BAB VI

KESIMPULAN DAN SARAN

6.1 Kesimpulan

1. Dengan adanya aplikasi ini dapat meningkatkan keamanan pada aplikasi *instant messenger* khususnya pada proses pengamanan pesan.
2. Dengan adanya aplikasi ini dapat mengurangi tingkat penyadapan pesan (*eavesdroppingo*) karena aplikasi mengimplementasikan algoritma RSA.

6.2 Saran

Program *instant messenger* yang mengimplementasikan algoritma RSA dalam pengamanan pesan perlu dilakukan pengembangan-pengembangan ke arah yang lebih baik guna memenuhi kebutuhan privasi komunasi yang semakin bertambah. Adapun saran-saran terhadap pengembangan program *instant messenger* adalah sebagai berikut :

1. Kekuatan Algoritma RSA

   Kekuatan algoritma RSA diantaranya :

   1. Keamanan algoritma RSA terletak pada tingkat kesulitan dalam memfaktorkan bilangan bilangan non prima menjadi faktor primanya, yang dalam hal ini $r=p.q$

2. Penemu algoritma RSA menyarankan nilai *p* dan *q* panjangnya lebih dari 100 digit. Dengan demikian hasil kali *r=p.q* akan berukuran lebih dari 200 digit. Menurut Rivest dan kawan-kawan, usaha untuk mencari faktor bilangan 200 digit membutuhan waktu komputasi selama 4 milyar tahun.
3. Merupakan algoritma yang paling baik dalam hal memfaktorkan bilangan besar. Selama belum ditemukan algoritma yang mangkus untuk memfaktorkan bilangan bulat menjadi faktor primanya, maka algoritma RSA tetap direkomendasikan untuk menyandikan pesan.

2. Kelemahan Algoritma RSA

   Adapun kelemahan algoritma RSA yaitu proses pemfaktoran menjadi menjadi kunci algoritma RSA ini, tapi dapat berdampak pada turunnya performa komputer karena memori yang digunakan untuk memfaktorkan sangatlah besar dan harus terus dilakukan selama sistem berjalan.

3. Mendukung input berupa *audio*.

   Pengguna nantinya dapat saling mengirim file yang berformat *audio* seperti *.mp3, .mp4, .wav, .flv* dan *emoticon* yang mengeluarkan bunyi *audio* yang khas.

4. Mendukung fasilitas *add friend, delete friend* dan *block friend*.

   Disamping dapat mengirim pesan, pengguna dapat melakukan operasi *add friend* yaitu untuk menambah kontak teman, *delete friend* untuk

menghapus teman yang masuk dalam daftar teman dan *block friend* untuk memblok teman karena alasan-alasan tertentu misalnya masalah yang berkaitan dengan SARA yang menyinggung salah satu pengguna.

5. Mendukung operasi *transfer file*.

   Pengguna dapat saling mengirim file baik itu berupa dokumen atau berbentuk file yang sudah dikompres (.*zip* atau .*rar*).

6. Sinkronisasi dengan database

   Untuk pengembangann ke depan, aplikasi *instant messenger* ini sudah tersinkron (tersambung) dengan database sehingga data user dan data hasil percakapan dapat terlihat di dalam database.