PENERAPAN ALGORITMA KRIPTOGRAFI WAKE
PADA APLIKASI CHATTING & INTERNET MONITOR BERBASIS LAN

SKRIPSI

disusun oleh :

Ryan Maulana A

07.12.2377

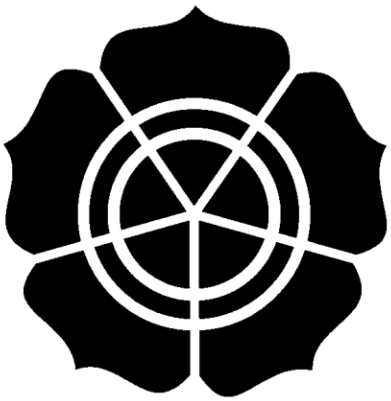
JURUSAN SISTEM INFORMASI
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM
YOGYAKARTA

2012

PENERAPAN ALGORITMA KRIPTOGRAFI WAKE
PADA APLIKASI CHATTING & INTERNET MONITOR BERBASIS LAN

Skripsi

untuk memenuhi sebagian persyaratan
mencapai derajat Sarjana S1
pada jurusan Sistem Informasi



disusun oleh

Ryan Maulana A

07.12.2377

JURUSAN SISTEM INFORMASI
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM
YOGYAKARTA
2012

PERSETUJUAN

SKRIPSI

PENERAPAN ALGORITMA KRIPTOGRAFI WAKE PADA APLIKASI CHATTING & INTERNET MONITOR BERBASIS LAN

yang dipersiapkan dan disusun oleh

Ryan Maulana A
07.12.2377

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 9 Februari 2012

Dosen Pembimbing,

Sudarmawan, M.T.
NIK. 190302035

PENGESAHAN

SKRIPSI

Penerapan Algoritma Kriptografi WAKE

Pada Aplikasi Chatting & Iinternet Monitor Berbasis LAN

yang dipersiapkan dan disusun oleh

Ryan Maulana A

07.12.2377

telah dipertahankan di depan Dewan Penguji
pada tanggal 1 Maret 2012

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Sudarmawan, S.T., M.T. **NIK. 190302035**	
Amir Fatah Sofyan, S.T., M.Kom. **NIK. 190302047**	
Tonny Hidayat, M.Kom. **NIK. 190302128**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 1 Maret 2012

KETUA STMIK AMIKOM YOGYAKARTA

Prof. Dr. M. Suyanto, M.M.
NIK. 190302001

PERNYATAAN

Saya yang bertanda tangan dibawah ini menyatakan bahwa, skripsi ini merupakan hasil karya saya sendiri (ASLI), dan isi dalam skripsi ini tidak terdapat karya yang pernah diajukan oleh orang lain untuk memperoleh gelar akademis di suatu Institusi Pendidikan, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis dan/atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Demikian surat pernyataan ini saya buat, apabila di kemudian hari ternyata saya terbukti melakukan pelanggaran akademik tersebut di atas, maka saya bersedia menerima sanksi dicabut ijazah serta gelar yang telah diberikan kepada saya.

Yogyakarta, 29 Februari 2012

Ryan Maulana A
07.12.2377

PERSEMBAHAN

Terucap syukur Alhamdulillah kepada Allah SWT dan do'a yang tak hentinya kupanjatkan padaMu. Saya persembahkan skripsi ini teruntuk :

- Kedua orang tua Bapak Agussalim dan Ibu Nining Sukartiningsih. Atas kasih sayang, dukungan do'a, materi dan moril hingga skripsi ini bisa terselesaikan. Jika bukan karena do'a dan dukungan dari kalian maka tidak mungkin skripsi ini selesai tepat pada waktunya.
- Untuk keluarga besarku terima kasih atas semua support yang telah diberikan terlebih untuk tante fifi, mama tua, om leo.
- Bapak Sudarmawan M.T yang selalu sabar dan membimbing saya untuk menyelesaikan skripsi ini.
- IBM (Agung, Eko, Hanung, Ijun, Joko, Radit, Ryan Fahmi, Bangkit) yang telah memberikan kenangan manis dalam hidup ini, terima kasih untuk persahabatan yang tidak akan terlupakan sampai kapan pun, kalian adalah sahabat dan keluarga paling dekat bagiku.
- Teman-teman S1-SI 2007 Kelas E terima kasih atas kebersamaan selama kita kuliah, semoga pertemanan ini dapat terjalin selamanya.
- bangkit, Ijun, dan Fahmi terima kasih atas semua dukungan yang sangat banyak dari kalian semangat, materi, pengalaman berharga di saat keadaan susah maupun senang terhormat punya sahabat seperti kalian.
- Sepupu – sepupu yang selalu bisa memberi tambahan semangat saat sedang berkumpul.
- Teman dan kawan yang tak bisa disebutkan semua, makasih dan salam hangat dariku.

KATA PENGANTAR

Alhamdulillah, puji syukur penulis panjatkan kehadirat Allah SWT atas limpahan rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan penyusunan skripsi ini. Shalawat serta salam semoga tercurahkan kepada junjungan kita Nabi Muhammad SAW yang telah melimpahkan segala kebaikan kepada umatnya.

Penyusunan skripsi ini tidaklah lepas dari berbagai macam hambatan dan kesulitan baik dari segi materi maupun moral dan spiritual. Namun, atas petunjuk-Nya melalui berbagai macam cara serta media, penulis akhirnya dapat menyelesaikan skripsi ini. Oleh karena itu, penulis mengucapkan rasa terima kasih yang dalam kepada :

1. Bapak M. Suyanto, Prof. Dr, M.M. selaku Ketua STMIK Amikom Yogyakarta.
2. Bapak Bambang Sudaryatno, Drs. MM selaku Ketua Jurusan Sistem Informasi Reguler STMIK Amikom Yogyakarta
3. Bapak Sudarmawan, MT selaku Pembimbing yang telah memberikan bimbingan dan pengarahan dengan penuh kesabaran serta motivasi dari awal hingga terselesaikannya penulisan skripsi ini..
4. Segenap dosen Jurusan Sistem Informasi beserta segenap staf pendukungnya atas bekal ilmu dan pengetahuan materi selama penulis menempuh studi.

Penulis menyadari dalam penulisan skripsi ini masih banyak kekurangannya baik dari segi materi maupun penyajian tulisan. Oleh karena itu

penulis sangat mengharapkan kritik dan saran guna menyempurnakan penulisan ini. Dan semoga tulisan ini dapat bermanfaat bagi peningkatan perkembangan ilmu pengetahuan terutama dibidang Sistem Informasi.

Yogyakarta, 1 Maret 2012

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

INTISARI

Demi Meningkatkan kemanan informasi yg terjadi di saat user sedang melakukan chating maka diperlukannya suatu metode pengamanan yaitu dengan menggunakan salah satu metode algoritma kriptografi yaitu WAKE (Word Auto Encryption),Algoritma ini sendiri menggunakan kunci 128 bit, dan sebuah tabel 256 x 32 bit. Dalam algoritmanya, algoritma ini menggunakan operasi XOR, AND, OR dan *Shift Right,* Sebelum data dikirim atau ditransmisikan, data terlebih dahulu disandikan dengan proses enkripsi. Dengan demikian, data ditransmisikan dalam bentuk teks tersandi dan tak terbaca. Pada keadaan ini, walaupun *hacker* dapat menyadap komunikasi, tetapi *hacker* tidak dapat mengetahui komunikasi yang terjadi, karena data yang berhasil disadap *hacker* adalah data dalam bentuk tersandi (terenkripsi) sehingga tidak dapat dibaca. Di tempat penerima, teks tersandi dikembalikan lagi menjadi teks semula dengan proses dekripsi.

Tujuan penelitian adalah cara/langkah bagaimana menerapkan metode *WAKE* (Word Auto Key Encryption) pada aplikasi chatting, mempelajari pemakaian konektifitas yang diberikan oleh winsock pada Visual Basic sehingga dapat mengimplementasikannya dengan membuat aplikasi chatting.

Dari hasil pembahasan mengenai penerapan kriptografi WAKE pada aplikasi *Chatting* dan setelah menyelesaikan beberapa tahap yaitu pengumpulan data, mengidentifikasi masalah, membuat solusi untuk memecahkan masalah yaitu dengan menambahkan fasilitas kriptografi, membuat rancangan, implementasi sistem aplikasi chatting yang menggunakan sistem kriptografi wake sebagai *tool* pengaman pesan yang saling di pertukarkan, yang bertujuan untuk mengurangi resiko adanya pihak yang tak bertanggung jawab yang bertujuan merusak, merubah, mengetahui isi pesan dari para *user* demi memuaskan *user* yang menuntut *privacy* mereka tetap terjaga.

Kata Kunci : ***Word Auto Key Encryption(WAKE)***

ABSTRACT

In order to Improving security that occurred when the user is doing chating in, then the need for a security method is by using one of the cryptographic algorithm that is WAKE (Word Auto Encryption), this algorithm itself uses 128-bit key, and a table 256 x 32 bits. In the algorithm, this algorithm uses XOR, AND, OR and Shift Right, before data is sent or transmitted, data is first encrypted with the encryption process. Thus, data is transmitted in the form of encrypted and unreadable text. In this situation, even though hackers can tap communication, but hackers can not know the communication that occurs, because the data is successfully intercepted a hacker is data in the form of encoded (encrypted) so it can not be read. At the receiver, encrypted text returned to the original text with the decryption process

Purpose the research is the way / step how to implement the method WAKE (Word Auto Key Encryption) on the application chatting, studying the discharging 'connectivity is given by winsock on Visual Basic so that can implements it with create chatting applications.

From the results of the discussion concerning the application of cryptography WAKE Chatting on the application and after completing several stages of data collection, identify problems, create solutions to solve the problem by adding a cryptographic facility, making the design, implementation of the chat application that uses cryptographic system WAKE as a safety tool messages at each interchange, which aims to reduce the risk of irresponsible parties aimed at the destruction, change, knowing the contents of the message from the user in order to satisfy users who demand their privacy is maintained.

Keyword: Word Auto Key Encryption (WAKE)