APLIKASI PENGAMANAN DATA MENGGUNAKAN METODE GOVERNMENT STANDARD (GOST)

SKRIPSI

disusun oleh

Andrian Sah

09.11.2728

JURUSAN TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM
YOGYAKARTA
2012

APLIKASI PENGAMANAN DATA MENGGUNAKAN METODE GOVERNMENT STANDARD (GOST)

SKRIPSI

untuk memenuhi sebagian persyaratan
mencapai derajat Sarjana S1
pada jurusan Teknik Informatika

disusun oleh

Andrian Sah

09.11.2728

JURUSAN TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM
YOGYAKARTA
2012

PERSETUJUAN

SKRIPSI

APLIKASI PENGAMANAN DATA MENGGUNAKAN METODE GOVERNMENT STANDARD (GOST)

yang dipersiapkan dan disusun oleh

Andrian Sah

09.11.2728

Telah disetujui oleh Dosen Pembimbing Skripsi
Pada tanggal 5 November 2012

Dosen Pembimbing,

Dr. Ema Utami, S.Si, M.Kom
NIK. 190302037

PENGESAHAN

SKRIPSI

APLIKASI PENGAMANAN DATA MENGGUNAKAN METODE GOVERNMENT STANDARD (GOST)

yang dipersiapkan dan disusun oleh

Andrian Sah

09.11.2728

Telah dipertahankan di depan Dewan Penguji
Pada tanggal 16 November 2012

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Dr. Ema Utami, S.Si, M.Kom **NIK. 190302037**	
Anggit Dwi Hartanto, M.Kom **NIK. 190000002**	
Joko Dwi Santoso, M.Kom **NIK. 190302181**	

Skripsi ini telah diterima sebagai salah satu persyaratan
Untuk memperoleh gelar Sarjana Komputer
Tanggal 27 November 2012

KETUA STMIK AMIKOM YOGYAKARTA

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

PERNYATAAN

Saya yang bertandatangan dibawah ini menyatakan bahwa, skripsi ini merupakan 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.

Yogyakarta, 27 November 2012

Andrian Sah

09.11.2728

MOTTO

“Berbicara demi suatu perubahaan.”

“Jenius adalah 1 % inspirasi dan 99 % kerja keras.”

“Saya datang, saya bimbingan, saya ujian, saya revisi dan saya menang!”

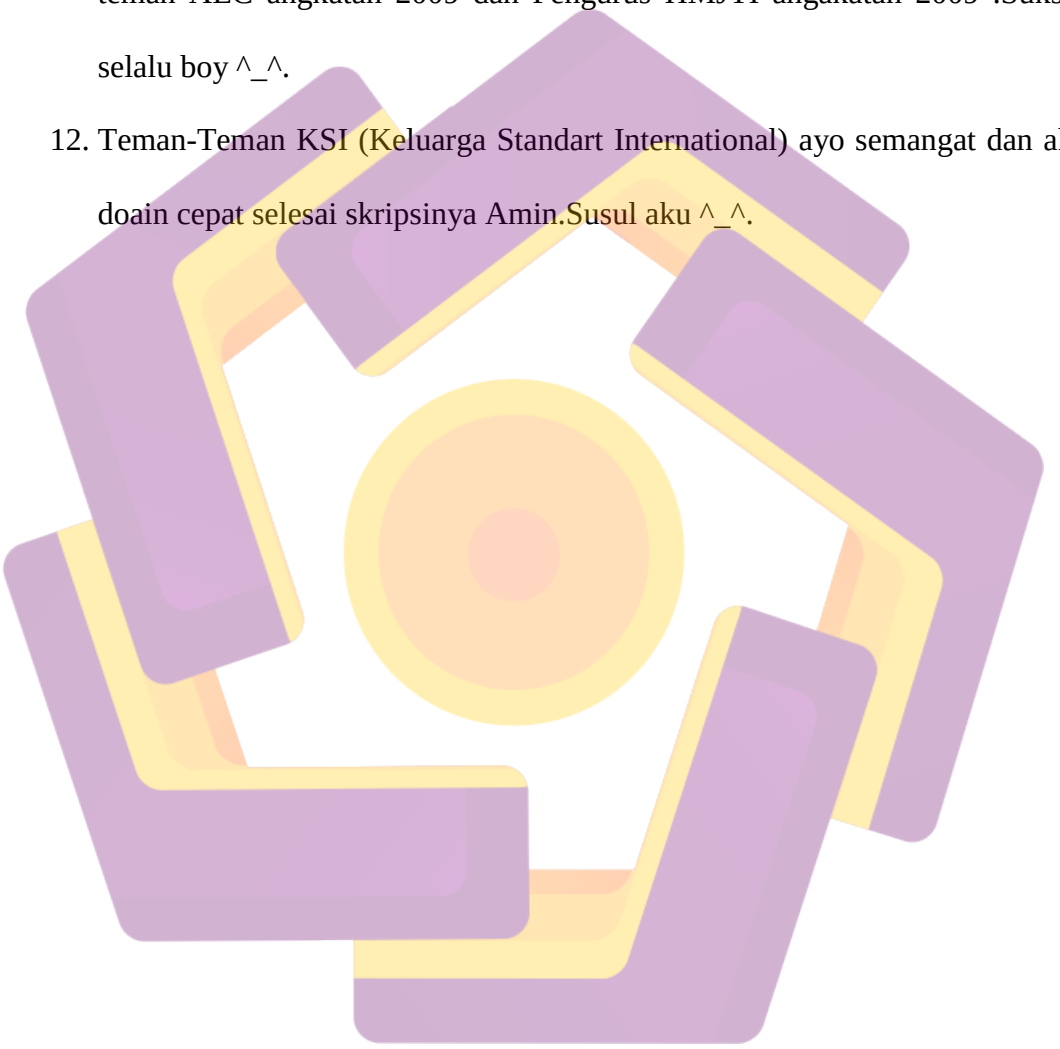
"Tidak ada masalah yang tidak bisa diselesaikan selama ada komitmen bersama untuk menyelesaikannya."

PERSEMBAHAN

Alhamdulillah akhirnya laporan skripsi ini selesai. Dengan selesainya skripsi ini penyusun mempersemahkan ucapan terima kasih kepada :

1. Allah SWT, Berkat kuasa-Nya dan semua kehendak-Nya semua bisa terjadi seperti ini. Thankz God.
2. Nabi Muhammad SAW. Engkaulah yang membimbing kami dijalan yang benar.
3. Ayah dan Ibu yang selalu membimbingku serta doa yang menyertaiku akhirnya saya telah selesaikan kuliahku.
4. Om Boni , mama Heri dan keluarga besar Taniasik di Toraja terima kasih doa serta dukungannya.God Bless You .
5. Ade ku Nurul Shalin dan Iyem Syahira terima kasih doanya jangan kalah dengan kakak mu ini yang udah wisuda. good luck.
6. Gina Anggita Putri Kinasih dan keluarga terima kasih doanya. Neko-neko polo-polo semngat nyo ^o^.
7. Teman-teman seperjuangan Maulana Akbar, Tri Wahyu Pamungkas, Bayu Aswin Nur Indra, Arif Dwi Sutanto dan Fajrul Falach aku wisuda teman-taman.aku menyusulmu Faqih.
8. Si boy Muhammad Adi Sulistyo, Denny Natanael, Indra Ramadhani dan Lukman terima kasih bantuannya.Tetap semangat, boy susul aku wisuda.
9. Teman dari Jayapura dan Papua yang kuliah di jogja Irvan Umbora, Bertha Tabuni, Josua Mandosir, Risal, Eva, Teo, Farul dan ari . Teman-teman aku wisuda duluan. Tetap semangat sampai ketemu lagi di papua ^_^.

10. Teman-teman S1 TI 03 angkatan 2009 .Senang telah ketemu kalian dan terima kasih udah banyak membantu serta maaf jika aku ada salah.Good Luck ^_^.
11. Teman-teman Seperjuang pengurus Taekwondo angkatan 2009, Teman-teman AEC angkatan 2009 dan Pengurus HMJTI angakatan 2009 .Sukses selalu boy ^_^.
12. Teman-Teman KSI (Keluarga Standart International) ayo semangat dan aku doain cepat selesai skripsinya Amin.Susul aku ^_^.



KATA PENGANTAR

Alhamdulillah puji syukur penulis panjatkan kehadirat Allah SWT yang senantiasa melimpahkan rahmat dan anugerah kepada setiap hamba-hambanya yang beriman dan berikhtiar. Shalawat serta salam juga tidak lupa penulis kirimkan kepada junjungan kita Nabi Besar Muhammad SAW yang telah memberikan teladan mulia dalam menuntun ummatnya.

Skripsi ini disusun sebagai salah satu syarat kelulusan bagi setiap mahasiswa STMIK "AMIKOM". Selain itu juga merupakan suatu bukti bahwa mahasiswa telah menyelesaikan kuliah jenjang program Strata-1 dan untuk memperoleh gelar Sarjana Komputer.

Dengan selesainya skripsi ini, maka penulis tidak lupa mengucapkan terima kasih kepada :

1. Bapak Prof. Dr. M. Suyanto, M.M selaku Ketua STMIK "AMIKOM" Yogyakarta.
2. Bapak Sudarmawan, M.T dan Hanif Al Fatta, M.Kom selaku Ketua Jurusan Teknik Informatika STMIK "AMIKOM" Yogyakarta.
3. Ibu Dr. Ema Utami, S.Si., M.Kom selaku dosen pembimbing yang telah banyak memberikan pengarahan bagi penulis dalam pembuatan skripsi.
4. Bapak dan Ibu dosen STMIK "AMIKOM" Yogyakarta yang telah banyak memerikan ilmunya selama penulis kuliah.
5. Semua pihak yang telah memantu baik dukungan moril maupun materiil, pikiran, dan tenaga dalam penyelesaian skripsi ini.

Penulis tentunya menyadari ahwa pemuatan skripsi ini masih banyak sekali kekurangan-kekurangan dan kelemahan-kelemahannya. Oleh karena itu penulis berharap kepada semua pihak agar dapat menyampaikan kritik dan saran yang membangun untuk menambah kesempurnaan skripsi ini. Namun penulis tetap berharap skripsi ini akan bermanfaat bagi semua pihak yang membacanya.

Yogyakarta, 16 November 2012

Penulis

Andrian Sah

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

INTISARI

Keamanan menjadi isu yang paling penting di era informasi. Untuk menjamin keamanan komunikasi, metode kriptografi dapat digunakan untuk mengenkripsi pesan sebelum mengirim dan mendekripsi untuk semua pesan yang diterima. Salah satu metode kriptografi yang dapat digunakan adalah metode GOST (Government Standard). Proses utama adalah pembentukan S-Box meja, pembentukan kunci, enkripsi dan dekripsi proses. Kompleksitas metode ini adalah dalam proses pembentukan S-Box tabel dan pembentukan kunci. Proses enkripsi dan dekripsi pada metode GOST hanya operasi XOR antara plaintext dan bit kunci untuk menghasilkan operasi ciphertext atau XOR antara kunci untuk menghasilkan ciphertext dan plaintext.

Algoritma Gost merupakan blok cipher 64 bit dengan panjang kunci 256 bit. Algoritma adalah algoritma enkripsi sederhana iterates total 32 putaran (putaran). Untuk mengenkripsi plaintext pertama kali dipecah menjadi 64 bit 32 bit ke L, kiri dan 32 bit ke kanan, R. Subkunci (subkey) untuk putaran i adalah Ki. Pada putaran ke-i operasi adalah sebagai berikut:

$$Li=Ri-1$$

$$Ri = Li-1 \oplus f\,(Ri-1, Ki)$$

Secara struktural, Gost algoritma mirip dengan DES (Data Encryption Standard).

Setelah sepenuhnya dikembangkan Hasil dari tesis analisis, penulis menarik kesimpulansebagaiberikut:

1. Membuat modul metode kriptografi belajar GOST membutuhkan dua komponen penting, yaitu MSFlexGrid (Microsoft FlexGrid) digunakan sebagai meja dan Pengendalian Dialog umum digunakan untuk membuka Open atau Save kotak dialog.
2. Perangkat lunak ini dapat membantu memahami bagaimana khususnya metode atau algoritmaGOST.
3. Proses pembentukan kunci untuk metode ini sangat sederhana sedangkan enkripsi GOST dan proses dekripsi panjang dan rumit.

Kata Kunci: Kriptografi, metode GOST, Enkripsi Teks, Teks Dekripsi

ABSTRACT

Security being the most important issue in the information age. When the communication channels are used less secure, then hackers will easily break the existing channel and tap all communication happens. To ensure the security of communications, cryptographic methods can be used to encrypt the message before sending and decrypt to all messages received. One of cryptographic methods that could be used is the method of GOST (Government Standard). The main process is the formation of S-Box table, the formation of the key, the encryption and decryption process. The complexity of this method are in the process of formation of S-Box tables and key establishment. The process of encryption and decryption on the method of GOST just a XOR operation between the plaintext and key bits to produce ciphertext or XOR operation between keys to produce the ciphertext and the plaintext.

GOST is an acronym for "Gosudarstvennyi Standard" or "Government Standard". GOST method is a block cipher algorithm developed by a national of the Soviet Union. This method was developed by the Soviet Union during the cold war to hide data or confidential information during communication. Algorithm Gost is a 64 bit block cipher with a key length of 256 bits. The algorithm is simple encryption algorithm iterates a total of 32 rounds (round). To encrypt the plaintext is first broken down into 64 bit 32 bit to the left, L and 32 bits to the right, R. Subkeys (subkey) for round i is Ki. At the i-th round of operations is as follows:

$$Li = Ri\text{-}1$$
$$Ri = Li\text{-}1 \oplus f\,(Ri\text{-}1, Ki)$$

*Structurally, Gost algorithm similar to DES (Data Encryption Standard). DES is a block cipher with a key length of 64 bits 56 bits. This algorithm iterates as many as 16 rounds of encryption algorithms (round). Since the key length is only 56 bits, making the algorithm is very prone to be a brute force that is currently used 3 pieces of DES in order to encrypt a paintext called Triple DES. Key length is also extended 3 times to 168 bits (56 * 3 = 168).GOST weakness known until now is because of its key schedule simple so in certain circumstances be a weak point of the method as Related-key cryptanalysis cryptanalysis. But this can be overcome by passing the key to the functioning of a strong cryptographic hash such as SHA-1, and then use the results to input initialization hash key). The advantage of this method is the speed GOST pretty good, although not as fast but faster than Blowfish IDEA.*

Once fully developed The results of the analysis , the authors draw the following conclusion :

1. *Making learning module cryptographic GOST method requires two important components, namely MSFlexGrid (Microsoft FlexGrid) used as a table and the Common Dialog Control is used to open the Open or Save dialog box.*
2. *This software can help understanding how the particular method or algorithm GOST.*
3. *The process of formation of the key to the method is very simple whereas GOST encryption and decryption process is long and complicated.*

Keywords: Cryptography, method of GOST, Text Encryption, Decryption Text