

ABSTRAK

Keamanan data merupakan salah satu aspek yang sangat penting bagi berbagai keperluan sekarang ini. Di era informasi ini, merupakan keharusan untuk dapat menjaga keamanan dari data yang dikirimkan. Dalam upaya tersebut, salah satunya ialah dengan mengenkripsi data yang akan dikirimkan.

Enkripsi secara umum dibagi menjadi dua macam, yaitu enkripsi simetrik dan asimetrik. Untuk menyandikan dan menerjemahkan kembali suatu data digunakan kunci. Enkripsi simetrik menggunakan satu kunci yang sama untuk proses enkripsi dan dekripsi. Sedangkan enkripsi asimetrik menggunakan kunci rahasia untuk mengenkripsi, dan kunci privat untuk mendekripsi data yang telah disandikan sebelumnya.

Pada tugas akhir ini direalisasikan suatu perangkat lunak pengamanan data yang menggunakan algoritma simetrik dengan metode enkripsi VMPC. Perangkat lunak ini dibuat dalam bahasa pemrograman *Visual Basic*. Program pengamanan data ini mempunyai 7 program utama yaitu : program Inisialisasi VMPC dan *Mixing S-Box*, program Enkripsi *Plaintext*, program Pembangkit Kunci Tanda Tangan Digital, program Validasi dan Tanda Tangan Digital, program Dekripsi *Ciphertext*, program Pembuka *Decipheredtext*, dan program Verifikasi.

Berbagai pengamatan telah dilakukan terhadap input dan output dari perangkat lunak ini. Dari pengamatan-pengamatan tersebut, disimpulkan bahwa perangkat lunak pengamanan data dengan algoritma VMPC telah berhasil direalisasikan.

ABSTRACT

Data security are one of the most important aspects for numerous needs nowdays. In this information era, it's an undeniable need to guard the data security being deliver. To achieve that goal, one of the solutions is to encrypt that data.

Generaly there are two types of encryption, symmetric and asymmetric encryption. A key is use to encrypt and decrypt back a data. Symmetric encryption use exactly same key to encrypt and decrypt the data. In other hand asymmetric encryption use public key to encrypt, and private key to decrypt the data being encrypt before.

In this final assignment the software being realized is using symmetric algorithm with VMPC encryption methode. This software was made with *Visual Basic* programming language. This data security program consists of 7 main programs which are: Initializes VMPC and Mixing S-Box, Plaintext encryption, Digital Signature key generator, Validation and Digital Signature, Ciphertext decryption, Open Decipheredtext, and Verification.

Various observation have been done for this software input and output. From those observation, it have reach a conclusion that data security software with VMPC algorithm have succed being realized.

KATA PENGANTAR

Penulis memanjatkan puji syukur kepada Tuhan Yang Maha Esa atas berkat dan kasihNya sehingga penulis dapat menyelesaikan tugas akhir yang berjudul “Pengamanan Data dengan Kriptografi VMPC” yang merupakan salah satu syarat untuk menyelesaikan Program Studi Strata Satu di Fakultas Teknik Jurusan Teknik Elektro Universitas Kristen Maranatha.

Selesainya tugas akhir ini tidak terlepas dari bantuan pihak-pihak yang telah memberikan banyak masukan bagi penulis, karena tanpa mereka mungkin penulis tidak dapat menyelesaikan Tugas Akhir ini. Untuk itu penulis mengucapkan terimakasih yang sebesar – besarnya kepada :

1. Bapak Marvin Chandra Wijaya, ST., MM., MT. selaku dosen pembimbing atas semua bimbingan dan petunjuk untuk menyelesaikan tugas akhir ini.
2. Bapak Semuil Tjiharjadi, ST., MM., MT. selaku dosen pengajar dan dosen penguji.
3. Bapak Ir. Judea Janoto Jarden, MT. selaku dosen pengajar dan dosen penguji.
4. Ibu Ir. Audyati Gany selaku dosen pengajar dan penguji.
5. Ibu Ratnadewi, ST., MT. selaku dosen pengajar dan penguji.
6. Bapak Riko Arlando Saragih ST., MT. selaku dosen wali dan dosen pengajar.
7. Bapak Ir. Aan Darmawan, MT. selaku dosen pengajar dan Ketua Jurusan Teknik Elektro Universitas Kristen Maranatha.
8. Ibu Ir. Anita Supartono, M.Sc. selaku dosen pengajar dan Koordinator Tugas Akhir.
9. Seluruh Dosen dan Staff Pengajar di lingkungan Fakultas Teknik Elektro Universitas Kristen Maranatha.
10. Segenap Karyawan dan Karyawati Tata Usaha Jurusan Teknik Elektro Universitas Kristen Maranatha atas segala bantuannya.
11. Kepada ayah, kakak, dan saudara-saudara yang selalu mendoakan.

12. Kepada Teguh Reinaldo yang banyak membantu dalam perancangan dan pembuatan tugas akhir.
13. Kepada seluruh teman dan kenalan di Maranatha khususnya kepada Chandra, Danny Wibowo, Sandy Verdian, Sandy, Anton dan Tjei Eng.
14. Kepada Feri, Yunus, Ardianto, Audi, Lina, Novi, Sherly, Natalia, dan Jefry atas dukungan dan motivasinya.
15. Kepada Frans Setiadi, Katarina Kurniawan, dan semua teman-teman yang selalu menyemangati.
16. Segenap pihak yang belum disebutkan yang telah membantu secara langsung maupun tidak langsung terselesaiannya tugas akhir ini.

Akhir kata penulis mohon maaf atas segala kekurangan dalam penulisan tugas akhir ini. Segala saran dan kritik yang membangun akan diterima dengan senang hati agar laporan Tugas Akhir ini dapat lebih memberikan manfaat bagi yang memerlukannya, terimakasih.

Penulis

DAFTAR ISI

ABSTRAK.....	i
KATA PENGANTAR.....	iii
DAFTAR ISI.....	v
DAFTAR GAMBAR	viii
DAFTAR TABEL	ix
BAB I PENDAHULUAN.....	1
1.1 Latar Belakang.....	1
1.2 Identifikasi masalah.....	2
1.3 Tujuan.....	2
1.4 Pembatasan Masalah.....	2
1.5 Sistematika Pembahasan.....	2
BAB II TEORI PENUNJANG	4
2.1 Kriptologi, Kriptoanalisis, dan Kriptografi.....	4
2.1.1 Tujuan Kriptografi.....	4
2.1.2 Enkripsi dan Dekripsi.....	5
2.1.3 Algoritma dan Kunci.....	6
2.1.3.1 Algoritma Simetrik.....	7
2.1.3.2 Algoritma Kunci Publik.....	8
2.2 Perbandingan antara algoritma simetrik dengan algoritma kunci publik.....	9
2.3 Teori Matematika.....	11
2.3.1 Bilangan Prima.....	11
2.3.2 Operasi Modulus.....	11
2.3.3 Algoritma Euclidean.....	12
2.3.4 Algoritma Extended Euclidean.....	13
2.3.5 Eksponensial Modulus.....	14
2.3.6 Fungsi XOR.....	15
2.3.7 Fungsi AND.....	15
2.4 Algoritma VMPC	16
2.5 Algoritma Validasi Data.....	17

2.6 Algoritma Tanda Tangan Digital	17
2.6.1 Algoritma Pembangkit Kunci Tanda Tangan Digital.....	18
2.6.2 Algoritma Tanda Tangan Digital.....	18
2.6.3 Algoritma Verifikasi Tanda Tangan Digital.....	18
BAB III IMPLEMENTASI DAN REALISASI PERANGKAT LUNAK	19
3.1 Program Pengaman Data.....	19
3.2 Program Utama.....	21
3.2.1 Program Inisialisasi dan Mixing S-Box.....	21
3.2.2 Program Enkripsi Plaintext.....	22
3.2.3 Program Pembangkit Kunci Tanda Tangan Digital.....	23
3.2.3.1 Sub Program rdmprime dan rdmprime2.....	24
3.2.3.2 Sub Program gcd.....	26
3.2.3.3 Sub Program euclid.....	27
3.2.4 Program Validasi dan Tanda Tangan Digital.....	28
3.2.4.1 Sub Program Pangkatmod.....	29
3.2.4.2 Sub Program DecimalToBinary.....	30
3.2.5 Program Dekripsi Ciphertext.....	30
3.2.6 Program membuka Deciphered Text.....	32
3.2.7 Program Verifikasi.....	33
BAB IV HASIL PENGAMATAN	34
4.1 Hasil Pengamatan	34
4.1.1 Hasil Pengamatan 1	34
4.1.2 Hasil Pengamatan 2	35
4.1.3 Hasil Pengamatan 3	35
4.1.3.1 Hasil Pengamatan <i>File Text</i> 1	35
4.1.3.2 Hasil Pengamatan <i>File Text</i> 2	36
4.1.4 Hasil Pengamatan 4	37
4.1.5 Hasil Pengamatan 5	38
4.1.6 Hasil Pengamatan 6	38
4.1.7 Hasil Pengamatan 7	40

4.1.7.1 Pengamatan <i>PlainText</i> , <i>CipherText</i> , <i>DecipeheredText</i> , nilai publik key dan private key, dengan file <i>Validasi+Sign</i> yang benar	40
4.1.7.2 Pengamatan <i>PlainText</i> , file <i>Validasi+Sign</i> , nilai publik key dan private key dengan <i>DecipeheredText</i> yang salah karena perubahan pada <i>CipherText</i>	41
4.1.7.3 Pengamatan <i>PlainText</i> , <i>CipherText</i> , <i>DecipeheredText</i> , file <i>Validasi+Sign</i> , dengan pengisian nilai public key yang salah	42
4.1.7.4 Pengamatan <i>PlainText</i> , <i>CipherText</i> , <i>DecipeheredText</i> , file <i>Validasi+Sign</i> , dengan membuka file <i>Validasi+Sign</i> yang salah pada waktu perbandingan	43
4.2 Analisa Hasil Pengamatan.....	44
BAB V KESIMPULAN DAN SARAN	46
5.1 Kesimpulan.....	46
5.2 Saran.....	46
DAFTAR PUSTAKA.....	47
LAMPIRAN A LISTING PROGRAM.....	A-1
LAMPIRAN B TAMPILAN PROGRAM PENGAMAN DATA.....	B-1

DAFTAR GAMBAR

Gambar 2.1 Diagram Blok Enkripsi	5
Gambar 2.2 Diagram Blok Dekripsi	6
Gambar 2.3 Diagram Blok Enkripsi Dengan Menggunakan Kunci	7
Gambar 2.4 Diagram Blok Dekripsi Dengan Menggunakan Kunci	7
Gambar 2.5 Diagram Blok Algoritma Simetrik	8
Gambar 2.6 Diagram Blok Enkripsi Pada Algoritma Kunci Publik	9
Gambar 2.7 Diagram Blok Dekripsi Pada Algoritma Kunci Publik	9
Gambar 3.1 Diagram Alir Utama Program Pengaman Data	20
Gambar 3.2 Diagram Alir Program Inisialisasi dan Mixing S-Box	21
Gambar 3.3 Diagram Alir Program Enkripsi Plaintext	22
Gambar 3.4 Diagram Alir Program Pembangkit Kunci Tanda Tangan Digital ..	23
Gambar 3.5 Diagram Alir Sub Program RdmPrime	24
Gambar 3.6 Diagram Alir Sub Program RdmPrime2	25
Gambar 3.7 Diagram Alir Sub Program gcd	26
Gambar 3.8 Diagram Alir Sub Program euclid	27
Gambar 3.9 Diagram Alir Sub Program Validasi dan Tanda Tangan Digital ..	28
Gambar 3.10 Diagram Alir Sub Program Pangkatmod	29
Gambar 3.11 Diagram Alir Sub Program DecimalToBinary	30
Gambar 3.12 Diagram Alir Program Dekripsi CipherText	31
Gambar 3.13 Diagram Alir Program Pembuka Dechiphered Text	32
Gambar 3.14 Diagram Alir Program Verifikasi	33

DAFTAR TABEL

Tabel 2.1 Nilai Extended Euclidean.....	13
Tabel 4.1 Hasil Pengamatan Dengan Secret Key sama.....	34
Tabel 4.2 Hasil Pengamatan Dengan Karakter Plaintext Berbeda.....	35
Tabel 4.3 Hasil Pengamatan Ukuran File Ciphertext Dengan Plaintext Yang Berbeda dan Secret Key Sama.....	38
Tabel 4.4 Hasil Pengamatan Ukuran File Ciphertext Dengan Plaintext Yang Sama dan Secret Key Berbeda-beda.....	38