IMPLEMENTASI ALGORITMA KEY DEPENDENT SECURE MESSENGER PADA INSTANT MESSAGING

TUGAS AKHIR

Oleh :

RIDUAN AHMAD
NIM. 11.111.1900

FITRA WIJAYA
NIM. 11.111.0904

PROGRAM STUDI TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER MIKROSKIL
MEDAN
2016

THE IMPLEMENTATION OF KEY DEPENDENT SECURE MESSENGER ALGORITHM ON INSTANT MESSAGING

FINAL RESEARCH

By :

RIDUAN AHMAD
ID. 11.111.1900

FITRA WIJAYA
ID. 11.111.0904

STUDY PROGRAM OF INFORMATICS ENGINEERING
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
MIKROSKIL
MEDAN
2016

LEMBARAN PENGESAHAN

IMPLEMENTASI ALGORITMA KEY DEPENDENT SECURE MESSENGER PADA INSTANT MESSAGING

TUGAS AKHIR

Diajukan untuk Melengkapi Persyaratan Guna
Mendapatkan Gelar Sarjana Strata Satu
Program Studi Teknik Informatika

Oleh:

RIDUAN AHMAD
NIM. 11.111.1900

FITRA WIJAYA
NIM. 11.111.0904

Disetujui Oleh:

Dosen Pembimbing I,	Dosen Pembimbing II,
Andri, S.Kom,.M.T.I.	Andrew Sagitta Jauhari S.Kom, M.T

Medan, 24 Februari 2016

Diketahui dan Disahkan oleh:

Ketua Program Studi
Teknik Informatika,

Hardy, S.Kom, M.Sc.

ABSTRAK

Instant messaging adalah salah satu jenis layanan komunikasi yang memungkinkan seseorang untuk melakukan percakapan dengan orang lain secara *real time*. Dalam pengiriman pesan, keamanan tentunya menjadi salah satu aspek penting untuk menghindari terjadinya penyadapan oleh pihak ketiga. Untuk melindungi kerahasiaan pesan yang dikirim, maka dilakukan enkripsi untuk menjaga keamanan informasi tersebut.

Key Dependent Secure Messenger merupakan algoritma simetris yang digunakan untuk melakukan enkripsi dan dekripsi dalam kriptografi, yaitu kunci yang digunakan untuk enkripsi sama dengan kunci yang digunakan untuk dekripsi. Dengan demikian, proses enkripsi dan dekripsi akan lebih cepat tanpa perlu pertukaran kunci setiap saat. Kunci yang acak dan memiliki panjang 128 bit dapat menghasilkan pesan yang benar-benar acak sehingga penyadap tidak mudah untuk mengetahui pesan yang sebenarnya.

Pada hasil penelitian yang dilakukan, aplikasi yang dihasilkan sudah memenuhi persyaratan algoritma kriptografi yang baik. Hal ini dapat dilihat dari *avalanche effect* yang didapatkan berada di antara 40 % sampai 60 %. Dimana *avalanche effect* untuk perubahan 1 bit pada *plaintext* dengan kunci yang sama dan perubahan 1 bit pada *key* dengan *plaintext* yang sama. Berdasarkan pengujian menggunakan aplikasi *wireshark*, bahwa pesan yang dikirimkan berhasil terenkripsi dalam bentuk *chipertext* sehingga penyadapan tidak mudah untuk mengetahui isi pesan sebenarnya.

Kata kunci : *Instant messaging, Block cipher,* Kriptografi, *Avalache effect, Key Dependent Secure Messenger.*

KATA PENGANTAR

Ucapan syukur kepada Tuhan Yang Maha Esa karena berkat rahmatnya penulis bisa menyelesaikan Tugas Akhir yang berjudul, "**Implementasi Algoritma Key Dependent Secure Messanger Pada Instant Messenger**", sesuai dengan yang direncanakan. Untuk itu puji syukur penulis panjatkan kepada-Nya. Selanjutnya menyampaikan ucapan terima kasih kepada:

1. Bapak Andri S.Kom, M.T.I, selaku pembimbing I yang telah membimbing penulis selama mengerjakan Tugas Akhir ini.
2. Bapak Andrew Sagitta Jauhari, S.Kom, M.T., selaku pembimbing II yang telah membimbing penulis selama mengerjakan Tugas Akhir ini.
3. Ibu Florida N.S. Damanik, S.T., M.M., selaku penguji I.
4. Bapak Wenripin Chandra, S.Kom., M.TI., selaku penguji II.
5. Bapak Hardy, S.Kom., M.Sc., selaku Ketua Program Studi Teknik Informatika.
6. Bapak Dr. Mimpin Ginting, M.S., selaku Ketua STMIK Mikroskil Medan.
7. Bapak Djoni, S.Kom., M.T.I., selaku Wakil Ketua I STMIK Mikroskil Medan.
8. Bapak/Ibu Dosen yang telah memberikan bimbingan kepada penulis selama mengerjakan tugas akhir ini.
9. Orang tua penulis dan teman – teman yang telah memberikan dukungan kepada penulis selama pengerjaan tugas akhir ini.

Tugas Akhir ini dibuat untuk melengkapi persyaratan guna memperoleh gelar Sarjana Strata Satu pada Program Studi Teknik Informatika, STMIK Mikroskil Medan. Semoga hasil dari Tugas Akhir ini ada manfaatnya bagi pihak yang berkepentingan.

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL