PEMBUATAN PERANGKAT LUNAK SEBAGAI MEDIA PEMBELAJARAN KRIPTOGRAFI MODERN METODE BLOWFISH

SKRIPSI

disusun oleh

Reza Fitra Kesuma

08.11.2273

JURUSAN TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM YOGYAKARTA
YOGYAKARTA
2013

PEMBUATAN PERANGKAT LUNAK SEBAGAI MEDIA PEMBELAJARAN KRIPTOGRAFI MODERN METODE BLOWFISH

SKRIPSI

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

disusun oleh

Reza Fitra Kesuma

08.11.2273

JURUSAN TEKNIK INFORMATIKA
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM YOGYAKARTA
YOGYAKARTA
2013

PERSETUJUAN

SKRIPSI

PEMBUATAN PERANGKAT LUNAK SEBAGAI MEDIA PEMBELAJARAN KRIPTOGRAFI MODERN METODE BLOWFISH

yang dipersiapkan dan disusun oleh

Reza Fitra Kesuma

08.11.2273

telah disetujui oleh dosen pembimbing skripsi
pada tanggal 11 Juli 2012

Dosen Pembimbing,

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

PENGESAHAN

SKRIPSI

PEMBUATAN PERANGKAT LUNAK SEBAGAI MEDIA PEMBELAJARAN KRIPTOGRAFI MODERN METODE BLOWFISH

yang dipersiapkan dan disusun oleh

Reza Fitra Kesuma

08.11.2273

telah dipertahankan di depan Dewan Penguji

pada tanggal 18 Juli 2013

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Ema Utami, Dr., S.Si, M.Kom **NIK. 190302037**	
Dony Ariyus, M.Kom **NIK. 190302128**	
Erik Hadi Saputra, S.Kom, M.Eng **NIK. 190302107**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 26 Juli 2013

KETUA STMIK AMIKOM YOGYAKARTA

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

PERNYATAAN

Saya yang bertanda tangan 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 disuatu 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, 28 Agustus 2013

Reza Fitra Kesuma
NIM 08.11.2273

MOTTO

Sesungguhnya kita milik Allah dan hanya kepada-Nya kita kembali

Hidup ini indah maka berjuanglah, jangan pernah menyerah dan putus asa, terus semangat

Hidup mulia atau mati syahid, kerjakan untuk dunia kita seakan kita hidup selamanya dan kerjakan untuk akhirat kita seakan kita akan mati esok hari

Masa depan kita ada ditangan kita sendiri, tidak ada yang bisa merubah selain diri kita sendiri, selalu kerjakan yang bermanfaat, yang terbaik menurut kita maka kita akan berbahagia

Manusia itu mulia selama harga dirinya belum ternoda

Jadikan sabar dan ikhlas pedoman hidup kita

Jangan jadi orang munafik, jujurlah, katakan yang sebenarnya walaupun itu pahit

PERSEMBAHAN

Skripsi ini kupersembahkan untuk :

- Ayahanda tercinta bapak M. Hanafiah, S.E. dan Ibunda tercinta ibu Terangta br. Karo, terima kasih atas doa dan dukungannya yang telah menuntunku sampai seperti sekarang ini.
- Abang-abangku M. Januar Hanta dan Sonny Prima Putra, terima kasih atas doanya.
- Seluruh guru dan dosenku yang telah memberikan ilmu yang bermanfaat kepadaku.
- Kawan-kawan seperjuangan Livonk, Danni, Ando, Puput, Fahri, Zakki dan banyak lagi.
- Dan Semua yang gak bisa ku sebutkan satu per satu karena keterbatasan ingatan ***thanks for all***

Kata Pengantar

Puji syukur kehadirat Allah SWT Yang Maha Mendengar lagi Maha Melihat dan atas segala limpahan rahmat, taufik, serta hidayah-Nya sehingga penulis dapat menyelesaikan karya tulis yang berbentuk skripsi ini sesuai dengan waktu yang telah direncanakan.

Shalawat serta salam semoga senantiasa tercurahkan kepada baginda Nabi Besar Muhammad SAW beserta seluruh keluarga dan sahabatnya yang selalu eksis membantu perjuangan beliau dalam menegakkan Dinullah di muka bumi ini.

Pesatnya kemajuan teknologi telah menjadikannya salah satu media utama pertukaran informasi. Melalui internet pertukaran informasi tersebut menjadi sangat mudah. Informasi tersebut ada yang bersifat publik, ada juga yang hanya ditujukan untuk satu orang ataupun kelompok tertentu. Internet merupakan jaringan komputer yang bersifat publik, oleh karena itu dibutuhkan suatu usaha untuk menjamin keamanan informasi tersebut.

Menyikapi hal tersebut, penulis merasa perlu untuk menulis skripsi dan menyajikannya untuk pembaca sebuah bagian dari ilmu keamanan komputer yaitu tentang kriptografi dimana penulis memfokuskan diri pada judul "Pembuatan Perangkat Lunak sebagai Media Pembelajaran Kriptografi Modern Metode Blowfish".

Dalam penulisan skripsi ini, tentunya banyak pihak yang telah memberikan bantuan baik moril maupun materil. Oleh karena itu penulis ingin menyampaikan ucapan terimakasih yang tiada hingganya kepada :

1. Ibu Dr. Ema Utami, S.Si, M.Kom selaku dosen pembimbing yang telah banyak memberikan bimbingan, nasehat dan arahan kepada penulis.
2. Bapak Prof. Dr. M.Suyanto M.M selaku ketua STMIK AMIKOM Yogyakarta beserta para dosen dan seluruh karyawan/ staf pegawai STMIK AMIKOM Yogyakarta atas bantuan selama penulis mengikuti studi.

3. Secara khusus penulis ingin mengucapkan terima kasih kepada Ayahanda yang penulis banggakan dan Ibundaku yang tercinta yang telah banyak memberikan dukungan dan pengorbanan baik secara moril maupun materil sehingga penulis dapat menyelesaikan studi dengan baik.
4. Ucapan terima kasih kepada semua sahabat yang telah banyak memberikan bantuan, dorongan serta motivasi sehingga skripsi ini dapat terselesaikan.

Penulis menyadari bahwa skripsi ini masih jauh dari kesempurnaan, maka saran dan kritik yang konstruktif dari semua pihak sangat diharapkan demi penyempurnaan selanjutnya.

Akhirnya hanya kepada Allah SWT kita kembalikan semua urusan dan semoga skripsi ini dapat bermanfaat bagi semua pihak, khususnya bagi penulis dan para pembaca pada umumnya, semoga Allah SWT meridhoi dan dicatat sebagai ibadah disisi-Nya, amin.

Yogyakarta, Juli 2013

Penyusun

DAFTAR ISI

DAFTAR GAMBAR

INTISARI

Kriptografi merupakan salah satu cabang ilmu komputer yang sangat mendasar dan sulit dipahami. Dalam hal teknik pengaman data, banyak metode kriptografi yang digunakan. Metode-metode kriptografi tersebut mempunyai teknik dan cara tersendiri. Langkah-langkah pengerjaan setiap metode pun berbeda-beda, baik dari segi panjang maupun kerumitan.

Salah satu metode kriptografi yang menarik untuk dipelajari adalah metode Blowfish. Keamanan metode Blowfish berada pada proses pembentukan kuncinya yang panjang dan rumit. Pembelajaran dari buku saja tentunya akan sulit untuk memahami kriptografi metode Blowfish. Maka untuk membantu memahami kriptografi Blowfish perlu disediakan perangkat lunak sebagai media pembelajaran berbasis dekstop yang dibuat menggunakan Visual Basic 6.0.

Perancangan perangkat lunak media pembelajaran tersebut diawali dengan membuat *form-form* yang mendukung pembelajaran kriptografi Blowfish, seperti *form* teori, *form* pengekspansian kunci, *form* enkripsi dan *form* dekripsi. *Form-form* tersebut kemudian dituangkan ke dalam program Visual Basic 6.0. Output yang didapat adalah *form-form* tersebut dapat memvisualisasikan proses pengekspansian kunci, proses enkripsi dan proses dekripsi. Dengan menggunakan media pembelajaran berbasis dekstop yang dibuat menggunakan Visual Basic 6.0, diharapkan dapat membantu memahami kriptografi metode Blowfish sehingga diharapkan pula dapat bermanfaat kedepannya.

Kata Kunci : Kriptografi, Blowfish, Media Pembelajaran, Visual Basic 6.0

ABSTRACT

Cryptography is one branch of computer science which is basic and hard to understand. In a technic of data security, there are a lot of cryptography methods that being used. These cryptography methods have its own way and technic. Steps that used to solve every method are different, both in terms of extensive and complexity.

One of the method of cryptography that interesting to be learned is Blowfish cryptography. The security of Blowfish method is inextensive and complexity of its expansion key. Learning from book only will be hard to understand Blowfish cryptography. Therefore to help to understand Blowfish cryptography there is need to provide a software as a media of learning Blowfish cryptography using Visual Basic 6.0.

The design of software as a media of learning Blowfish cryptography start from making forms that support learning of Blowfish cryptography, like theory form, expansion-key form, encryption form and decryption form. These form will be casted into visual basic 6.0. The output will be forms that can visualize expansion-key process, encryption process and decryption process. By using media of learning that based on dekstop which is made by Visual Basic 6.0, hoped can help to understand Blowfish cryptography and can be usefull in the future.

Keywords :*Cryptography, Blowfish, Media of learning, Visual Basic 6.0*