

**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

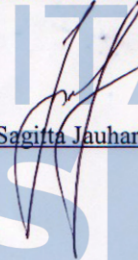
Disetujui Oleh:

Dosen Pembimbing I,



Andri, S.Kom., M.T.I.

Dosen Pembimbing II,



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 *chiphertext* sehingga penyadapan tidak mudah untuk mengetahui isi pesan sebenarnya.

Kata kunci : *Instant messaging, Block cipher, Kriptografi, Avalanche 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

ABSTRAK	i
KATA PENGANTAR	ii
DAFTAR ISI	iii
DAFTAR GAMBAR	v
DAFTAR TABEL	viii
DAFTAR LAMPIRAN	ix
BAB I PENDAHULUAN	1
1.1. Latar Belakang	1
1.2. Rumusan Masalah	2
1.3. Tujuan dan Manfaat	2
1.4. Batasan Masalah	3
1.5. Metodologi Penelitian	3
BAB II TINJAUAN PUSTAKA	6
2.1. Kriptografi	6
2.2. Block Cipher	9
2.3. Key Dependent Secure Messenger	10
2.3.1. Tahap Enkripsi	10
2.3.2. Tahap Dekripsi	12
2.4. Instant Messaging	13
2.6. Avalanche Effect	15
BAB III ANALISIS DAN PERANCANGAN	16
3.1. Analisis	16
3.1.1. Analisis Masalah	16
3.1.1.1. Proses Arsitektur Client – Server	16
3.1.2 Analisis Proses	17
3.1.2.1. Proses Pembentukan Nilai Kunci	17

3.1.2.2. Proses Enkripsi Pesan	18
3.1.2.3. Proses Dekripsi Pesan	26
3.1.2.4. Proses Avalanche Effect	35
3.1.3. Analisis Kebutuhan	37
3.1.3.1. Kebutuhan Fungsional	37
3.2. Perancangan	45
3.2.1. Perancangan Proses	45
3.2.2. Rancangan Basis Data	52
3.2.3. Perancangan Menu	55
BAB IV HASIL DAN PENGUJIAN	73
4.1. Hasil	73
4.2. Pengujian	82
4.2.1. Pengujian menggunakan Avalanche Effect	82
4.2.2. Pengujian Integritas Enkripsi Paket Data	99
4.2.3. Percobaan Kebenaran Hasil Enkripsi	109
BAB V KESIMPULAN DAN SARAN	110
5.1. Kesimpulan	110
5.2. Saran	110
DAFTAR PUSTAKA	111

DAFTAR GAMBAR

Gambar 2. 1. Proses enkripsi dan dekripsi. Sumber : (Ariyus, D., 2008).....	6
Gambar 2. 2. Gambar Enkripsi dan dekripsi Algoritma Simetris	8
Gambar 2. 3. Enkripsi dan dekripsi algoritma Asimetris	8
Gambar 2. 4. Instant Messaging dengan Arsitektur Client – Server (Arie Karhendana, 2006)	14
Gambar 3. 1 Proses Arsitektur client – server	16
Gambar 3. 2 Proses Pembentukan Nilai Kunci	17
Gambar 3. 3 Flowchart Proses Enkripsi Tahap I	18
Gambar 3. 4. Flowchart Proses Enkripsi Tahap II	21
Gambar 3. 5. Flowchart Proses Dekripsi Tahap I	26
Gambar 3. 6. Flowchart Proses Dekripsi Tahap II	32
Gambar 3. 7. Use Case Diagram Instan Messaging	38
Gambar 3. 8 Activity Diagram Register	45
Gambar 3. 9. Activity Diagram Login	46
Gambar 3. 10. Activity Diagram Search Friend	47
Gambar 3. 11. Activity Diagram Chat	48
Gambar 3. 12. Activity Diagram Edit Profile	49
Gambar 3. 13. Activity Diagram Manage User	50
Gambar 3. 14. Activity Diagram Avalanche Effect	51
Gambar 3. 15 Halaman Utama	55
Gambar 3. 16. Perancangan Halaman Login	56
Gambar 3. 17. Perancangan Halaman Register	57
Gambar 3. 18. Perancangan Halaman Chats	58
Gambar 3. 19. Perancangan Halaman Chatting	59
Gambar 3. 20. Perancangan Halaman Updates	60
Gambar 3. 21. Perancangan Halaman Contacts	61
Gambar 3. 22. Perancangan Halaman Add Friends	62
Gambar 3. 23. Perancangan Halaman Settings	64

Gambar 3. 24 Perancangan Halaman Admin	65
Gambar 3. 25. Perancangan Halaman Dashboard	66
Gambar 3. 26. Perancangan Halaman Avalanche Effect Test	67
Gambar 3. 27 Perancangan Halaman Encrypt Test	68
Gambar 3. 28. Perancangan Halaman Manage Users	70
Gambar 3. 29. Perancangan Halaman Edit Profile Admin	71
Gambar 3. 30. Perancangan Halaman Edit Password Admin	72
Gambar 4. 1 Perancangan Halaman Edit Profile Admin	73
Gambar 4. 2. Tampilan Login	73
Gambar 4. 3. Tampilan Halaman Register	74
Gambar 4. 4. Tampilan Halaman Chats	75
Gambar 4. 5. Tampilan Halaman Chatting	75
Gambar 4. 6. Tampilan Halaman Updates	76
Gambar 4. 7. Tampilan Halaman Contacts	76
Gambar 4. 8. Tampilan Halaman Add Friend	77
Gambar 4. 9. Tampilan Settings	78
Gambar 4. 10. Tampilan Dashboard	78
Gambar 4. 11. Tampilan Avalanche Effect Test	79
Gambar 4. 12. Tampilan Avalanche Effect Test	79
Gambar 4. 13. Tampilan Manage Users	80
Gambar 4. 14. Tampilan halaman Edit Profile	81
Gambar 4. 15. Tampilan halaman Edit Password	81
Gambar 4. 16 IP Address client 2	100
Gambar 4. 17 IP Address Client 1	100
Gambar 4. 18 IP Address server	100
Gambar 4. 19 Mengirimkan Pesan dari client 1 ke client 2	101
Gambar 4. 20 Pengiriman pesan sebelum proses enkripsi dari client 1 ke server	102
Gambar 4. 21 Pengiriman pesan sebelum proses enkripsi dari server ke client 2	103
Gambar 4. 22 Pengiriman pesan sebelum proses enkripsi dari server ke client1	103

Gambar 4. 23 Penangkapan data dari client 2 ke server	104
Gambar 4. 24 Mengirimkan Pesan dari client 1 ke client 2	105
Gambar 4. 25 Pengiriman pesan yang terenkripsi dari client 1 ke server	105
Gambar 4. 26 Pengiriman pesan sesudah proses enkripsi dari server ke client2	106
Gambar 4. 27 Pengiriman pesan sesudah proses enkripsi dari server ke client1	107
Gambar 4. 28 Penangkapan data dari client 2 ke server	108
Gambar 4. 29 Encrypt Test	115



DAFTAR TABEL

Tabel 3. 1. Deskripsi Use Case Sign Up	38
Tabel 3. 2. Deskripsi Use Case Find Friend	39
Tabel 3. 3. Deskripsi Use auto Confirm	40
Tabel 3. 4. Deskripsi Use Case Login.....	40
Tabel 3. 5. Deskripsi Use Case Edit Profile	41
Tabel 3. 6. Deskripsi Use Case Chat	41
Tabel 3. 7. Deskripsi Use Case Manage User	43
Tabel 3. 8. Deskripsi Use Case Avalanche Effect Test	43
Tabel 3. 9. Struktur users	52
Tabel 3. 10. Struktur friends	53
Tabel 3. 11. Struktur chats	53
Tabel 3. 12. Struktur userinformations	54
Tabel 3. 13. Struktur userstatus	54
Tabel 4. 1 Pengujian perubahan 1 bit pada kunci dengan plaintext yang sama ...	82
Tabel 4. 2 Pengujian perubahan 1 bit pada kunci dengan plaintext yang sama ...	91

UNIVERSITAS
MIKROSKIL