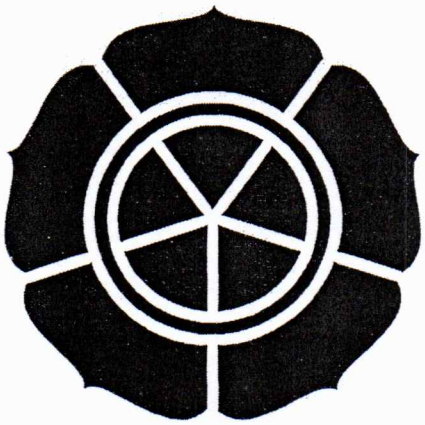
PERANGKAT LUNAK BANTU PEMAHAMAN KRIPTOGRAFI METODE MMB

(*MODULAR MULTIPLICATION-BASED BLOCK CHIPER*)

SKRIPSI

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



disusun oleh :

Hendra Yuliantoro

06.12.1946

JURUSAN SISTEM INFORMASI
SEKOLAH TINGGI MANAJEMEN INFORMATIKA DAN KOMPUTER
AMIKOM
YOGYAKARTA
2010

PERSETUJUAN

SKRIPSI

Perangkat Lunak Bantu Pemahaman Kriptografi

Metode MMB

(Modular Multiplication-Based Block Chiper)

Yang dipersiapkan dan disusun oleh

Hendra Yuliantoro

06.12.1946

telah disetujui oleh Dosen Pembimbing Skripsi

pada tanggal 22 Juli 2010

Dosen Pembimbing

Ema Utami, S.Si, M.Kom

NIK. 190302037

PENGESAHAN

SKRIPSI

Perangkat Lunak Bantu Pemahaman Kriptografi

Metode MMB

(Modular Multiplication-Based Block Chiper)

yang dipersiapkan dan disusun oleh

Hendra Yuliantoro

06.12.1946

telah dipertahankan di depan Dewan Penguji
pada tanggal 20 Juli 2010

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Amir Fatah Sofyan,ST,M.Kom **NIK. 190302047**	
Hanif Al Fatta,M.Kom **NIK. 190302096**	
Ema Utami,S.Si,M.Kom **NIK. 190302037**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 30 Oktober 2010

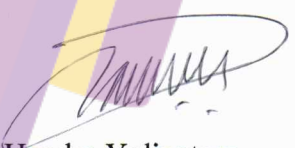
KETUA STMIK AMIKOM YOGYAKARTA

Prof. Dr. M. Suyanto, MM.
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 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,23 Juli 2010



Hendra Yuliantoro

06.12.1946

PERSEMBAHAN

Tiada kata yang bijak dari pada kata terima kasih .....

Pada halaman persembahan ini saya ingin mengucapkan puji syukur kehadirat **Allah SWT** yang telah memberikan rahmat dan hidayahnya sehingga saya mampu menyelesaikan pembuatan skripsi ini. Skripsi ini saya persembahkan kepada :

- Terutama kepada kedua orang tuaku yang tercinta terima kasih atas kasih sayangnya , nasihatnya ,do'a restunya dan dukungannya selama ini.
- Buat seluruh anggota keluargaku yang selalu jadi inspirasiku.
- Buat dosen pembimbing dan penguji yang telah mempermudah jalannya skripsiku.
- Buat saudara-saudara ku/teman-teman ku **ASEM KERE** yang selalu menjadi saudara/teman terbaik, TETAP SEMANGAT!!.
- Ank-anak SI kelas G 2006 terima kasih juga atas dukungannya.

MOTTO

✓ "Hidup Adalah Perjuangan"
(Life For Nothing Or Die For Something)

✓ "Hati Seluas Samudera"
(Tanpa Ada Batas Tak Pernah Bertepi)
(Menerima, Tak keluh kesah)

✓ "Malam Yang Gelap Selalu Di ikuti
Pagi Yang Tenang"

KATA PENGANTAR

Assalamu'alaikum Wr.Wb.

Puji syukur kehadirat Allah Subhanahu Wata'ala" hanya karena izinNya lah penulis mampu menyelesaikan kewajiban sebagai mahasiswa. Sanjungan kebaikan hanya penulis tujukan kepada Habibullah Muhammad SAW yang telah menaburkan kilau Al-Qur'anulkarim dan mutiara sunnah-Nya.

Penyusunan dan penulisan skripsi dengan judul "***Perangkat Lunak Bantu Pemahaman Kriptografi Metode MMB (Modular Multiplication-Based Block Chiper)***" ini bertujuan untuk memenuhi syarat kelulusan perguruan tinggi program studi Strata-1 Sistem Informasi dan mendapatkan gelar kesarjanaan dalam bidang komputer di Sekolah Tinggi Manajemen Informatika dan Komputer AMIKOM Yogyakarta.

Dalam proses penyusunan dan penulisan skripsi, penulis menyadari bahwa kemampuan penulis terbatas. Oleh karena itu, penulis menyampaikan terima kasih kepada pihak-pihak yang turut terlibat dari awal proses hingga akhir, antara lain:

1. Bapak Prof.Dr.M.Suyanto,MM,Ph.d selaku Ketua Sekolah Tinggi Manajemen Informatika dan Komputer AMIKOM Yogyakarta.
2. Ibu Ema Utami,S.Si,M.Kom selaku Pembimbing yang telah banyak meluangkan waktu untuk membimbing dan mengarahkan sehingga skripsi ini dapat terselesaikan.
3. Teman-teman semua yang turut membantu dalam penyusunan skirpsi sehingga skripsi ini dapat terselesaikan.

Penulis memahami bahwa dalam penyusunan dan penulisan skripsi ini masih ada kekurangan, untuk itu penulis mengharapkan peran aktif pembaca dengan memberikan kritik dan saran sebagai masukan.

Mudah-mudahan penyusunan dan penulisan skripsi ini dapat memberikan manfaat dan ruang yang lebar bagi pembaca untuk berkreasi lebih sempurna dalam menuangkan hasil karya.

Wassalamu'alaikum Wr.Wb.

Yogyakarta, Juli 2010

Hendra Yuliantoro

DAFTAR ISI

DAFTAR GAMBAR

INTISARI

Kelemahan metode IDEA yang menggunakan *plaintext* 64 bit dan operasi perkalian modulo $2^{16} + 1$, diperbaiki oleh Joan Daemen dalam sebuah algoritma yang dinamakan MMB (*Modular Multiplication-based Block cipher*). Dengan menggunakan *plaintext* 64 bit (4 buah 16 bit *subblock text*), metode IDEA hanya dapat diimplementasikan pada prosesor 16 bit, sehingga dinilai tidak dapat mengikuti perkembangan teknologi pada saat ini yang kebanyakan telah menggunakan prosesor 32 bit. Kriptografi metode MMB menggunakan *plaintext* 128 bit dan algoritma iteratif yang terdiri dari langkah-langkah linier (seperti XOR dan aplikasi kunci) serta aplikasi paralel dari empat substitusi non linier besar yang dapat dibalik. Substitusi ini ditentukan oleh sebuah operasi perkalian modulo $2^{32} - 1$ dengan faktor konstan, yang memiliki tingkat sekuritas lebih tinggi bila dibandingkan dengan metode IDEA yang hanya menggunakan operasi perkalian modulo $2^{16} + 1$. MMB menggunakan 32 bit *subblock text* (x_0, x_1, x_2, x_3) dan 32 bit *subblock* kunci (k_0, k_1, k_2, k_3). Hal ini membuat algoritma tersebut sangat cocok diimplementasikan pada prosesor 32 bit. Sebuah fungsi non linier, f, diterapkan enam kali bersama dengan fungsi XOR.

Kerumitan algoritma ini, yang terletak pada proses operasi perkalian modulo $2^{32} - 1$, perhitungan fungsi non linier f pada proses enkripsi dan dekripsi, serta operasi *invers* pada proses dekripsi, menyebabkan algoritma ini sulit diproses secara manual.

Berdasarkan uraian di atas, maka program *Microsoft Visual Basic 6.0* dipilih sebagai bahan utama.

kata kunci.

ABSTRACT

The weakness of IDEA method which using plaintext 64 bit and multiple modulo operation $2^{16} + 1$, fixed by Joan Daemen in an algorithm that called MMB (Modular Multiplication-based Block Chiper). Using plaintext 64 bit (4 pieces of 16 bit subblock text), IDEA only can implemented on 16 bit processor. So that unfollowed by technology development for now that most of it using 32 bit processor. Kriptografi MMB method using plaintext 128 bit and itearatif algorithm which consist of linier steps (like XOR and application key) also parallel application from four big non linier substitution that can be turned. This substitution determined by an multiple modulo $2^{32} - 1$ operation with constant factor, which is have higher security level it compared with IDEA method that used multiple modulo $2^{16} + 1$ operation. MMB using 32 bit subblock text (x_0, x_1, x_2, x_3) and 32 bit subblock key (k_0, k_1, k_2, k_3). This one make the algorithm very appropriate it implemented on 32 bit procesor. A non linier function,f, applied six times with the function of XOR.

Complexity of this algorithm, multiple modulo $2^{32} - 1$ process is the calculation of non linier f function on encryption and description process, also invers operation on description process which is causes this algorithm difficult in manual process.

Based on explanation above, so Microsoft visual basic 6.0 program choosed as the main limitation.

Keyword :