proses transormasi *ciphertext* ke *plaintext*. Pada kedua proses tersebut dikenal dengan sebuah kunci atau *key*.

Berdasarakan kunci yang dipakai algoritma kriptografi dibagi menjadi tiga bagian, yaitu :

a. Algoritma simetri

Algoritma simetri disebut juga dengan algoritma klasik karena algoritma ini menggunakan kunci yang sama untuk kegiatan enkripsi maupun dekripsi. Bila ingin mengirim pesan dengan menggunakan algoritma ini, si pengirim pesan harus diberitahu kunci dari pesan yang telah dienkripsi menggunakan algoritma ini ke penerima pesan lalu penerima pesan menggunakan kunci tersebut mendekripsikan pesan yang terkirim. Keamanan dari pesan yang menggunakan algoritma ini tergantung pada kunci. Kelemahan dari algoritma ini adalah jika kunci tersebut diketahui oleh orang lain maka orang tersebut akan dapat melakukan enkripsi dan dekripsi terhadap pesan tersebut. Algoritma yang memakai kunci simetri di antaranya adalah:

1. Data Encryption Standard (DES),
2. Advanced Encryption Standard (AES),
3. International Data Encryption Algorithm (IDEA),
4. RC2, RC4, RC5, RC 6,
5. On Time Pad (OTP) dan lain sebagainya.

b. Algoritma Asimetri

Algoritma asimetri sering juga disebut dengan algoritma kunci public, yang mana kunci yang digunakan untuk melakukan enkripsi berbeda dengan kunci

yang digunakan untuk dekripsi. Pada algoritma asimetri kunci terbagi menjadi dua bagian, yaitu :

1. Kunci umum (public key), kunci yang boleh semua orang tahu (dipublikasikan).

2. Kunci rahasia (private key), kunci yang dirahasiakan (hanya boleh diketahui oleh satu orang).

Kunci-kunci tersebut berhubungan satu sama lain. Kunci public orang dapat mengenkripsi pesan dan kunci private digunakan untuk mendekripsi. Hanya orang yang memiliki kunci rahasia yang dapat mendekripsikan pesan tersebut. Algoritma asimetri bisa mengirimkan pesan dengan lebih aman daripada algoritma simetri. Algoritma yang memakai kunci public di antaranya adalah :

1.ElGamal,

2. RSA,

3. Diffle-Hellman (DH),

4. Elliptic Curve Cryptography (ECC),

5. Digital Signature Algorithm (DSA),

6. Kriptografi Quantum, dan lain sebagainya.

2.3.1 Algoritma RSA

RSA merupakan salah satu algoritma kriptografi asimetris. Ditemukan pertama kali pada tahun 1977 oleh Ron Rivest, Adi Shamir, dan Leonard Adleman, peneliti dari Massachussets Institute of Technology (MIT). Sebagai

algoritma kunci publik, algoritma RSA mempunyai dua kunci, yaitu kunci publik dan kunci private. Kunci publik boleh diketahui oleh siapa saja, kunci ini digunakan untuk proses enkripsi. Sedangkan kunci private hanya diketahui oleh si pembuat kunci itu saya, yang mana kunci digunakan untuk proses dekripsi (Wahyuni, 2011).

Algoritma RSA memiliki keamanan yang lebih kompleks dan lebih tinggi dari pada algoritma konvensional lainnya, hal ini dikarenakan algoritma ini mempunyai faktorisasi bilangan dalam jumlah yang banyak dan mencari modulo akar e dari sebuah bilangan komposit n yang faktor-faktornya tidak diketahui. Oleh sebab itu hasil enkripsi menggunakan metode ini memiliki memiliki bentuk yang tidak beraturan dan sulit untuk dikembalikan ke bentuk asal tanpa mengetahui kunci privat nya.

Pada algoritma *RSA* terdiri atas tiga langka utama, yaitu proses pembentukan kunci, enkripsi, dan dekripsi (Setiawan, 2013).

1. Pembentukan kunci

   Proses pembentukan kunci terdiri dari dua kunci, yaitu kunci publik dan kunci privat. Dimana proses ini membutuhkan dua buah bilangan prima p dan q. proses pembangkitan kunci Algoritma RSA aadalah sebagai berikut:

   a. Generate bilangan prima p dan q
   b. n=p*q
   c. m=(p-1)*(q-1)

d. Pilih d yang relative prima terhadap m, e relative prima terhadap m artinya faktor pembagi terbesar keduanya adalah 1, secara matematis disebut gcd(e,m) = 1. Untuk mencarinya dapat digunakan algoritma Euclid.

e. Cari d, sehingga e*d = 1 mod (m), atau d = (1+nm)/e Untuk bilangan besar, dapat digunakan algoritma extended Euclid

f. Kunci publik: e, n Kunci private: d, n.

Pihak yang melakukan pembentukan kunci adalah pihak penerima, sedangkan pihak pengirim hanya menerima kunci publik yang diberikan oleh pihak penerima, dan kunci publik tersebut digunakan untuk mengenkripsi pesan.

Pada algoritma RSA pesan harus dikonversi dahulu ke dalam suatu bilangan bulat agar dapat dihitung. Untuk mengubah pesan menjadi bilangan bulat, maka digunakan kode ASCII (American Standard for Information Interchange) yang merupakan representasi numerik dari karakter-karakter yang digunakan pada komputer.

2. Inskripsi

Proses inskripsi pesan dilakukan pada pihak pengirim pesan dengan menggunakan kunci publik (e dan n). Pesan yang akan dikirim dirubah ke dalam blok-blok karakter dan setiap karakter du konversikan kedalam kode ASCII. Setiap blok plaintext P dienskripsi dengan cara

$$C = P^e \bmod n$$

3. Deskripsi

Setelah menerima Ciphertext dari pengirim proses selanjutnya adalah mendekripsi menggunakan kunci privat d dan kunci publik n untuk mendekripsi C menjadi plaintext P, dengan cara.

$$P = C^d \bmod n$$

Selanjutnya blok-blok plaint text P digabungkan sehingga plaintext dapat ditemukan kembali.

2.3.2 Algoritma ElGamal

Algoritma ElGamal pertama kali dipublikasikan oleh Tahern ElGamal pada tahun 1985. Algoritma ElGamal terdiri dari tiga proses, yaitu proses pembentukan kunci, proses enkripsi dan proses dekripsi. Algoritma ini merupakan cipher blok, yang mana untuk melakukan proses enkripsi pada suatu plainteks dipecah menjadi blok-blok plainteks blok-blok ini dienskripsi menjadi blok-blok Ciphertext, dan untuk proses deskripsi dari blok-blok cipherteks yang kemudian dilakukan proses dekripsi per blok, dan hasilnya digabungkan kembali menjadi pesan yang utuh dan dapat dibaca (Rizal, 2010).

ElGamal merupakan salah satu algoritma kriptografi kunci asimetris yang memiliki dua kunci berbeda, yaitu kunci publik dan kunci privat. Kunci publik untuk disebar luaskan, dan digunakan dalam proses enskripsi sedangkan kunci privat hanya untuk diri sendiri saja, dan digunakan dalam proses dekripsi.

ElGamal merupakan algotitma yang cocok digunakan untuk digital signature seperti halnya enkripsi dikarenakan memiliki tingkat kesulitan dalam menghitung logaritma diskrit menjadikan algoritme ini memiliki tingkat

kemananan yang cukup baik (Munir, Rinaldi, 2006). dikarenakan karakter enskripso algoritma ElGamal itu sendiri yang akan menghasilkan ukuran chiphertext menjadi dua kali lipat dari pada plaintext. Proses enskripsi akan menghasilkan nilai acak pada Ciphertext, sehingga jika pada plaintext yang sama dilakukan enkripsi sebanyak dua kali, akan dihasilkan ciphertext yang berbeda.

Pada algoritma *ElGamal* terdiri atas tiga langka utama, yaitu proses pembentukan kunci, enkripsi, dan dekripsi (Karima, Handoko, & Saputro, 2017).

1. Pembentukan Kunci

   Proses pembentukan kunci terdiri dari dua kunci, yaitu kunci publik dan kunci privat. Dimana proses ini membutuhkan sebuah bilangan prima *p* dan dua buah bilangan acak *g* dan *x* dengan syarat $g < p$ dan $x < p$.

   $$y = g^x \bmod p.$$

   Kunci publik disimbolkan dengan variabel y, g dan p, sedangkan kunci privat disimbolkan dengan variabel x. Beberapa parameter yang digunakan dalam proses perhitungan algoritme ElGamal adalah sebagai berikut.

   - Bilangan prima p bersifat tidak rahasia.
   - Bilangan acak g (g < p) bersifat tidak rahasia
   - Bilangan acak x (x < p) bersifat rahasia.
   - Bilangan y bersifat tidak rahasia.
   - m (plaintext) bersifat rahasia merupakan pesan asli yang digunakan untuk proses enkripsi.

- a dan b (cipher text) bersifat tidak rahasia.

Pihak yang melakukan pembentukan kunci adalah pihak penerima, sedangkan pihak pengirim hanya mengetahui kunci publik yang diberikan oleh pihak penerima, dan kunci publik tersebut digunakan untuk mengenkripsi pesan. Jadi, penggunakan algoritma kriptografi kunci publik adalah tidak ada permasalahan pada distribusi kunci apabila jumlah pengirim sangat banyak serta tidak ada kepastian keamanan jalur yang digunakan.

Karena pada algoritma ElGamal menggunakan bilangan bulat dalam proses perhitungannya, maka pesan harus dikonversi dahulu ke dalam suatu bilangan bulat. Untuk mengubah pesan menjadi bilangan bulat, maka digunakan kode ASCII (American Standard for Information Interchange) yang merupakan representasi numerik dari karakter-karakter yang digunakan pada komputer.

2. Enskripsi

Proses enskripsi pesan dilakukan pada pihak pengirim pesan dengan menggunakan kunci publik (p, g dan y) dan memilih bilangan acak k yang berada dalam himpunan $1 \leq k \leq p-2$. Pesan yang akan dikirim dirubah ke dalam blok-blok karakter dan setiap karakter du konversikan kedalam kode ASCII. Setiap blok plaintext m dienskripsi dengana cara

$$a = g^k \bmod p$$

$$b = y^x m \bmod p$$

Bilangan acak k ditentukan oleh pihak pengirim dan bersifat rahasia, jadi hanya pengirim saja yang mengetahuinya,nilai k hanya digunakan saat melakukan enkripsi saja dan tidak perlu disimpan. Hal ini membuat suatu plainteks yang sama akan dienkripsi menjadi cipherteks yang berbeda-beda. dikarenakan pemilihan bilangan k yang acak. Akan tetapi, walaupun cipherteks yang diperoleh berbeda-beda, tetapi pada proses dekripsi akan diperoleh plainteks yang sama.

3. Dekripsi

Setelah menerimah Ciphertext dari pengirim proses selanjutnya adalah mendekripsi menggunakan kunci privat x dan dan kunci publik p untuk mendekripsi a dan b menjadi plaintext m, dengan cara.

$$m = b * a^{(p-1-x)} \bmod p$$

Sehingga plaintext dapat ditemukan kembali dari pasangan ciphertext a dan b.

2.3.3 Algoritma Vigenere Cipher

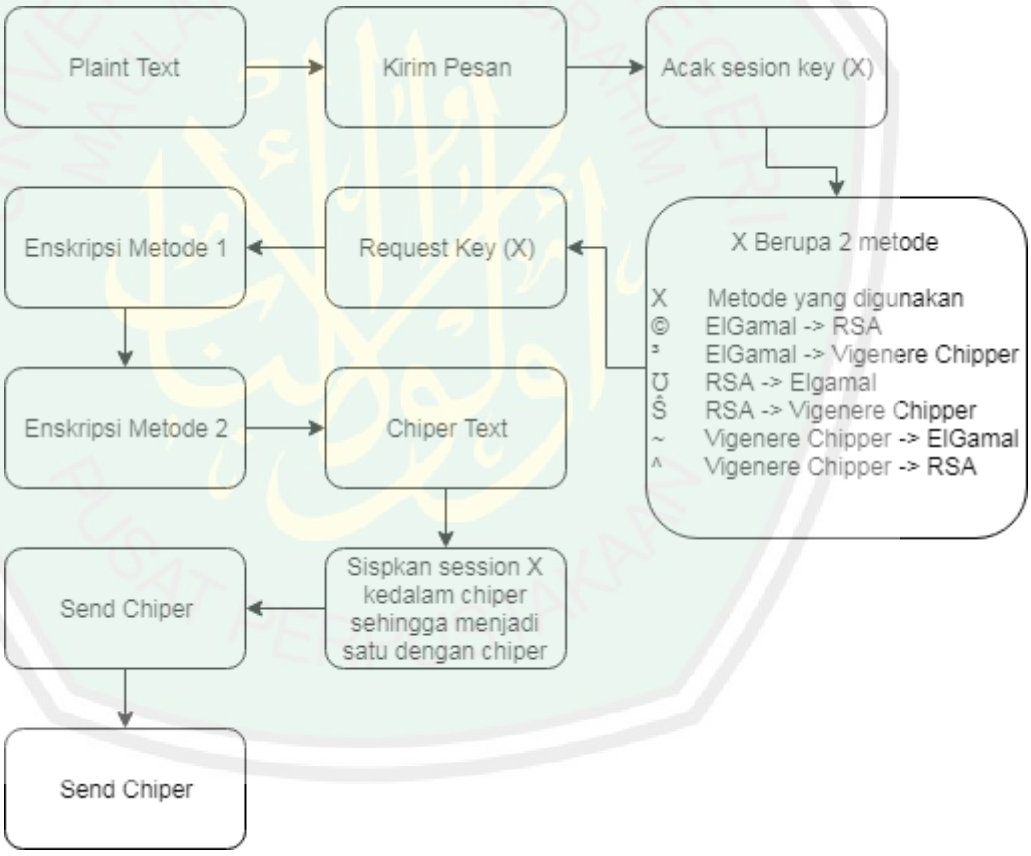
Algoritma Vigenere Cipher merupakan algoritma kode abjad mejemuk (polyalphabetic substitution Cipher) yang dipublikasikan pada tahun 1586 oleh kriptogis asal prancis, Blaise de Vigenere. Algoritma ini dalam proses enkripsi dan deskripsi menggunakan teknik substitusi yaitu dengan menggeser setiap huruf dengan jumlah yang berbeda-beda di setiap hurufnya. Jika panjang kunci lebih pendek daripada panjang teks-asli maka pengunaan kunci diulang (Kurniawan, 2013).

BAB 3

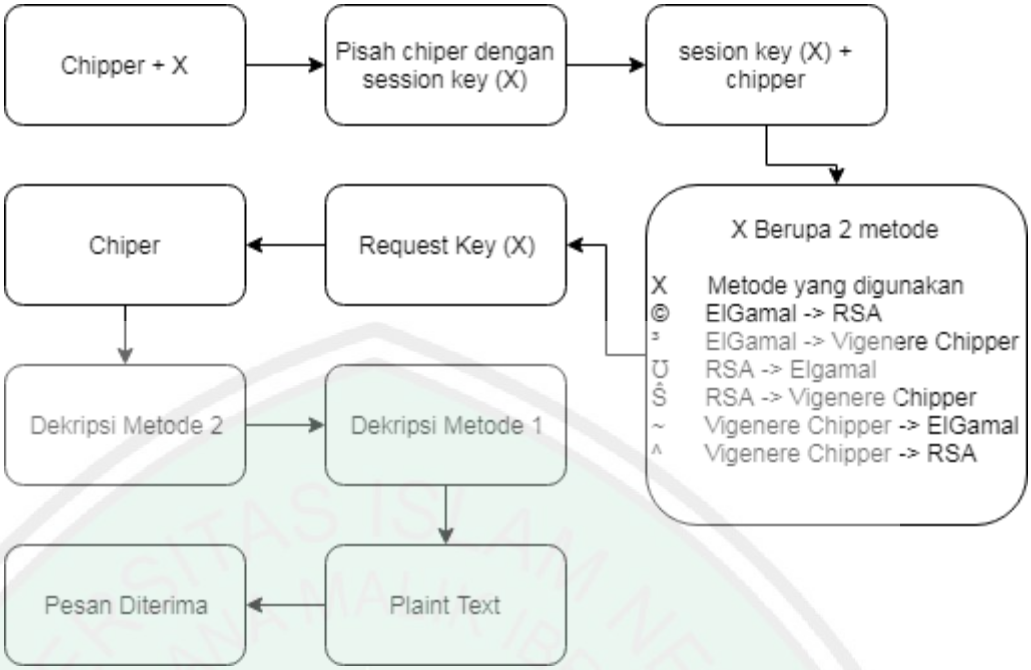
PERANCANGAN SISTEM

3.1 Diagram Blok

Diagram blok peningkatan keamanan grup chat terdapat dua bagian yaitu; diagram blok kirim pesan, dan terima pesan yang akan digambarkan pada Gambar 3.1 dan Gambar 3.2 berikut ini:



Gambar 3-1 Diagram Blok Kirim pesan



Gambar 3-2 Diagram Blok Terima pesan

3.2 Peningkatan Keamanan

Peningkatan keamanan dilakukan dengan cara kombinasi metode RSA, *Elgamal*, dan *Vigenere Cipher* dilakukan dengan teknik Sistem *Hybrid.* System ini menggabungkan dua atau metode kiptografi guna untuk meningkatkan keamanan data. Proses ini dilakukan dengan cara menegosiasikan penggunaan metode diantara pihak penerima dengan pihak pengirim pesan, ke dua belah pihak diharuskan setuju dengan metode yang dipakai

Proses negosiasi dimulai dari pihak pengirim pesan dimana pihak pengirim pesan mengirim *session key* yang disipkan ke dalam chipper text yang kemudian chipper text tersebut dikirim ke pihak penerima. Suatu *session key* hanya dipakai sekali sesi atau sekali pengiriman pesan. Untuk sesi selanjutnya *session key* harus dibuat kembali secara acak sesuai dengan tabel. *Session key*

tersebut berisi urutan penggunaan metode yang dipakai dalam proses enkripsi pesan, berikut merupakan table *session key* metode:

Tabel 3.1 Session Key

session key	metode yang digunakan
©	ElGamal -> RSA
³	ElGamal -> Vigenere Chipper
Ʊ	RSA -> ElGamal
Ŝ	RSA -> Vigenere Chipper
~	Vigenere Chipper -> ElGamal
^	Vigenere Chipper -> RSA

Session key disimbolkan menjadi X sedangkan panjang chipper text disimbolkan dengan C, session key ini nantinya akan dikirim bersamaan dengan chipper text sehingga X disisipkan pada N yang merupakan karakter ke 7/13 dari panjang chipper text, berikut merupakan contoh proses penyisipan session key kedalam chipper text

Chipper text = “l̨e}ìºNj]üǫ̣rAÝ"½ɗ‖LJ”

X = Ʊ (acak)

C = panjang chipper text = 18

N = C * 7 / 13 = 9

Session key disisipkan setelah N, jadi

Chipper text = “l̨e}ìºNj]ü **Ʊ** ǫ̣rAÝ"½ɗ‖LJ”

3.2.1 Elgamal

Kiptografi *Elgamal* merupakan kiptografi asimetris yang memiliki dua kunci yaitu kunci publik, dan kunci privat yang digunakan dalam proses enkripsi

dan dekripsi pesan. untuk memperoleh sepasang kunci tersebut sistem melakukan proses pembentukan kunci yang kemudian terbentuk kunci publik yang akan di bagikan kepada user lain, dan kunci private yang hanya akan disimpan dalam internal *device* itu saja.

Enkripsi merupakan salah satu cara mengamankan suatu informasi dengan cara membuat informasi tersebut tidak dapat dibaca oleh pihak lain. Pada umumnya proses enkripsi dilakukan oleh pihak pengirim pesan dan membutuhkan kunci publik dari pihak penerima pesan secara *one-to-one communication*. Namun untuk mengirim satu pesan ke beberapa penerima (*on-to-many communication*) dalam suatu grup chat pengirim pesan harus mengenkripsi pesan tersebut satu-persatu sesuai dengan kunci publik setiap anggota dalam grup tersebut.

Kemudian untuk membaca pesan masuk yang sudah diennkrisi (*chiphietext*). Pihak penerima akan mendekripsi pesan tersebut secara otomatis menggunakan kunci private dan publik yang telah digenerate sebelumnya. Proses generate kunci adalah sebagai berikut.

$y = g^x \bmod p$

Contoh pembentukan kunci ElGamel

proses ini membutuhkan sebuah bilangan prima *p* dan dua buah bilangan acak *g* dan *x* dengan syarat $g < p$ dan $x < p$.

$p=2903$

$g=1324$

$x=1794$

Maka

$y = g^x \ mod \ p$

$y = 1324^{1794} \ mod \ 2903$

$y = 331$

Kunci Publik = p, g, y

= 2903, 1324, 331

Kunci Private = x

= 1794

Setelah didapatkan kunci publik, dan kunci private, maka proses selanjutnya adalah mengirim kunci publik ke sever dan menyimpan kunci private ke penyimpanan internal device itu sendiri.

Langka selanjutnya adalah melakukan enskripsi pada pesan yang akan dikirim, proses enskripsi pesan adalah sebagai berikut.

Contoh enskripsi pesan

Plaint text = Bismillah

Plaint text dirubah ke blok-blok karakter dan setiap karakter du konversikan kedalam kode ASCII dan setiap karakter diganerate bilangan acak 1 ≤ k ≤ p-2

Tabel 3.2 Konversi ASCII ElGamal

Pesan	ASCII	Nilai Random
B	66	1473
i	105	1799
s	115	2252
m	109	2217
i	105	416
l	108	2663
l	108	1032
a	97	2123
h	104	1107

Kemudian setiap blok tersebut di enskripsi dengan cara:

k = nilai random

m = ASCII

$a = g^k \bmod p$

$b = y^x m \bmod p$

blok blok tersebut dienskripsikan sebagai berikut

$a = 1324^{1223} \bmod 2903$

a = 1643

$b = 331^{1223} * 66 \bmod 2903$

b = 365

$a = 1324^{1996} \bmod 2903$

a = 335

$b = 331^{1996} * 105 \bmod 2903$

b = 1493

a = 1324^{2157} mod 2903

a = 602

b = 331^{2157} * 115 mod 2903

b = 1784

a = 1324^{280} mod 2903

a = 2296

b = 331^{280} * 109 mod 2903

b = 2397

a = 1324^{1873} mod 2903

a = 1455

b = 331^{1873} * 105 mod 2903

b = 2124

a = 1324^{946} mod 2903

a = 81

b = 331^{946} * 108 mod 2903

b = 1993

a = 1324^{299} mod 2903

a = 1770

$b = 331^{299} * 108 \bmod 2903$

$b = 1201$

$a = 1324^{1074} \bmod 2903$

$a = 2246$

$b = 331^{1074} * 97 \bmod 2903$

$b = 636$

$a = 1324^{1737} \bmod 2903$

$a = 486$

$b = 331^{1737} * 104 \bmod 2903$

$b = 1283$

jadi cipper yang dihasilkan

chipperASCII:

1643 365 335 1493 602 1784 2296 2397 1455 2124 81 1993 1770 1201 2246 636 486 1283

Cipper text:

□ ਬਉ ़ ي 3ڵ ा८ ЛП □ ́ □ Ûჯ Ƅफ ɤ

Gambar 3-3 Flowcart Enskripsi Pesan ElGamal

Untuk dapat membaca pesan dalam bentuk Cipher text perlu dilakukan proses dekripsi pesan, dengan cara :

$m=b * a^{(p-1-x)} \bmod p$

m = 2237 * 299 ^ (2903 - 1 - 1794) mod 2903

m = 66

m = 1621 * 800 ^ (2903 - 1 - 1794) mod 2903

m = 105

m = 1972 * 1700 ^ (2903 - 1 - 1794) mod 2903

m = 115

m = 80 * 192 ^ (2903 - 1 - 1794) mod 2903

m = 109

m = 761 * 25 ^ (2903 - 1 - 1794) mod 2903

m = 105

m = 273 * 1510 ^ (2903 - 1 - 1794) mod 2903

m = 108

m = 897 * 2450 ^ (2903 - 1 - 1794) mod 2903

m = 108

m = 1814 * 2790 ^ (2903 - 1 - 1794) mod 2903

m = 97

m = 1376 * 1433 ^ (2903 - 1 - 1794) mod 2903

m = 104

Plain text ASCII:

66 105 115 109 105 108 108 97 104

Plain text ASCII:

Bismillah

Gambar 3-4 Dekripsi pesan ElGamal

3.2.2 RSA

Algoritma RSA memiliki tiga fungsi utama dalam proses, yaitu: pembentukan kunci, enkripsi, dan deskripsi. Pada proses pembentukan kunci akan menghasilkan dua kunci, yaitu kunci public dan kunci private. Kunci public yang nantinya akan di bagikan kepada pihak penerima yang akan digunakan untuk

proses enkripsi sedangkan kunci private tidak boleh dibagikan oleh siapa pun dan hanya akan disimpan oleh si penerima pesan/pembuat kunci. Proses pembentukan kunci adalah sebagai berikut:

a. Pilih 2 bilangan prima, misalnya p = 17 dan q = 11.
b. Hitung n = pq = 17 × 11 = 187.
c. Hitung m = (p – 1)(q – 1) = 16 × 10 = 160.
d. Pilih nilai e sedemikian sehingga relatif prima terhadap m = 160 dan kurang dari 187 kita pilih e = 7.
e. Hitung d sedemikian sehingga de ≡ 1 (mod 160) dan d < 160.Nilai yang didapatkan d = 23, karena 23 × 7 = 161 = (1 × 160) + 1; d dapat dihitung dengan Extended Euclidean Algorithm.
f. Sehingga dapat diperoleh pasangan Kunci Publik {d,n}={7,187} dan Kunci Privat {e,n}={23, 187}

Setelah diketahui kunci public dengan kunci private selanjutnya adalah proses enkripsi, Proses ini dimulai dari plaint text dirubah ke blok-blok karakter dan setiap karakter dulu konversikan kedalam kode ASCII.

Setelah itu setiap blok ASCII tersebut dimasukan dalam persamaan

$C = P^e \bmod n$

C=chipper text

P=nilai ASCII

E=23

N=187

B = 66 ^{23} mod 187 = 110

i = 105 ^{23} mod 187 = 62

s = 115 ^{23} mod 187 = 4

m = 109 ^{23} mod 187 = 131

i = 105 ^{23} mod 187 = 62

l = 108 ^{23} mod 187 = 14

l = 108 ^{23} mod 187 = 14

a = 97 ^{23} mod 187 = 58

h = 104 ^{23} mod 187 = 26

Proses selanjutnya adalah untuk mengembalikan cipher text ke dalam plaint text maka diperlukan proses deskripsi, berikut merupakan proses deskripsi:

$P = C^d \, mod \, n$

P=plaint text

C=nilai ASCII chipper

E=23

N=187

110 ^{7} mod 187 = 66 = B

62 ^{7} mod 187 = 105 = i

$4^{7} \bmod 187 = 115 = s$

$131^{7} \bmod 187 = 109 = m$

$62^{7} \bmod 187 = 105 = i$

$14^{7} \bmod 187 = 108 = l$

$14^{7} \bmod 187 = 108 = l$

$58^{7} \bmod 187 = 97 = a$

$26^{7} \bmod 187 = 104 = h$

3.2.3 Vigenere Chipper

Vigenere Chipper merupakan algoritma kiptografi simetris yang mana hanya memiliki satu kunci untuk proses enkripsi dan deskripsi. Proses enkripsi dan deskripsi menggunakan teknik substitusi yaitu dengan menggeser setiap huruf dengan jumlah yang berbeda-beda di setiap hurufnya. Chipper text diperoleh dengan menggeser index plaint text sebanyak index kunci dengan menggunakan kunci yang sudah ditentukan. Jika panjang kunci lebih pendek daripada panjang teks-asli maka pengunaan kunci diulang. Berikut merupakan contoh enkripsi menggunakan Vigenere Chipper:

Setelah itu setiap blok ASCII tersebut dimasukan dalam persamaan

$C = (P + K - 2 * 3) \bmod 500 + 1$

C= Chipper

P = Plaint text

K = Key

K = “qwerty”

B = (66 + 113(q) - 2 * 3) mod 500 + 1

i = (105 + 119(w) - 2 * 3) mod 500 + 1

s = (115 + 101(e) - 2 * 3) mod 500 + 1

s = (115 + 114(r) - 2 * 3) mod 500 + 1

m = (109 + 116(t) - 2 * 3) mod 500 + 1

i = (105 + 121(y) - 2 * 3) mod 500 + 1

l = (108 + 113(q) - 2 * 3) mod 500 + 1

a = (97 + 119(w) - 2 * 3) mod 500 + 1

h = (104 + 101(e) - 2 * 3) mod 500 + 1

Sehingga diperoleh Chipper

²ß×äàáÜ×Ì

Proses selanjutnya adalah untuk mengembalikan ciphet text ke dalam plaint text maka diperlukan proses deskripsi, berikut merupakan proses deskripsi:

P = (C – K + 500) mod 500 + 1

C= Chipper

P = Plaint text

K = Key

K = “qwerty”

² = (178 - 113(q) + 500) mod 500 + 1

ß = (223 - 119(w) + 500) mod 500 + 1

× = (215 - 101(e) + 500) mod 500 + 1

ä = (228 - 114(r) + 500) mod 500 + 1

à = (224 - 116(t) + 500) mod 500 + 1

á = (225 - 121(y) + 500) mod 500 + 1

Ü = (220 - 113(q) + 500) mod 500 + 1

× = (215 - 119(w) + 500) mod 500 + 1

Ì = (204 - 101(e) + 500) mod 500 + 1

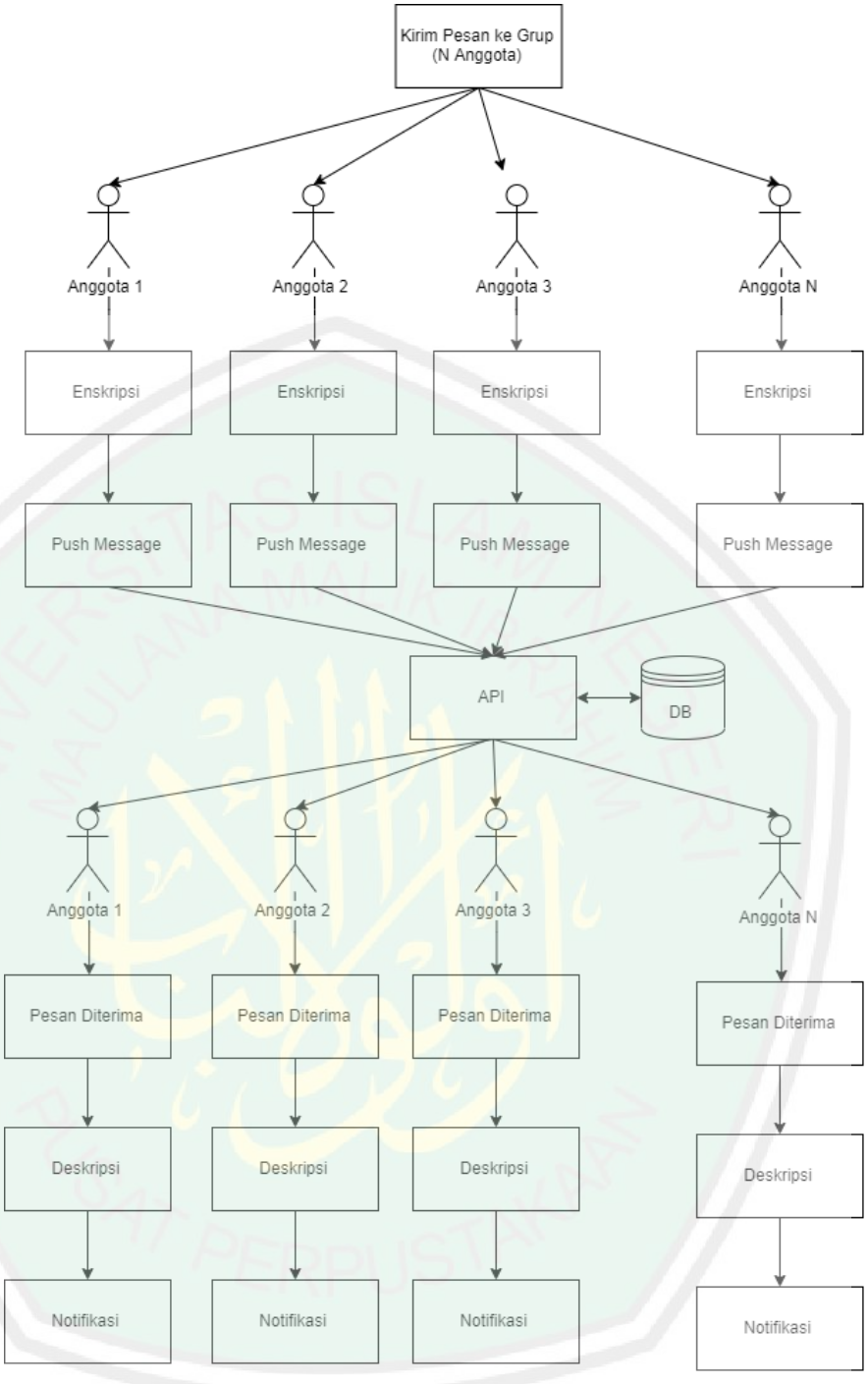
Sehingga didapatkan kembali plait text

Bismillah

3.3 Arsitektur Grup Chat

Aplikasi chat yang tidak di enkripsi biasanya menggunakan “server-side fan-out” untuk pesan grup. Seorang klien yang ingin mengirim pesan ke sekelompok pengguna mentransmisikan satu pesan, yang kemudian didistribusikan N kali ke N anggota grup yang berbeda oleh server (Tamori, Bhujade, Sinhal, & Professor, 2018).

Berbeda dengan aplikasi chat tanpa enkripsi pada aplikasi chat yang menggunakan enkripsi menggunakan "client-side fan-out" di mana klien akan mengirimkan satu pesan N kali ke N anggota grup yang berbeda itu sendiri.



Gambar 3-5 Arsitektur Grup Chat

3.4 Spesifikasi Aplikasi

Aplikasi yang dibangun untuk client memiliki kemampuan diantaranya.

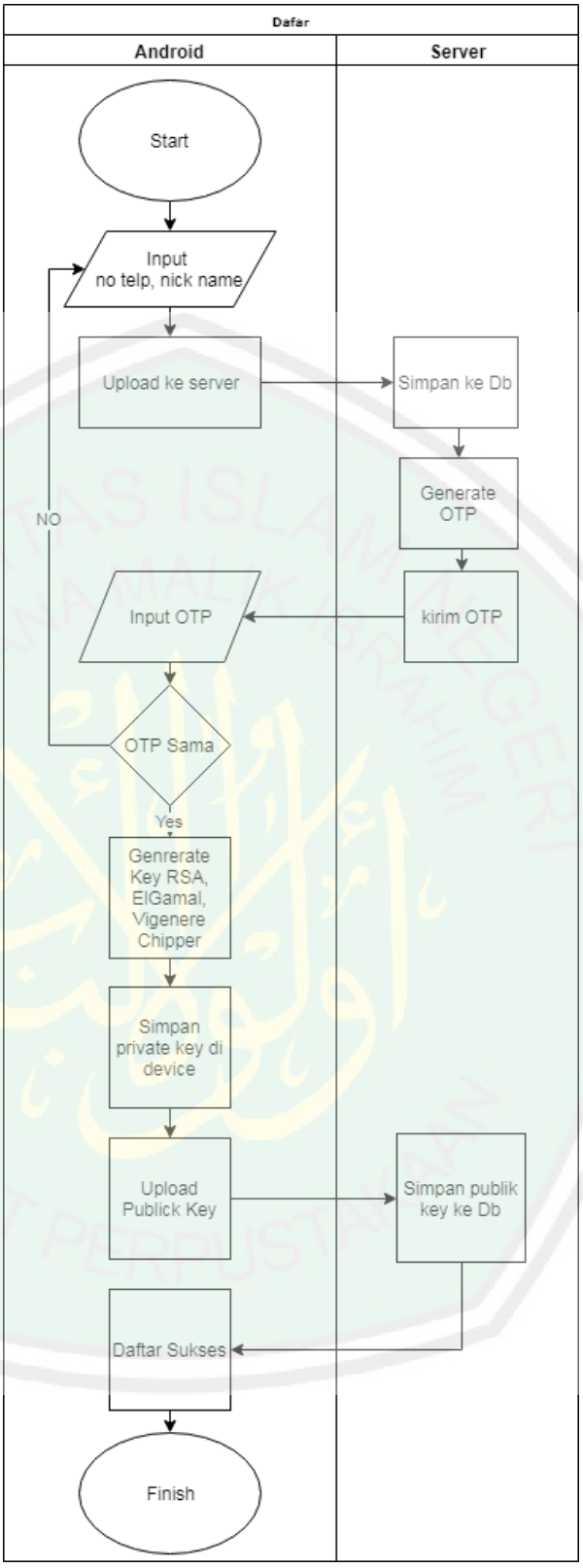
1. Daftar
2. Kirim pesan (Grup dan pribadi)
3. Terima pesan (Grup dan pribadi)
4. Buat kontak
5. Buat group

3.5 Activity Diagram

Activity diagram bermaksud memperlihatkan banyak jalan aktivitas pada sistem yang dibangun, bagaimana setiap alur berawal, kemudian decision yang mungkin terjadi, dan kemudian bagaimana mereka berakhir. Activity diagram juga bisa menggambarkan tahap paralel yang bisa terjadi pada eksekusi.

1. Activity Diagram daftar/login

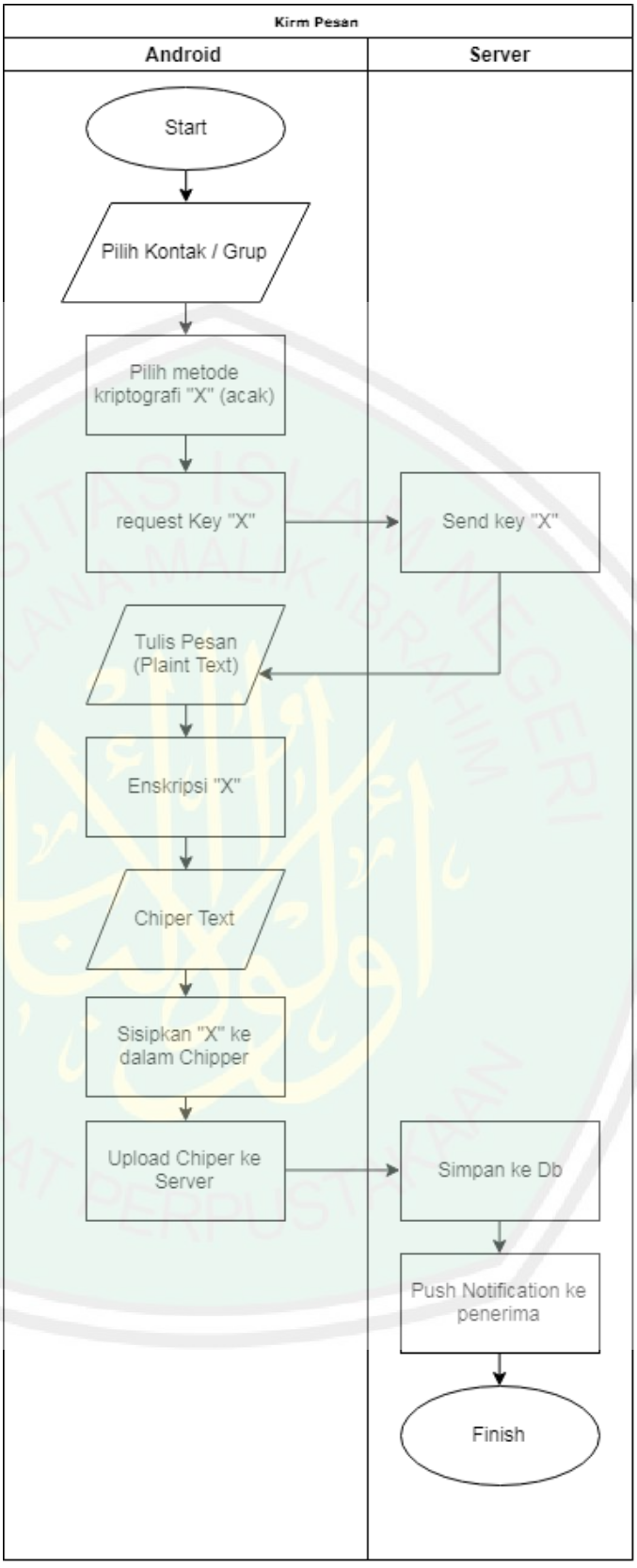
   Berikut merupakan activity diagram daftar/login yang dilakukan oleh user untuk dapat menggunakan aplikasi, pertama user cukup menginputkan no telp, dan nick name saja, lalu system akan mengirim kode OTP kemudian user memasukan kode OTP sebagai konfirmasi, yang akan ditnjukan pada **Gambar 3 7.**



Gambar 3-6 Activity diagram login/daftar

2. Activity Diagram Kirim pesan

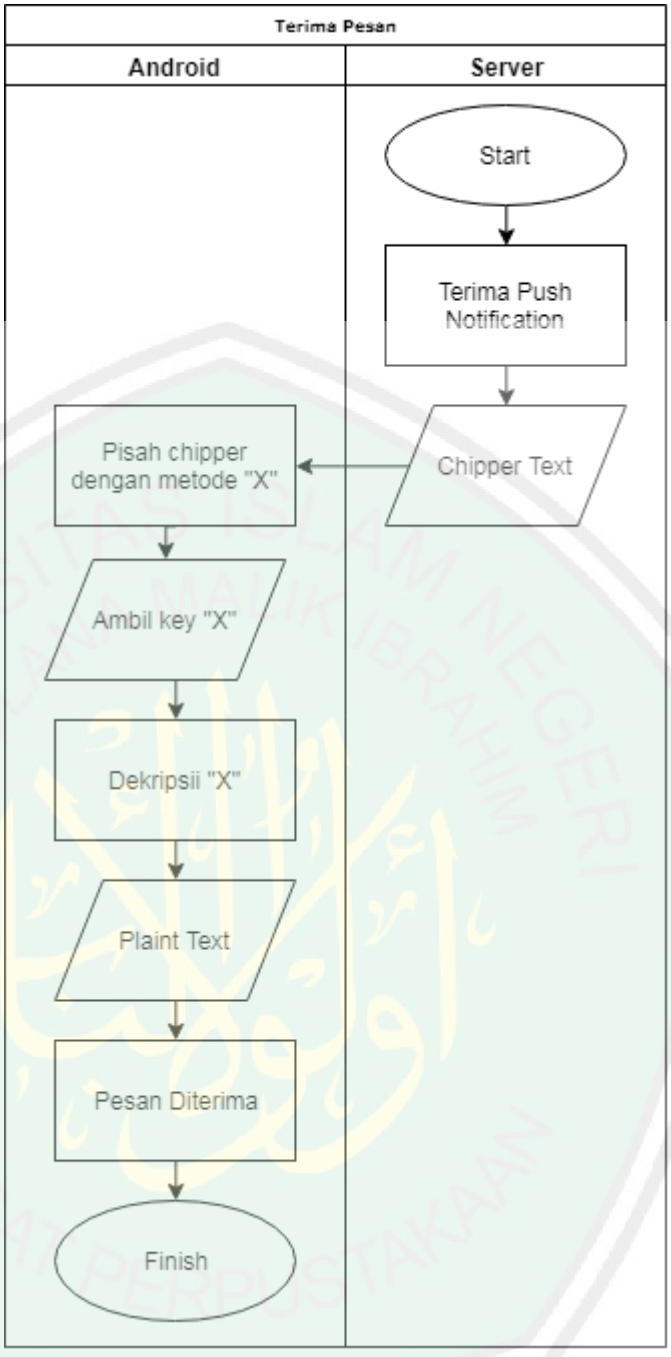
Berikut merupakan activity diagram kirim pesan, pertama user cukup memilih kontak / grup lalu menginputkan isi pesan yang akan dikirim, lalu system akan menentukan metode enkripsi “X” pesan secara acak, mengambil kunci public dari metode “X” untuk mengenkripsi pesan setelah itu system melakukan enkripsi dengan kunci public tersebut dan mengirim hasil enkripsi (chipper text) ke server, yang akan ditnjukan pada **Gambar 3 8.**



Gambar 3-7 Activity Diagram Kirim Pesan

3. Activity Diagram Terima pesan

   Berikut merupakan activity diagram terima pesan, pertama sistem menerima notifikasi berisi pesan dalam bentuk chipper text setelah itu system akan memecah chipper text dangan key “X” yang berisi kiptografi yang digunakan dalam mengenkripsi pesanan lalu system mengambil kunci public dan kunci private untuk mendekripsi pesan setelah itu system memunculkan notifikasi kepada user, yang akan ditnjukan pada **Gambar 3 9**.



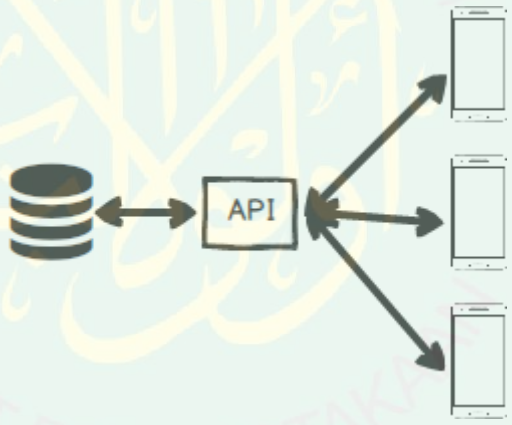
Gambar 3-8 Terima Pesan

3.6 API

API merupakan singkatan dari Application Programming Interface, yang mana memungkinkan developer untuk mengintegrasikan dua bagian dari aplikasi

atau dengan aplikasi yang berbeda secara bersamaan. Berikut merupakan beberapa fungsi dari API, antara lain:

1. Mendukung fungsi CRUD yang bekerja melalui HTTP protocol dengan method GET, POST, PUT dan DELETE
2. Memiliki response Accept Header dan HTTP status code
3. Response dengan format JSON, XML atau format apapun yang kamu inginkan. Akan tetapi kebanyakan digunakan kedalam format JSON.
4. Mendukung fitur MVC seperti routing, controllers, action results, filter, model, IOC container, dll.
5. Web API dapat berjalan di Apache atau web server lainnya yang didukung sesuai bahasa pemrograman yang digunakan.



Gambar 3-9 Alur Kerja API

Pada penelitian ini penulis menggunakan framework Code Igniter sebagai API pada aplikasi yang akan dibuat yang mana memiliki fungsi antara lain:

1. Mengambil pesan
2. Mengirim pesan

3. Menambah kontak
4. Menampilkan kontak
5. Mengubah kontak

3.7 Langkah-Langkah Pengujian

Pada langkah-langkah pengujian penulis akan menguji tingkat efisien keamanan grup chat menggunakan kombinasi metode algoritma RSA, ElGamal, dan Vigenere Chipper.

3.7.1 Langkah Pertama

Pada langkah pertama penulis akan menguji kesesuaian data setelah melewati proses enkripsi dan deskripsi. Parameter yang menjadi ukuran dalam pengujian ini adalah metode kiptografi yang digunakkan, panjang plaint text, besaran kunci yang digunakan, isi plaint text (huruf, angka, symbol unik)

3.7.2 Langkah Kedua

Pada langkah kedua penulis akan menguji seberapa besar pembengkakan ukuran data dari plaint text ke chipper text. Parameter yang menjadi ukuran dalam pengujian ini adalah metode kiptografi yang digunakkan, panjang plaint text.

3.7.3 Langkah Ketiga

Pada langkah ketiga penulis akan menguji seberapa lama waktu yang digunakan untuk pengirim dalam proses mengenkripsi pesan, waktu dihitung sejak pengirim menekan tombol kirim sampai dengan pesan terkirim ke server. Dan seberapa lama waktu yang digunakan penerima dalam proses mendeskripsikan pesan, waktu dihitung sejak pesan masuk sampai dengan pesan

selesai di dekripsikan. Parameter yang menjadi ukuran dalam pengujian ini adalah metode kiptografi yang digunakkan.

3.7.4 Langkah Keempat

Pada langkah keempat penulis akan menguji kekuatan chipper untuk didekripsikan kembali oleh penyerang untuk mengetahui probabilitas ditemukannya text asli. Pengujian dilakukan dalam berbagai skenario, yaitu.

- Probabilitas ditebaknya metode yang digunakan oleh responden
- Banyak kemungkinan didekripsikanya kembali dengan brute force

BAB 4

PEMBAHASAN

4.1 Antarmuka Aplikasi

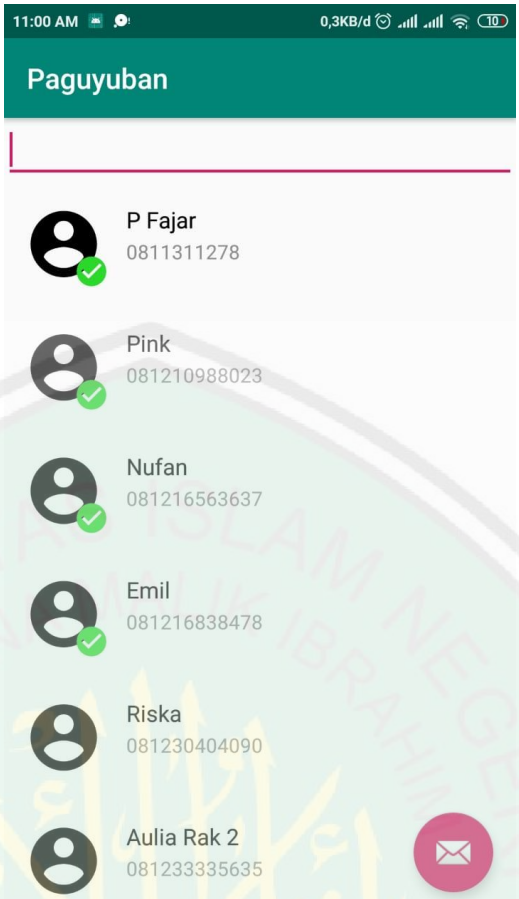
Tampilan Beranda Aplikasi adalah sebuah list grup dimana user menjadi anggotanya yang berisi nama grup, isi pesan terakhir, dan waktu pesan terakhir.

Gambar 4-1 Beranda

Tampilan Chating merupakan tampilan dimana user dapat mengirim dan menerima pesan yang mana pesan tersebut sudah diamankan oleh enskripsi. Tampilan chating terdapat nama grup, isi pesan, pengirim pesan, dan waktu dari pesan terrkirim.

Gambar 4-2 Chating

Buat Grup merupakan tampilan untuk membuat grup dengan cara menambahkan anggota pada list kontak.



Gambar 4-3 Buat Grup

4.2 Uji Coba

Untuk uji coba sistem penguji membuat 5000 user dummy yang memiliki kunci public dan kunci private yang berbeda-beda, kunci tersebut user dummy ini akan dijadikan sebagai objek testing. User dummy tersebut dikempokan menjadi 5 kelompok berdasarkan besaran kunci yang dimikinya. Untuk algoritma RSA, dan ElGamal setiap kunci pada user tersebut degenerate secara acak dengan range yang sesuai dengan kelompok user tersebut lalu key tersebut dipakai untuk menciptakan kunci public dan kunci private. Sedangkan untuk Algoritma Vigenere Cipher dikelompokkan berdasarkan jenis kunci yang dipakai

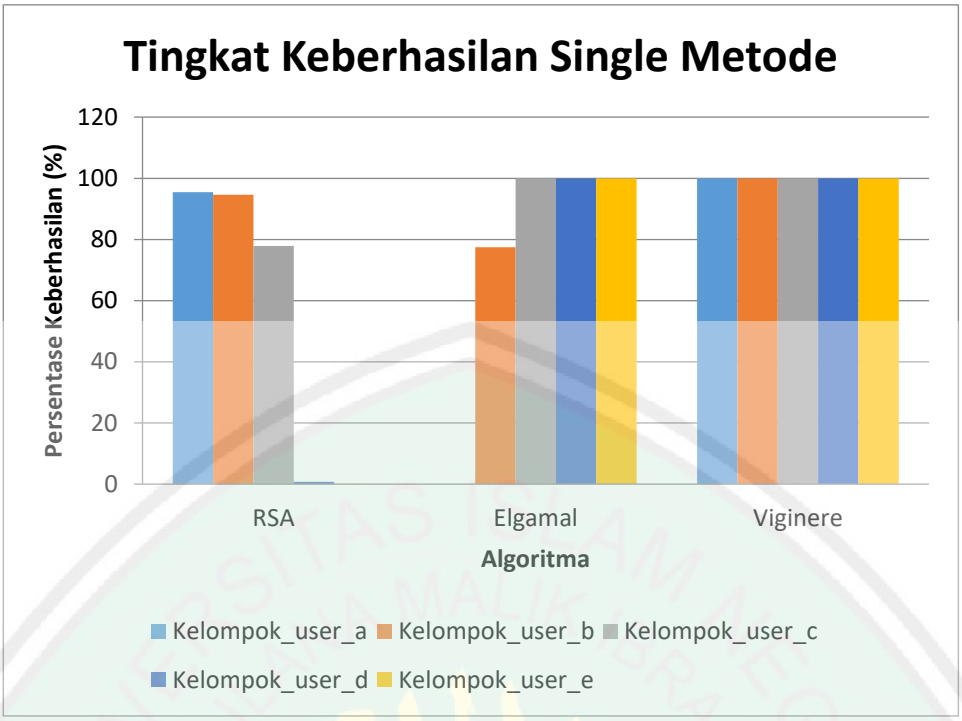
Tabel 4.1 Kelompok User

Kelompok User	Range key (RSA & ElGamal)	Jenis Kunci (Vigenere Cipher)	Banyak
Kelompok_user_a	10 - 100	Huruf (low case)	1000 users
Kelompok_user_b	100 - 200	Huruf (low case + Uppercase)	1000 users
Kelompok_user_c	200 - 300	Huruf (low case + Uppercase) + angka	1000 users
Kelompok_user_d	300 - 400	Huruf (low case + Uppercase) + angka + simbol unik	1000 users
Kelompok_user_e	400 - 500	Huruf (low case + Uppercase) + angka + simbol unik	1000 users
Total			5000 users

4.2.1 Uji Coba Pertama

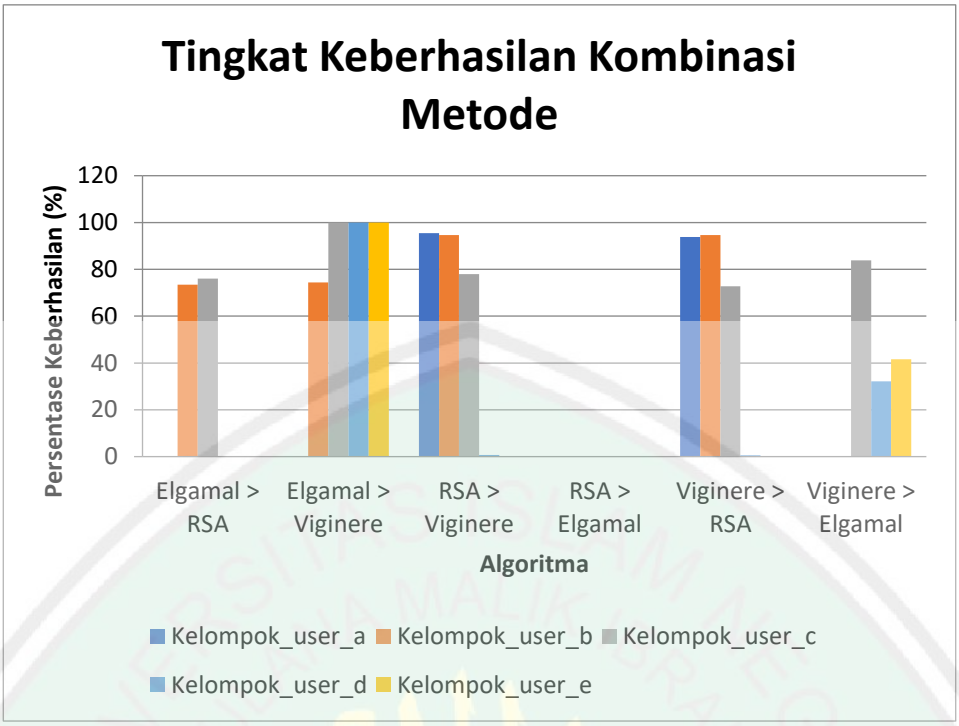
Pada uji coba pertama penulis akan menguji kesesuaian data setelah melewati proses enkripsi dan deskripsi. Parameter yang menjadi ukuran dalam pengujian ini adalah metode kiptografi yang digunakkan, besaran kunci yang digunakan.

Pada uji coba ini penulis mengelompokkan berdasarkan algoritma yang digunakan terlebih dahulu, setelah itu penulis akan menguji berdasarkan besaran kunci. Besaran kunci yang dipakai diambil sesuai dengan Table 4.1



Gambar 4-4 Tingkat Keberhasilan Enskripsi Dekripsi Single Metode

Pada gambar 4.4 pengujian dilakukan dengan cara melakukan proses enskripsi menggunakan single metode dan mendekripsikannya kembali sebanyak 1000 kali untuk setiap sigle metode, kelompok user. Lalu pengujian dilakukan dengan menghitung banyak data yang berhasil didekripsikan kembali dan menghitung presentase data yang berhasil dengan total banyak percobaan. Sehingga dapat disimpulkan dari pengujian tingkat keberhasilan enskripsi dekripsi single metode memiliki total percobaan sebanyak 45.000 total percobaan dengan 30.876 percobaan yang berhasil dengan rata-rata keberhasilan sebanyak 68,6%. Sehingga dapat diperoleh bahwa metode *vigenere cipher* memiliki tingkat keberhasilan paling tinggi yaitu sebesar 100% sedangkan RSA memiliki tingkat keberhasilan terendah.



Gambar 4-5 Tingkat Keberhasilan Enskripsi Dekripsi Kombinasi Metode

Pada gambar 4.5 pengujian dilakukan dilakukan pengujian enskripsi dekripsi menggunakan kombinasi metode. Berdasaraan tabel tersebut dapat disimpulkan dari pengujian tingkat keberhasilan enskripsi dekripsi single metode memiliki total percobaan sebanyak 90.000 total percobaan dengan 28.628 percobaan yang berhasil dengan rata-rata keberhasilan sebanyak 31,8%. Sehingga dapat diperoleh kombinasi metode RSA > Elgamal memiliki tingkat keberhasilan paling rendah sedangkan Elgamal > Vigenere memiliki tingkat keberhasilan tertinggi.

Pada uji coba pertama dapat disimpulkan bahwa tingkat keberhasilan menggunakan siggle metode lebih besar dari pada menggunakan kombinasi metode dengan, yaitu dengan nilai 68,6 % untuk single metode dan 31,7 % untuk

kombinasi metode, dengan nilai tersebut terjadi penurunan tingkat keberhasilan dari single metode ke kombinasi metode sebanyak 46,2%. Sehingga dapat diperoleh bahwa kegagalan proses enskripsi dekripsi semakin besar dikarenakan semakin beras kunci yang dipakai dan semakin besar ukuran karakter(ASCII) maka persentasi kegagalan akan semakin besar. Hal ini disebabkan oleh keterbatasan unicode karakter yang hanya bisa menampung data sebesar 16-bit atau minimum \u0000 (0) sampai dengan \uffff (65.535).

4.2.2 Uji Coba Kedua

Pada uji coba kedua penulis akan menguji seberapa besar pembengkakan ukuran data dari plaint text ke chipper text. Pembengkakan data dilihat berdasarkan perbandingan plaint text dengan chipper text. Parameter yang menjadi ukuran dalam pengujian ini adalah size pesan dan metode kiptografi yang digunakkan.

Tabel 4.2 Peningkatan Size Single Metode

No	Metode	size awal	size akhir	Peningkatan %
1	RSA	10	10	100
2		20	20	
3		40	40	
4		80	80	
5		160	160	
6	Elgamal	10	20	200
7		20	40	
8		40	80	
9		80	160	
10		160	320	
11	Vigenere	10	10	100
12		20	20	
13		40	40	
14		80	80	

15		160	160	
Rata-rata peningkatan pada sigle metode				133,33333

Pada tabel tabel 4.4 pengujian dilakukan dengan cara melakukan proses enskripsi menggunakan single metode dengan size pesan yang berbed. Lalu pengujian dilakukan dengan menghitung size plaint text, size Cipher text, dan menghitung presentase peningkatan size pesan dari plain text keCipher text. Sehingga dapat disimpulkan dari peningkatan size pesan menggunakan single metode sebanyak 133,3%

Tabel 4.3 Peningkatan Size Antara Kombinasi Metode

No	Metode	size awal	size akhir	Peningkatan %
1	RSA > Elgamal	10	20	200
2		20	40	
3		40	80	
4		80	160	
5		160	320	
6	RSA > Viginere	10	10	100
7		20	20	
8		40	40	
9		80	80	
10		160	160	
11	Elgamal > RSA	10	20	200
12		20	40	
13		40	80	
14		80	160	
15		160	320	
16	Elgamal > Vigenere	10	20	200
17		20	40	
18		40	80	
19		80	160	
20		160	320	
21	Viginere > RSA	10	10	100
22		20	20	
23		40	40	

24		80	80	
25		160	160	
26	Viginere > Elgamal	10	20	200
27		20	40	
28		40	80	
29		80	160	
30		160	320	
Rata-rata peningkatan pada sigle metode				166,66667

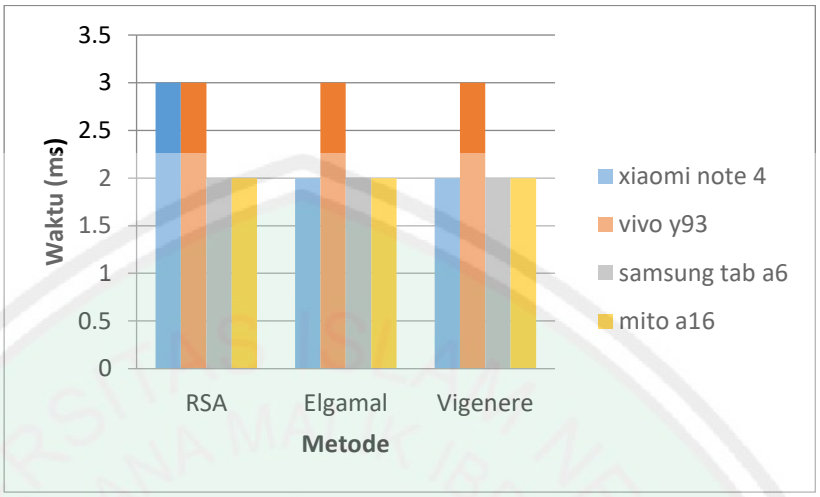
Pada tabel tabel 4.5 pengujian dilakukan dengan cara melakukan proses enskripsi menggunakan kombinasi metode dengan size pesan yang berbeda. Lalu pengujian dilakukan dengan menghitung size plaint text, size Cipher text, dan menghitung presentase peningkatan size pesan dari plain text keCipher text. Sehingga dapat disimpulkan dari peningkatan size pesan menggunakan single metode sebanyak 166,6%

Pada uji coba kedua dapat disimpulkan bahwa size pesan menggunakan kombinasi metode lebih besar dari pada menggunakan single metode dengan, yaitu dengan nilai 133,3 % untuk single metode dan 166,6 % untuk kombinasi metode, dengan nilai tersebut terjadi peningkatan size pesan dari single metode ke kombinasi metode sebanyak 80%. Sehingga dapat diperoleh peningkatan size pesan meningkat dikarenakan terdapat algoritma Elgamal yang mana memiliki karakteristik dimana cipher yang dihasilkan meningkat sebanyak 2x dari pesan asli.

4.2.3 Uji Coba Ketiga

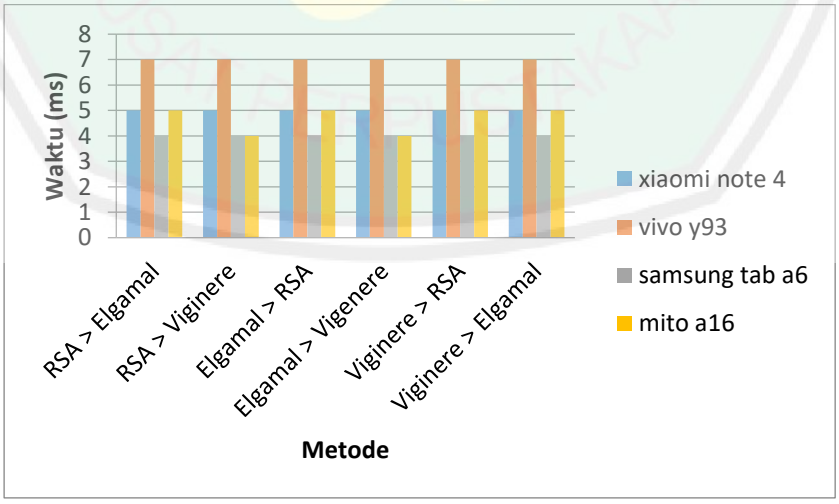
Pada uji coba ketiga penulis akan menguji seberapa lama waktu yang digunakan untuk pengirim dalam proses mengenkripsi pesan, dan seberapa lama

waktu yang digunakan penerima dalam proses mendeskripsikan pesan, waktu dihitung sejak pesan masuk sampai dengan pesan selesai didekripsikan.



Gambar 4-6 Banyak Waktu Enskripsi Menggunakan Single Metode

Pada Gambar 4.6 pengujian dilakukan dengan cara melakukan proses enskripsi dan dekripsi menggunakan single metode dan untuk mengetahui rata-rata banyak waktu yang digunakan permetode maka diperlukan pengujian langsung dengan beberapa device. Dapat disimpulkan dari peningkatan size pesan menggunakan single metode sebanyak 2,3 ms.



Gambar 4-7 Banyak Wakt,u Enskripsi Menggunakan Kombinasi Metode

Pada Gambar 4.7 pengujian dilakukan dengan cara melakukan proses enskripsi dan dekripsi menggunakan kombinasi metode dan untuk mengetahui rata-rata banyak waktu yang digunakan permetode maka diperlukan pengujian langsung dengan beberapa device. Dapat disimpulkan dari peningkatan size pesan menggunakan single metode sebanyak 5,1 ms.

Pada uji coba ketiga dapat disimpulkan bahwa banyak waktu yang digunakan untuk proses enskripsi-dekripsi menggunakan kombinais metode lebih besar dari pada menggunakan single metode dengan, yaitu dengan 2,3 ms untuk single metode dan 5,1 ms untuk kombinasi metode, dengan nilai tersebut terjadi peningkatan konsumsi waktu dari single metode ke kombinasi metode sebanyak 45%. Sehingga dapat diperoleh konsumsi waktu pada kombinasi metode lebih lama jika dibandingkan dengan single metode, dan konsumsi waktu juga tergantung pada spesifikasi *device* yang digunakan, semakin tingga spesifikasinya maka semakin sedikit waktu yang diperlukan.

4.2.4 Uji Coba keempat

Pada langkah keempat penulis akan menguji kekuatan chipper untuk didekripsikan kembali oleh penyerang untuk mengetahui probabilitas ditemukannya text asli. Pengujian dilakukan dalam berbagai skenario, yaitu.

4.2.4.1 Probalitas Ditebaknya Metode Yang Digunakan Oleh Responden

Pada langka ini penulis melakukan servei terhadap beberapa responden untuk menebak metode apa yang digunakan, sebelumnya para responden akan diberi pengetahuan tentang kiptografi terutama oleh penulis sendiri secara singkat

kemudia paraa responden menebak metode yang digukanan didalam beberapa Cipher, Hasilnya adalah sebagai berikut.

Tabel 4.4 Hasil Tebak oleh Responden

no	Metode yang digunakan		Responden	metode yang ditebak oleh responden		persentase tertebak (%)	
	Metode 1	Metode 2		Metode 1	Metode 2	single	kombinasi
1	Elgamal	RSA	Arinal Rifqi	RSA	Vigenere	50	20
			Maskur Hadi	Elgamal	Vigenere		
			Afifudin Zhuri	Vigenere	RSA		
			Zainur Ridho	Elgamal	RSA		
			Firhan Prayoga	Vigenere	RSA		
2	Elgamal	Vigenere	Arinal Rifqi	Vigenere	RSA	40	20
			Maskur Hadi	Elgamal	Vigenere		
			Afifudin Zhuri	Elgamal	Elgamal		
			Zainur Ridho	RSA	Vigenere		
			Firhan Prayoga	RSA	Elgamal		
3	RSA	Elgamal	Arinal Rifqi	Elgamal	Vigenere	40	0
			Maskur Hadi	RSA	Elgamal		
			Afifudin Zhuri	Vigenere	Elgamal		
			Zainur Ridho	RSA	RSA		
			Firhan Prayoga	RSA	Vigenere		
4	RSA	Vigenere	Arinal Rifqi	RSA	Elgamal	30	0
			Maskur Hadi	Vigenere	RSA		
			Afifudin Zhuri	RSA	RSA		
			Zainur Ridho	Elgamal	Vigenere		
			Firhan Prayoga	Elgamal	Elgamal		
5	Vigenere	Elgamal	Arinal Rifqi	Vigenere	RSA	20	0
			Maskur Hadi	Elgamal	RSA		
			Afifudin Zhuri	Elgamal	Vigenere		
			Zainur Ridho	Elgamal	RSA		
			Firhan Prayoga	Vigenere	Elgamal		
6	Vigenere	RSA	Arinal Rifqi	RSA	Elgamal	20	0
			Maskur Hadi	Vigenere	RSA		
			Afifudin Zhuri	RSA	RSA		
			Zainur Ridho	Elgamal	Vigenere		
			Firhan Prayoga	Elgamal	Elgamal		
Rata-rata tertebaknya metode yang digunkan oleh responden						33,33	6,66

Pada tabel tabel 4.9 pengujian dilakukan dengan cara melakukan survei terhadap responden. Dalam survei tersebut setiap responden diharuskan menebak 6 Cipher yang dihasilkan dari kombinasi 2 metode. Lalu dihitung persentasi tertebaknya single metode dengan cara membandingkan salah satu metode hasil tebakan responden yang sama dengan metode yang digunakan oleh Cipher dengan banyak semua percobaan. Sedangakan persentase tertebak kombinasi metode didapat dengan cara membandingkan kombinasi metode hasil tebakan responden yang sama dengan kombinasi metode yang digunakan oleh Cipher dengan banyak semua semua kombinasi percobaan.

Pada uji ini dapat disimpulkan bahwa probabilitas tertebaknya metode yang digunakan menggunakan kombinasi metode lebih kecil dari pada menggunakan single metode dengan, yaitu dengan 6,6% untuk kombinasi metode dan 33,3% untuk single metode, dengan nilai tersebut terjadi penurunan probabilitas ditebaknya Cipher oleh responden dari single metode ke kombinasu metode sebanyak 19,8%.

4.2.4.2 Probabilitas dipecahkannya Cipher dengan *Brute Force*

Pada langka ini penulis akan menghitung seberapa banyak kemungkinan didekripsinya kembali Cipher menggunakan metode *brute force*, *brute force* sendiri merupakan metode mengalahkan skema kriptografi dengan mencoba semua kemungkinan password atau kunci(Wicaksono, 2013). disini penulis mempersempit kemungkinan dengan beranggapan bahwa penyerang mengetahui sistem peningkatan keamanan menggunakan kombinasi 2 metode dari 3 metode yang dipakai maka didapatkan hanya 6 kemungkinan metode yang dipakai.

Setalah mengetahui kemungkinan metode yang dipakai penyerang juga harus menebak kunci yang dipakai, untuk mempersempit kemungkinan kunci yang harus dicoba hanya dengan persentasi kesesuain diatas 90% sesuai padauji coba pertama, sehingga didapatkan batas kunci sebagai berikut.

Tabel 4.5 Banyak Percobaan Dipecahkannya Cipher Text Single Metode

Metode	Range	kunci yang dibutuhkan	total kemungkinan
RSA	10-200	Angka prima p (42 kemungkinan)	74.088
		Angka prima q (42 kemungkinan)	
		Angka prima m (42 kemungkinan)	
Elgamal	200-500	Angka prima p (49 kemungkinan)	4.410.000
		Angka Desiamal g (300 kemungkinan)	
		Angka Desiamal x (300 kemungkinan)	
Viginere	Huruf (low case + Uppercase) + angka + simbol unik	key (65276 kemungkinan)	1.044.416
Rata-rata banyak percobaan dipecahkannya Cipher text			2.727.208

Pada tabel tabel 4.9 pengujian dilakukan dengan menghitung banyak total kemungkinan dengan cara mengalikan banyak kunci yang dibutuhkan. Banyak kunci yang dibutuhkan didapatkan dari banyak key yang berada diantara range. Sehingga didapatkan rata-rata dari total kemungkinan menggunakna single kombinasi adalah sebesar 2.272.208 banyak kemungkinan.

Tabel 4.6 Tabel Banyak Percobaan Dipecahkannya Cipher Text Kombinasi Metode

Kombinasi metode	banyak kemungkinan percobaan (metode 1 * metode 2)	jumlah percobaan metode 1 * metode 2
ElGamal -> RSA	4.410.000 * 74.088	326.728.080.000
ElGamal -> Vigenere Chipper	4.410.000 * 1.044.416	4.605.874.560.000

RSA -> Elgamal	74.088 * 4.410.000	326.728.080.000
RSA -> Vigenere Chipper	74.088 * 1.044.416	77.378.692.608
Vigenere Chipper -> ElGamal	1.044.416 * 4.410.000	4.605.874.560.000
Vigenere Chipper -> RSA	1.044.416 * 74.088	77.378.692.608
Rata-rata banyak percobaan dipecahkannya Cipher text		1.669.993.777.536

Pada tabel tabel 4.10 pengujian dilakukan dengan menghitung banyak total kemungkinan dari kombinasi metode dengan cara mengalikan banyak kemungkinan metode 1 dengan metode 2 yang didapatkan dari Tabel 4.10. Sehingga didapatkan rata-rata dari total kemungkinan menggunakan kombinasi adalah sebesar 1.669.993.777.536 banyak kemuungkinan.

Pada uji Probabilitas dipecahkannya Cipher dengan *Brute Force* dapat disimpulkan bahwa banyak percobaan yang digunakan untuk proses enskripsi-dekripsi menggunakan kombinasi metode lebih besar dari pada menggunakan single metode dengan, yaitu sebanyak 2.272.208 kemungkinan untuk rata-rata single metode dan 1.669.993.777.536 kemungkinan untuk rata-rata kombinasi metode, dengan nilai tersebut terjadi penurunan probabilitas dipecahkannya Cipher dari single metode ke kombinasi metode meningkat sebanyak 73.496.518,7%. Hal ini sesuai dengan pernyataan (Wicaksono, 2013) semakin banyak usaha *brute force* maka semakin banyak waktu yang dibutuhkan untuk mendekripsikan pesan dan semakin sulit pula dibobol menggunakan *brute force attack.*

Dengan meningkatnya banyak usaha *brute force* maka tingkat keamanan enskripsi juga semakin meningkat dan pesan yang dikirim oleh pengguna jauh

lebih aman, kerahasiaan pesan merupakan amanah dari pengguna yang harus dijaga. Menyangkut hal tersebut Allah berfirman dalam surah annisa ayat 58:

نِعِمَّا اللَّهَ إِنَّ ۚ بِالْعَدْلِ تَحْكُمُوا أَنْ النَّاسِ بَيْنَ حَكَمْتُمْ وَإِذَا أَهْلِهَا إِلَىٰ الْأَمَانَاتِ تُؤَدُّوا أَنْ يَأْمُرُكُمْ اللَّهَ إِنَّ

بَصِيرًا سَمِيعًا كَانَ اللَّهَ إِنَّ ۗ بِهِ يَعِظُكُمْ

"*Sesungguhnya Allah menyuruh kamu menyampaikan amanat kepada yang berhak menerimanya, dan (menyuruh kamu) apabila menetapkan hukum di antara manusia supaya kamu menetapkan dengan adil. Sesungguhnya Allah memberi pengajaran yang sebaik-baiknya kepadamu. Sesungguhnya Allah adalah Maha Mendengar lagi Maha Melihat.*"

Menurut Tafsir Al-Muyassar / Kementerian Agama Saudi Arabia surah annisa ayat 58 menjelaskan Sesungguhnya Allah menyuruh kalian menunaikan amanat kepada pemiliknya. Dan Dia menyuruh kalian, apabila kalian memutuskan perkara di antara manusia dalam semua urusan mereka, maka putuskanlah perkara mereka dengan adil, jangan memihak atau zalim dalam memutuskan. Sesungguhnya Allah mengingatkan dan memberi bimbingan yang sebaik-baiknya ke arahnya (menjaga amanat) dalam setiap kondisi kalian. Sesungguhnya Allah Maha Mendengar ucapan-ucapan kalian dan Maha Melihat perbuatan-perbuatan kalian.

Hasil penelitian ini berusaha untuk membuat orang-orang yang memakainya akan melakukan tindakan yang sama sesuai hadist dan firman Allah SWT tersebut, yakni menjaga amanat. Sehingga diharapkan penelitian ini bisa membuat setiap insan yang memakainya mendapatkan manfaat dan kebaikan di dalamnya.

BAB 5

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Setelah dilakukan penelitihan mengenai peningkatan keamanan grup chat menggunakan kombinasi metode RSA, *Elgamal*, dan *Vigener Cipher* untuk mencari perbandingan peningkatan keamanan antara single metode dengan kombinasi metode, maka dapat diambil kesimpulan sebagai berikut:

- Terjadi penurunan tingkat keberhasilan dideskripsikannya pesan kembasi sebesar 30.867 pesan berhasil di deskripsikan dari 45.000 percobaan menurun sebesar 28.628 pesan berhasil di deskripsikan dari 90.000 percobaan, Sehingga terjadi penurunan tingkat keberhasilan sebanyak 46,2%.
- Peningkatan konsumsi waktu rata-rata sebesar 2,3 ms oleh single metode meningkat sebesar 5,1 ms oleh kombinasi metode, Sehingga terjadi peningkatan konsumsi waktu sebanyak 45%.
- Terjadi peningkatan size pesan dari size text asli rata-rata sebesar 62 bit mengingkat rata-rata sebesar 82.6 bit dan meningkat rata-rata sebesar 133.3 bit untuk kombinasi metode, Sehingga terjadi peningkatan size sebesar 80%.
- Terjadi penurunan probabilitas tertebaknya metode yang digunakan oleh responden sebesar 22 metode tertebak dari 60 percobaan untuk single metode, menurun sebesar 2 metode tertebak dari 30 percobaan untuk kombinasi metode, dengan nilai tersebut terjadi penurunan probabilitas ditebaknya Cipher oleh responden dari single metode ke kombinasi metode sebanyak 19,8%.

- Terjadi peningkatan banyak usaha *brute force* yang dilakukan untuk memecahkan chipper sebesar rata-rata 2.272.208 perulangan usaha *brute force* oleh single metode meningkat sebanyak 1.669.993.777.536 perulangan usaha *brute force* oleh single metode, Sehingga terjadi peningkatan usaha brute force sebesar 73.496.518,7%.

5.2 Saran

Penelitih menyedari bahwa penelitian ini jauh dari sempurna. Adapun saran untuk penelitihan lebih lanjut agar penelitihan ini lebih baik adalah sebagai berikut:

- Penelitihan selanjutnya diharapkan dapat mempertimbangkan kunci yang lebih besar.
- Penelitihan selanjutnya diharapkan dapat menghitung besar kunci yang aman dan resposif untuk dipakai pada setiap device.
- Penelitihan selanjutnya diharapkan dapat menambah metode kiptografi lainya sebagai perbandingan.

DAFTAR PUSTAKA

Bing, H., Bo, W., & Hui, Z. (2014). A design and realization of digital signature of e-government management website group based on Elgamal cipher system. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 8351 LNCS*, 143–149. https://doi.org/10.1007/978-3-319-09265-2_16

Chandra. (2016). Keamanan Data Dengan Metode Kriptografi Kunci Publik. *Jurnal TIMES*, *2*(2), 11–15.

Karima, A., Handoko, L. B., & Saputro, A. (2017). Pemfaktoran Bilangan Prima pada Algoritme ElGamal untuk Keamanan Dokumen PDF. *Jurnal Nasional Teknik Elektro Dan Teknologi Informasi (JNTETI)*, *6*(3), 252–258. https://doi.org/10.22146/jnteti.v6i3.326

Kurniawan, G. (2013). *Aplikasi Mobile Enkripsi SMS Menggunakan Metode Vigenere Cipher dan Base64*.

Moran, E. (2017). *End To End Encryption an Answer To Security Concerns in Private Sector*.

Rizal, M. S. (2010). *Implementasi Algoritma Kriptografi Kunci-Publik ElGamal Entuk Keamanan Pengiriman Email*.

Setiawan, R. (2013). *Enkripsi Short Message Service (SMS) dengan Menggunakan Metode RSA pada Smartphone*. i–69.

Seufert, M., Hoβfeld, T., Schwind, A., Burger, V., & Tran-Gia, P. (2016). Group-based communication in WhatsApp. *2016 IFIP Networking Conference (IFIP Networking) and Workshops, IFIP Networking 2016*, 536–541. https://doi.org/10.1109/IFIPNetworking.2016.7497256

Tamori, A., Bhujade, R. K., Sinhal, A., & Professor, A. (2018). Analysis on Whatsapp Security. *International Journal of Ethics in Engineering & Management Education Website: Www.Ijeee.In*, *5*(6), 2348–4748. Retrieved from www.ijeee.in

Wahyuni, A. (2011). Keamanan Pertukaran Kunci Kriptografi dengan Algoritma Hybrid : Diffie-Hellman dan RSA. *Majalah Ilmiah INFORMATiKA*, *2*(2), 15–23.

Wicaksono, L. (2013). Ketahanan Algoritma RSA Terhadap Brute Force Attack. *Jurnal Teknologi*, *1*(1), 69–73. https://doi.org/10.11113/jt.v56.60