PENGAMANAN CHATTING DENGAN ALGORITMA RSA CIPHER PADA PT PRINTMATE BERBASIS ANDROID

Yohanes[1)], **Ferdiansyah**[2)]
Program Studi, Fakultas Teknologi Informasi, Universitas Budi Luhur
Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260
E-mail : yohanes.yp91@gmail.com[1)], ferdiansyah@budiluhur.ac.id [2)]

Abstrak

Sebagai perusahaan yang menjadi supplier bagi dunia percetakan, PT Printmate begitu sering melakukan komunikasi untuk pertukaran informasi atau pesan melalui aplikasi chatting baik dalam perusahaan antara pimpinan dengan karyawan, sesama karyawan maupun dengan customer yang ada, dari kegiatan chatting tersebut sangat penting dalam menjaga kerahasiaan suatu pesan atau informasi yang dilakukan bagi perusahaan. Sehingga aplikasi chatting adalah pilihan yang tepat dalam melakukan kegiatan berkomunikasi, akan tetapi dalam kegiatan komunikasi ini dengan menggunakan aplikasi chatting pada smartphone melalui jaringan internet yang bersifat online ini memunculkan persoalan baru yaitu masalah dari pihak yang sangat tidak bertanggung jawab yang ingin menyadap, mencuri bahkan merubah isi pesan atau informasi penting tersebut untuk kepentingan pribadi dan merugikan perusahaan. Pada penelitian ini akan dibahas mengenai aplikasi chatting menggunakan algoritma RSA Cipher pada PT Printmate yang bertujuan dapat memberikan solusi kepada perusahaan dalam menjaga kerahasiaan informasi atau pesan dan dengan membuat aplikasi chatting berbasis android yang dapat mengenkripsi dan dekripsi isi pesan teks yang ditulis oleh pengguna aplikasi chatting dengan menggunakan algoritma RSA Cipher, sehingga komunikasi pengiriman informasi atau pesan tidak dapat diketahui oleh pihak-pihak yang tidak bertanggung jawab. Aplikasi ini menggunakan bahasa pemprograman Java berbasis Android dan Database MySQL. Dari hasil tersebut dapat disimpulkan bahwa implementasi kriptografi dengan algoritma RSA Cipher untuk pengamanan chatting berhasil dilakukan untuk melindungi pesan atau informasi pada PT Printmate. Aplikasi ini diharapkan mampu mempermudah proses kegiatan chatting yang dilakukan oleh PT Printmate.

Kata kunci: Kriptografi, Chatting, RSA Cipher, Keamanan Informasi.

1. PENDAHULUAN

Chatting adalah kegiatan komunikasi antara satu sama lain dalam bentuk pengiriman pesan *text* dengan media *smartphone* atau sering disebut dengan *handphone* yang melalui jaringan internet. Kegiatan *chatting* ini begitu mudah dilakukan kapan saja dan dimana saja tanpa harus bertemu antara satu sama lainnya sehingga *chatting* menjadi bagian yang tidak bisa dipisahkan dari kehidupan ini maupun dalam dunia kerja karena pengoperasiannya yang begitu mudah dilakukan. Sebagai perusahaan yang menjadi supplier bagi dunia percetakan, PT Printmate begitu sering melakukan komunikasi untuk pertukaran informasi atau pesan melalui aplikasi *chatting* baik dalam perusahaan antara pimpinan dengan karyawan, sesama karyawan maupun dengan customer yang ada, dari kegiatan *chatting* tersebut sangat penting dalam menjaga kerahasiaan suatu pesan atau informasi yang dilakukan bagi perusahaan.

Komunikasi langsung antara satu sama lain sangat mudah dalam menjaga kerahasiaan informasi atau pesan namun memakan waktu dan tempat dari kegiatan komunikasi langsung itu. Dengan adanya aplikasi *chatting* ini sangatlah bermanfaat bagi setiap orang dalam perusahaan untuk melakukan komunikasi langsung tidak harus mengatur waktu dan tempat bertemu, hanya dengan mudah membuka aplikasi *chatting* pada smartphone kapanpun dan dimanapun untuk langsung komunikasi bertukar pesan atau informasi satu sama lain setiap saat. Sehingga aplikasi *chatting* adalah pilihan yang tepat dalam melakukan kegiatan berkomunikasi, akan tetapi dalam kegiatan komunikasi ini dengan menggunakan aplikasi *chatting* pada *smartphone* melalui jaringan internet yang bersifat *online* ini memunculkan persoalan baru yaitu masalah dari pihak yang sangat tidak bertanggung jawab yang ingin menyadap, mencuri bahkan merubah isi pesan atau informasi penting tersebut untuk kepentingan pribadi dan merugikan perusahaan.

Dari persoalan diatas cara mengatasinya ialah dibuatkan aplikasi *chatting* berbasis android pada *smartphone* untuk menjaga kerahasiaan suatu informasi atau pesan yang dilakukan setiap saat dalam kegiatan *chatting* pada PT Printmate.

2. METODE PENELITIAN

2.1. *Chatting*

Chatting ialah fitur atau program di Internet untuk berkomunikasi langsung dengan pengguna internet yang sama dengan menggunakan Internet. *Chatting* tersebut berupa *text* ataupun dapat berupa *voice*. Definisi *chatting* juga berarti suatu pesan *instant* (*instant messaging*) dalam teknologi jaringan komputer yang memungkinkan pengguna mengirim pesan ke pengguna lain yang terhubung dikomputer atau jaringan internet.

Awalnya aplikasi *chat* berbasis desktop, namun sekarang bergeser berdasarkan perangkat *mobile* yang mengikuti jaman saat ini. *Chatting* tidak hanya populer di kalangan remaja tapi sekarang, telah menembus orang dewasa bahkan dalam lingkup pekerjaannya. Popularitas *mobile chat* bisa dikatakan telah menggeser popularitas SMS karena banyak fitur *chatting* dengan biaya rendah. Dalam lingkup kerja aplikasi *chatting* sangat berguna jika orang dalam satu gedung atau antar bagian ingin berkomunikasi dengan cepat tapi tidak bisa saling berhadapan.

Di internet *chatting* adalah ngobrol dengan orang lain yang menggunakan internet secara bersamaan. Biasanya obrolan ini adalah pertukaran pesan *text* yang membutukan server sebagai penyedia layanan dan sejumlah pengguna untuk terlibat dalam obrolan. *Chatting* bisa dilakukan dengan suara (*voice chat*) dan video.

2.2. Algoritma RSA *Cipher*

Algoritma RSA adalah sebuah algoritma berdasarkan skema kriptografi kunci *public*. Nama RSA sebagai diambil dari inisial nama para penemunya: Ron Rivest, Adi Shamir, dan Leonard Adleman. RSA dibuat di MIT pada tahun 1977 dan dipatenkan oleh MIT pada tahun 1983. Setelah bulan September tahun 2000, paten tersebut berakhir, sehingga saat ini semua orang dapat menggunakannya dengan bebas [3].

RSA terbagi menjadi tiga proses, yaitu pembangkitan kunci, enkripsi dan dekripsi. Dasar proses enkripsi dan dekripsi pada algoritma RSA yaitu konsep bilangan prima dan aritmatika modulo. Kunci enkripsi tidak dirahasiakan dan diberikan kepada umum (disebut kunci publik), sedangkan kunci untuk dekripsi bersifat rahasia (disebut kunci pribadi).

2.3.1 Proses Pembangkit Kunci

Algoritma RSA memiliki dua kunci yang berbeda untuk proses enkripsi dan dekripsi. Dalam menentukan dua bilangan prima sebagai kunci adalah bilangan prima yang besar, karena pemfaktoran bilangan dari dua bilangan prima besar sangat sulit, sehingga keamanan pesan lebih terjamin.

Pasangan kunci merupakan elemen penting dari algoritma RSA. Berikut adalah langkah-langkah dalam membangkitkan dua kunci algoritma RSA sebagai berikut:

a. Pilih dua bilangan prima sembarang, p dan q
b. Hitung n = p.q
c. Hitung ø(n) = (p-1) (q-1)
d. Pilih kunci publik e, yang relatif prima terhadap ø(n)
e. Bangkitkan kunci pribadi dengan menggunakan e.d ≡ 1 mod ø(n)

Hasil dari algoritma tersebut akan menghasilkan dua kunci, yaitu kunci publik (e,n) dan kunci pribadi (d,n).

2.3.2 Proses Enkripsi

Berikut ini langkah-langkah dalam melakukan proses enkripsi dengan algoritma RSA Cipher ialah sebagai berikut:

a. Ambil kunci public penerima pesan, e, dan modulus n.
b. Plainteks dibuat menjadi blok-blok m1,m2,m3,…….. sedemikian sehingga setiap blok merepresentasikan nilai di selang [0, n – 1].
c. Setiap blok mi dienkripsi menjadi blok ci dengan rumus ci = mie mod n

2.3.3 Proses Dekripsi

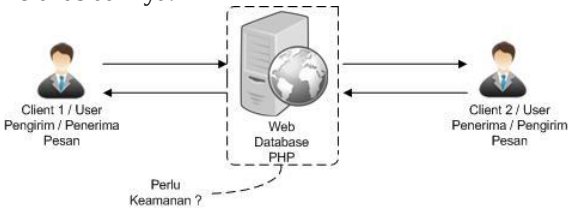
Berikut ini langkah-langkah dalam melakukan proses dekripsi adalah sebagai berikut:

a. Setiap blok chiperteks ci didekripsi kembali menjadi blok mi dengan rumus mi = cid mod n
b. Blok-blok m1,m2,m3,…….. diubah kembali menjadi bentuk huruf dengan kode ASCII.

3. RANCANGAN SISTEM DAN APLIKASI

3.1. Analisa Masalah

Dengan banyak aplikasi *chatting* yang beredar di era online ini maka sangat sulit sekali menjaga keamanan dan kerahasiaan dari kegiatan chatting yaitu pengiriman pesan atau informasi yang rahasia kepada sesama pengguna aplikasi chatting, karena banyak pihak-pihak yang tidak bertanggung jawab yang ingin menyadap, mencuri bahkan merubah isi pesan atau informasi penting tersebut untuk kepentingan pribadi dan yang merugikan perusahaan. Bagi PT Printmate menjaga keamanan suatu isi pesan atau informasi yang rahasia dari kegiatan chatting yang menjadi kebutuhan perusahaan sangatlah penting, supaya informasi tersebut tetap terlindungi. Berdasarkan masalah tersebut perlu rancangan sistem yang dapat melakukan fungsi tersebut, sehingga suatu isi pesan atau informasi dalam kegiatan pengiriman pesan pada aplikasi *chatting* tersebut terlindungi kerahasiaannya.

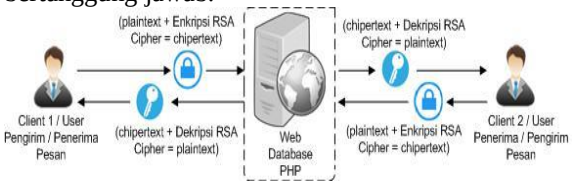


Gambar 1. Ilustrasi Kegiatan Chatting

3.2. Penyelesaian Masalah

Dari permasalahan yang telah diuraikan di atas, diperlukan adanya sebuah aplikasi yang dapat menjaga kerahasiaan dari suatu pesan atau informasi dalam melakukan kegiatan pada aplikasi *chatting*. Sehingga keberadaan pesan atau informasi tersebut tidak terdeteksi oleh pihak lain yang tidak berhak atas informasi tersebut. Aplikasi tersebut nantinya dapat mengamankan jalur dari kegiatan chatting yang ada yaitu dengan mengenkripsi dan mengdekripsi informasi atau pesan rahasia ke dalam wadah penampung database MSQL. Pengguna pertama (pengirim pesan) dapat mengirimkan pesan yang telah di enkripsi dengan algoritma RSA tersebut melalui jalur aplikasi *chatting*, kemudian di dekripsi kembali sehingga jalur komunikasi pada aplikasi chatting tersebut dapat melindungi kerahasiaan isi pesan tersebut. Pengguna kedua (penerima pesan) dapat langsung melihat isi pesan yang ada dengan jelas yang sudah melalui proses enkripsi dan dekripsi pada aplikasi chatting tersebut.

Dengan adanya aplikasi ini diharapkan suatu kerahasiaan informasi atau pesan penting tersebut dapat dilindungi oleh PT Printmate dan tidak dapat di curi dan di salah gunakan oleh pihak-pihak yang tidak bertanggung jawab.



Gambar 2. Ilustrasi Aplikasi *Chatting* dengan Algoritma RSA *Cipher*.

3.3. Rancangan Basis Data

Aplikasi *chatting* ini terdapat juga rancangan basis data yang dibuat untuk menyimpan data user dan juga pesan-pesan dalam kegiatan *chatting*. Berikut rancangan basis data yang terdapat dalam aplikasi ini yaitu:

a. Rancangan *Table Structure User*

Dalam *table structure user* ini terdapat beberapa *fields* dan jenisnya. Berikut Tabel 1. Rancangan *Table Structure User*.

Nama tabel : *tbl_user*
Primary_key : *Nick*

Tabel 1. Rancangan Table Structure User

No	Name	Type	Keterangan
1	Name	Varchar (50)	Nama lengkap pengguna
2	Email	Varchar (50)	Email pengguna
3	Password	Varchar (20)	Password pengguna untuk login
4	Nick (Primary)	Varchar (20)	Id pengguna untuk login
5	Status	Varchar (20)	Status pengguna online/ offline
6	Cdate	Datetime	Waktu pertama pengguna registrasi
7	Picture	Varchar (100)	Nama gambar foto profil
8	Public_key	Text	Kunci Publik RSA
9	Private_key	Text	Kunci Private RSA
10	N	Text	Nilai N

b. Rancangan *Table Structure Chatting*

Dalam *table structure chatting* ini terdapat beberapa *fields* dan jenisnya. Berikut Tabel 2. Rancangan *Table Structure Chatting*.

Nama tabel : *tbl_msg*
Primary_key : *Id*

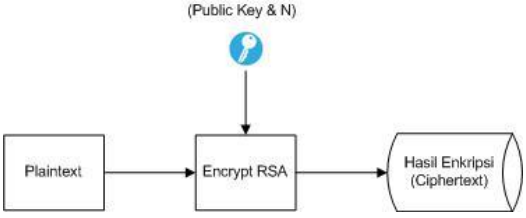
Tabel 2. Rancangan Table Structure Chatting

No	Name	Type	Keterangan
1	Id (Primary)	Int (11)	Keterangan nomor pesan
2	Dari	Varchar (20)	Nama user pengirim pesan
3	Ke	Varchar (20)	Nama user penerima pesan
4	Msg	Text	Isi pesan dalam (ciphertext)
5	Timestamp	Timestamp	Data waktu pesan pada web database
6	Status	Int (11)	Keterangan status pesan terkirim/tidak
7	Creation_date	Datetime	Data waktu pesan sesuai pada HP user

3.4. Proses *Chatting* Dengan Enkripsi Algoritma RSA *Cipher*

Enkripsi adalah proses mengubah isi pesan atau plaintext menjadi *ciphertext* berupa kode-kode teks yang sulit dimengerti. Dalam pembuatan aplikasi chatting ini terdapat proses enkripsi dengan menggunakan algoritma RSA Cipher. Berikut ini terdapat langkah-langkah proses enkripsi algoritma RSA cipher pada aplikasi chatting.

a. Pengirim pesan melakukan input pesan yang ingin dikirim kepada penerima.
b. Pada saat pengiriman pesan terjadi proses enkripsi dengan *Public Key* dan N (modulus).
c. Proses enkripsi menggunakan algoritma RSA cipher
d. Hasil dari enkripsi tersebut berupa ciphertext dan disimpan kedalam database.

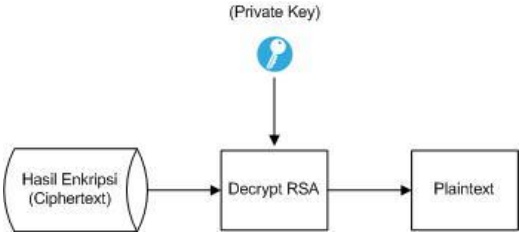


Gambar 3. Proses Enkripsi Algoritma RSA *Cipher*

3.5. Proses *Chatting* Dengan Dekripsi Algoritma RSA *Cipher*

Dekripsi adalah proses mengubah *cipherext* menjadi *plaintext* atau isi pesan. Dalam pembuatan aplikasi *chatting* ini terdapat juga proses Dekripsi dengan menggunakan algoritma RSA *Cipher*. Berikut ini terdapat langkah-langkah proses Dekripsi algoritma RSA *cipher* pada aplikasi *chatting*.

a. Saat penerima pesan dalam keadaan *online* pada aplikasi *chatting* maka pesan yang akan dikirim oleh pengirim akan dilakukan proses dekripsi menggunakan *Private Key*.
b. Proses Dekripsi menggunakan algoritma RSA *cipher*.
c. Hasil dekripsi tersebut berupa pesan.

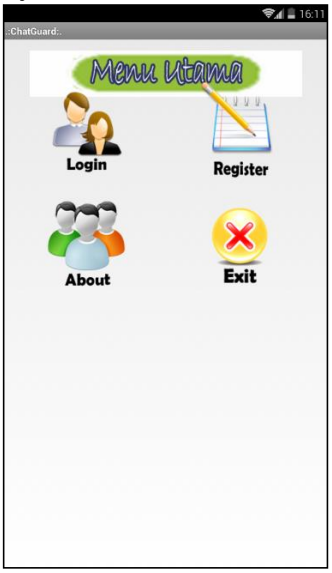


Gambar 4. Proses Dekripsi Algoritma RSA *Cipher*

4. HASIL DAN PEMBAHASAN

4.1 Tampilan Layar Menu Utama

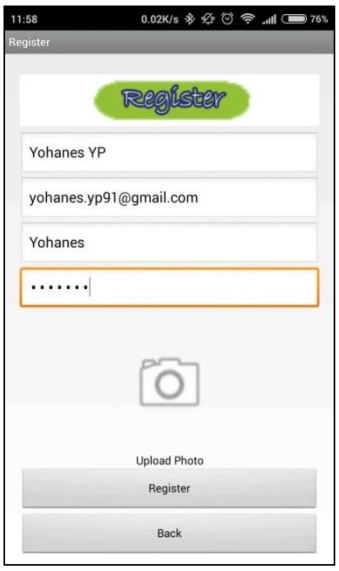
Pada tampilan layar menu utama ini *user* dapat memilih beberapa form diantaranya adalah *login*, Register, *About*, dan *Exit*. Berikut Gambar 5. Tampilan Layar Menu Utama.



Gambar 5. Tampilan Layar Menu Utama

4.2 Tampilan Layar Register

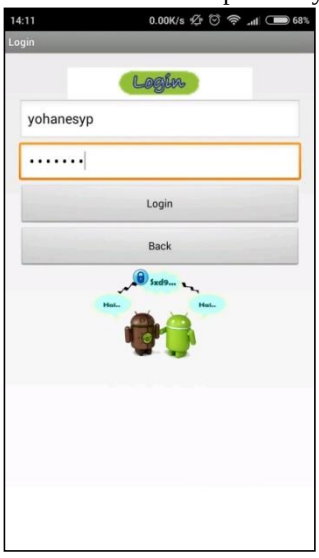
Pada tampilan layar Register *user* dapat mendaftarkan nama lengkap, *email*, *username*, dan *password* serta dapat menambahkan foto. Berikut Gambar 6. Tampilan Layar Register.



Gambar 6. Tampilan Layar Register

4.3 Tampilan Layar *Login*

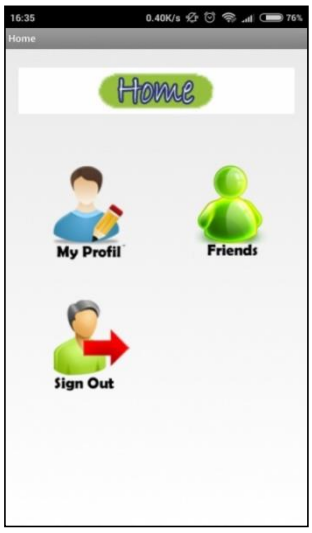
Pada tampilan layar login ini user harus memasukan data *username* dan *password* dengan benar sesuai yang sudah didaftarkan pada form register. Berikut Gambar 7. Tampilan Layar *Login*.



Gambar 7. Tampilan Layar *Login*

4.4 Tampilan Layar *Home*

Pada tampilan layar home ini *user* dapat memilih beberapa form diantaranya adalah *My* Profil, *Friends* dan *Sign Out*. Berikut Gambar 8. Tampilan Layar *Home*.



Gambar 8. Tampilan Layar *Home*

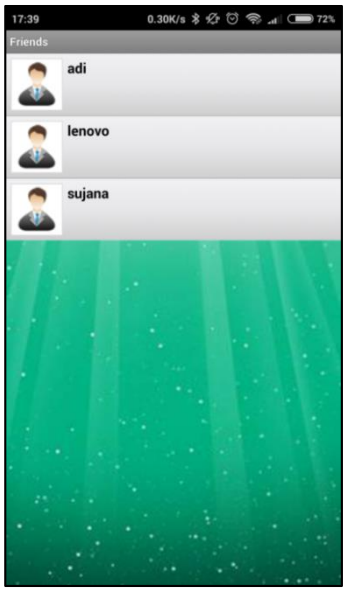
4.5 Tampilan Layar *My* Profil

Pada tampilan layar My Profil, *user* dapat melihat hasil data yang sudah berhasil Register dan juga bisa mengubah data user tersebut menjadi lebih *update* atau terbaru serta dapat melihat dan mengubah *public key*, *private key* dan n dengan *generate key* sebagai pengaman dalam aplikasi *chatting*. Berikut Gambar 9 Tampilan layar *My* Profil.

Gambar 9. Tampilan Layar *My* Profil

4.6 Tampilan Layar *Friends*

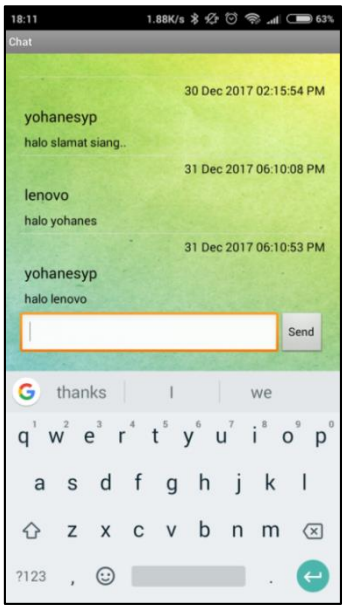
Pada tampilan layar *Friends*, *user* dapat langsung melihat *list friends* atau teman yang sudah terdaftar dalam aplikasi tersebut dan langsung dapat memilih nama teman untuk memulai *chatting*. Berikut Gambar 10 tampilan layar *Friends*.



Gambar 10. Tampilan Layar *Friends*

4.7 Tampilan Layar *Chatting*

Apabila *user* sudah memilih teman maka akan tampil dalam halaman *chatting* dan dapat langsung memulai *chatting*. Berikut Gambar 11 tampilan layar *chatting*.



Gambar 11. Tampilan Layar *Chatting*

4.8 Pengujian Program

Uji coba aplikasi berguna untuk mengetahui apakah program yang telah dibuat dapat berjalan secara maksimal atau bahkan terjadi kesalahan-kesalahan yang tidak diinginkan, maka dari itu program tersebut harus diuji dahulu mengenai kemampuannya agar dapat berjalan sesuai dengan yang diharapkan pada saat implementasi nantinya. Program ini dilakukan pengujian untuk mengetahui hasil pesan asli yang akan melalui *web database* sudah berjalan dengan algoritma RSA *Cipher* yaitu

untuk mengenkripsi isi pesan dari pesan asli atau *plaintext* menjadi pesan *ciphertext* supaya tidak dapat dimengerti oleh pihak-pihak yang tidak bertanggung jawab yang ingin mencuri isi pesan tersebut untuk kepentingan yang merugikan bagi perusahaan.

4.8.1 Proses Enkripsi

Poses enkripsi ini berjalan dengan menggunakan salah satu *Public Key* dan nilai N dari (*user* pengirim/penerima) untuk memasukan hasil enkripsi kedalam web database. Berikut contoh ujicoba proses enkripsi pesan dan hasil *screenshot* pada program android studio dan penjelasan proses enkripsi dengan keterangan sebagai berikut:

a. Ujicoba Pesan "Tugas Akhir"
   1) *Public key* : 167
   2) N (Modulus) : 3049905109
   3) *Plaintext* : Tugas Akhir
   4) *Ciphertext* : 2699776440,2140397471,1279058631,1496510919,1117110549,2232112163,2844259363,2216886920,175427009,2477898571,590993104
   5) *Encode Base64* : MjY5OTc3NjQ0MCwyMTQwMzk3NDcxLDEyNzkwNTg2MzEsMTQ5NjUxMDkxOSwxMTE3MTEwNTQ5LDIyMzIxMTIxNjMsMjg0NDI1OTM2MywyMjE2ODg2OTIwLDE3NTQyNzAwOSwyNDc3ODk4NTcxLDU5MDk5MzEwNA==

Gambar 12. Hasil *Screenshot* RSA *Encrypt* dengan pesan "Tugas Akhir"

b. Ujicoba Pesan "Universitas"
   a) A *Public key* : 167
   b) N (Modulus) : 3049905109
   c) *Plaintext* : Universitas
   d) *Ciphertext* : 1409668026,184265797,2477898571,1705448354,25147574,590993104,1117110549,2477898571,924410773,1496510919,1117110549
   e) *Encode Base64* : MTQwOTY2ODAyNiwxODQyNjU3OTcsMjQ3Nzg5ODU3MSwxNzA1NDQ4MzU0LDI1MTQ3NTc0LDU5MDk5MzEwNCwxMTE3MTEwNTQ5LDI0Nzc4OTg1NzEsOTI0NDEwNzczLDE0OTY1MTA5MTksMTExNzExMDU0OQ==

Gambar 13. Hasil *Screenshot* RSA *Encrypt* dengan pesan "Universitas"

4.8.2 Pengujian Proses Dekripsi

Poses dekripsi ini berjalan dengan menggunakan salah satu *Private Key* dari (*user* pengirim/penerima) untuk menampilkan isi pesan yang sudah melalui proses enkripsi kedalam kegiatan *chatting*, sehingga hanya dalam aplikasi ini saja yang dapat melihat pesan asli. Berikut contoh ujicoba proses dekripsi pesan dan hasil *screenshot* pada program android studio serta penjelasan proses dekripsi dengan keterangan sebagai berikut:

a. Ujicoba Pesan "Tugas Akhir"
   1) *Private key* : 786867391
   2) N (Modulus) : 2899859761
   3) *Ciphertext* : MjQzMDMxMTk0NSwxOTQ4NDgxNDE3LDE5Nzc1Njc2ODYsMTAxMjQ5NTk5MywxNDYzNzc1MjU1LDY3NjM2MTIzMiw4MzEyOTU1MjYsMjUzMDM3NDIxOSwyMjM0MDUwNDAsMjcyODE3Mjk3MiwyODM1OTUxNjY=
   4) *Decode Base64* : 2430311945,1948481417,1977567686,1012495993,1463775255,676361232,831295526,2530374219,223405040,2728172972,283595166
   5) *Plaintext* : Tugas Akhir

Gambar 14. Hasil *Screenshot* RSA *Decrypt* dengan pesan "Tugas Akhir"

b. Ujicoba Pesan "Universitas"
   1) *Private key* : 786867391
   2) N (Modulus) : 2899859761
   3) *Ciphertext* : NDA2MjM3MTU0LDI3MDYzMDEwNzgsMjcyODE3Mjk3MiwyMjYzMjk2NzQ2LDIwNzYyNDcyMTgsMjgzNTk1MTY2LDE0NjM3NzUyNTUsMjcyODE3Mjk3MiwyMDgzMzg2MjI5LDEwMTI0OTU5OTMsMTQ2Mzc3NTI1NQ==
   4) *Decode Base64* : 406237154,2706301078,2728172972,2263296746,2076247218,283595166,1463775255,2728172972,2083386229,1012495993,1463775255
   5) *Plaintext* : Universitas

Gambar 15. Hasil *Screenshot* RSA *Decrypt* dengan pesan "Universitas"

4.9 Evaluasi Sistem

Setelah adanya pengujian aplikasi maka dapat ditemukan beberapa kelebihan dan kekurangan pada aplikasi ini, diantaranya adalah:

a. Kelebihan Aplikasi

1) Aplikasi chatting ini menggunakan enkripsi algoritma RSA *Cipher* dimana keamanan dari algoritma ini sangat sulit dipecahkan.
2) Dengan demikian aplikasi chatting dengan algoritma RSA *Cipher* mampu menjaga kerahasian isi pesan bagi pengguna aplikasi ini.
3) Aplikasi ini menggunakan *web* database sebagai pertukaran data dengan mudah sehingga dapat diakses dimana saja tanpa menggunakan dan melalui komputer sebagai server.

b. Kekurangan Aplikasi

1) Aplikasi ini hanya dapat mengirim pesan dalam bentuk teks saja dan dalam jumlah yang terbatas.
2) Aplikasi ini masi kurang dalam fitur-fiturnya terutama belum tersedia untuk menggunakan foto profil.
3) Aplikasi ini sangat bergantung terhadap koneksi sinyal yang digunakan sebagai *wifi* dalam proses cepat atau lamanya pengiriman pesan.

5. KESIMPULAN

5.1 Kesimpulan

Berdasarkan evaluasi dari hasil uji coba yang telah dilakukan pada aplikasi yang dikembangkan, kesimpulan yang didapat adalah sebagai berikut :

a. Implementasi kriptografi dengan algoritma RSA cipher untuk pengamanan chatting telah berhasil dilakukan dan dapat diterapkan di PT Printmate.
b. Dengan menggunakan algoritma RSA Cipher pada aplikasi chatting ini dan data pesan tersimpan pada database sehingga dapat terjaga kerahasian pesan dari pihak yang tidak berwenang.

5.2 Saran

Adapun Saran untuk pengembangan lebih lanjut untuk sistem aplikasi ini agar berfungsi dengan lebih baik antara lain sebagai berikut :

c. Aplikasi *chatting* ini diharapkan dapat dikembangkan untuk pengiriman pesan suara, video maupun *image*.
d. Aplikasi *chatting* ini diharapkan dapat dikembangkan dengan fitur *notivication* atau pemberitahuan dalam chatting, pesan sudah diterima dan dibaca oleh pengguna atau belum.
e. Aplikasi *chatting* ini diharapkan dapat dikembangkan dalam proses pengiriman pesan yang lebih cepat dan tidak terpustus atau terganggu pada sinyal yang tidak bagus.

6. DAFTAR PUSTAKA

[1] Bagus, Anantavijaya, Giva, Andriana Mutiara. dan Isa, Puncuna, 2016, *Pembuatan Aplikasi Chat dengan Android Berbasis Protokol XMPP*. e-Proceeding of Applied Science : Vol.2, No.1 | Page 318

[2] Devha, Chandra Putra, 2013, *Pengamanan Pesan Rahasia Menggunakan Algoritma Kriptografi Rivest Shamir Adleman (RSA)*. Universitas Pendidikan Indonesia.

[3] Hersatoto, Listiyono, 2009, *Implementasi Algoritma Kunci Public Pada Algoritma RSA*. DINAMIKA INFORMATIKA – Vol I No 2.

[4] Kasih, Fitri, dan Yasin, S.M, 2016, *Perancangan Chatting Room Berbasis Network*. CESS (Journal Of Computer Engineering, System And Science) Vol 1, No2.

[5] Sasongko, Jati, 2005, *Pengamanan Data Informasi menggunakan Kriptografi Klasik*. Jurnal Teknologi Informasi DINAMIK Volume X, No.3, : 160-167.

[6] Yuhefizar, 2008, *10 Jam Menguasai Internet, Teknologi & Aplikasinya*. Jakarta: Elex Media Komputindo.