

ABSTRACT

Data security is very important at this moment, because many hackers or spywares want to know the important information from a message which is usable for personal purpose. To send data on personal computer networking or telecommunication system, a software which can protect information on a message is needed.

Encryption and decryption using SEAL stream cipher is a software which is made to randomize a message and can transform random message into original message, with RSA algorithm for digital signature and CRC algorithm for checking the difference between the message with the original one.

A plaintext which is converted to ciphertext with SEAL encryption and ciphertext which is sent to other people. If one want to read the original message from ciphertext then SEAL decryption software is needed and must put the right password.

ABSTRAK

Keamanan data saat ini merupakan suatu hal yang sangat penting, karena banyaknya penyusup atau *spyware* yang menginginkan informasi dari suatu pesan yang dapat dimanfaatkan untuk kepentingan pribadi. Untuk mengirimkan suatu data pada jaringan komputer atau sistem telekomunikasi diperlukan program yang dapat melindungi isi dari pesan tersebut.

Enkripsi dan dekripsi *stream cipher* dengan metoda SEAL adalah software yang dirancang untuk mengacak isi dari suatu pesan dan mengubah pesan acak tersebut menjadi pesan asli, disertai dengan algoritma RSA sebagai digital signature dan algoritma CRC check untuk memeriksa perbedaan dari suatu pesan dengan pesan aslinya.

Suatu pesan plaintext diolah kedalam enkripsi SEAL kemudian didapatkan keluaran sebuah file ciphertext yang siap dikirimkan kepada orang lain. Jika ingin membaca pesan asli dari ciphertext maka diperlukan software dekripsi SEAL dan harus memasukkan password yang sesuai.

DAFTAR ISI

LEMBAR PENGESAHAN

SURAT PERNYATAAN

ABSTRAK	i
ABSTRACT	ii
KATA PENGANTAR	iii
DAFTAR ISI	v
DAFTAR GAMBAR	viii
DAFTAR TABEL	x

BAB I. PENDAHULUAN	1
I.1. Latar Belakang	1
I.2. Identifikasi Masalah	2
I.3. Tujuan	2
I.4. Pembatasan Masalah	2
I.5. Sistematika Pembahasan	3

BAB II. TEORI PENUNJANG	4
II.1. Cryptografi Klasik	4
II.2. Simple XOR	5
II.3. Kunci Symetris	6
II.4. Kunci Asymetris	6
II.5. SHA (Secure Hash Algorithm)	8
II.6. Stream Cipher	9

II.7. Stream Cipher dengan algoritma SEAL	10
II.8. Microsoft Visual Basic	13
II.8.1. Tampilan aplikasi Visual Basic	14
II.8.2. Properties	15
II.8.3. Ruang dan teknik penulisan	20
II.8.4. Penulisan program	21
BAB III. PERANCANGAN	30
III.1. Pendahuluan	30
III.2. Perancangan SEAL berdasarkan key	30
III.3. Membuat interface program SEAL symetris key	30
III.4. Membuat interface program SEAL asymetris key	34
III.5. Membuat interface RSA keymaker	36
III.6. Diagram alir	38
III.6.1. Skema perancangan program symetris SEAL	39
III.6.2. Skema perancangan program asymetris SEAL(RSA)	42
BAB IV. UJI COBA DAN ANALISA DATA	48
IV.1. SEAL symetris key	48
IV.1.1. Enkripsi data	49
IV.1.2. Dekripsi data	51
IV.1.3. Test Speed	52
IV.2. SEAL asymetris key	53
IV.2.1. RSA keymaker	54
IV.2.2. Enkripsi data SEAL dengan RSA	56
IV.2.3. Dekripsi data SEAL dengan RSA	57

IV.3. Data pengamatan	59
BAB V. KESIMPULAN DAN SARAN	64
V.1. Kesimpulan	64
V.2. Saran	64
DAFTAR PUSTAKA	65
LAMPIRAN : <i>Source code</i> enkripsi dan dekripsi SEAL.	

DAFTAR GAMBAR

Gambar II.1 – Diagram blok SHA	8
Gambar II.2.1 – SEAL encryption	11
Gambar II.2.2 – SEAL decryption	12
Gambar II.3 – Tampilan kerja Microsoft Visual Basic	14
Gambar II.4 – Immediate Window	20
Gambar II.5 – View Code	21
Gambar III.1 – Menu Microsoft Visual Basic ver6.0	31
Gambar III.2 – Tampilan form	31
Gambar III.3 – Membuat tombol	32
Gambar III.4 – Mengganti nama pada tombol	32
Gambar III.5 – Membuat Text Box	33
Gambar III.6 – SEAL symetris key	34
Gambar III.7 – SEAL asyemetris key	36
Gambar III.8 – RSA key generator	37
Gambar III.9 – RSA key generator 2	37
Gambar III.10 – RSA key generator 3	38
Gambar III.11 – Diagram alur enkripsi SEAL symetris	39
Gambar III.12 – Diagram alur dekripsi SEAL symetris	40
Gambar III.13 – Diagram alur enkripsi SEAL asyemetris (RSA)	43
Gambar III.14 – Diagram alur dekripsi SEAL asyemetris (RSA)	44
Gambar III.15 – Diagram alur RSA keymaker	45
Gambar III.16 – Diagram alur SHA	46

Gambar III.17 – Diagram alur CRC.....	47
Gambar IV.1 – SEAL symetris key	48
Gambar IV.2 – Password dan open file enkripsi	49
Gambar IV.3 – Hasil enkripsi SEAL symetris	50
Gambar IV.4 – Hasil enkripsi SEAL symetris.....	51
Gambar IV.5 – Tes speed	52
Gambar IV.6 – SEAL asyemetis key.....	53
Gambar IV.7 – RSA <i>keymaker</i> tahap pertama	54
Gambar IV.8 – RSA <i>keymaker</i> tahap kedua	55
Gambar IV.9 – RSA <i>keymaker</i> tahap akhir.....	55
Gambar IV.10 – Hasil enkripsi SEAL asyemetris	56
Gambar IV.11 – Hasil dekripsi SEAL asyemetris	58
Gambar IV.12 – Dekripsi salah.....	59

DAFTAR TABEL

Tabel II.1 – Properties form.....	15
Tabel II.2 – Properties <i>label</i>	17
Tabel II.3 – Properties text box	18
Tabel II.4 – Properties command button.....	19
Tabel II.5 – Jenis data	23
Tabel II.6 – Tabel Aritmatik	25
Tabel II.7 – Tabel Pembanding.....	25
Tabel II.8 – Tabel Logika.....	26
Tabel II.9 – Contoh perintah immediate window	27
Tabel IV.1 – Enkripsi symetris key	60
Tabel IV.2 – Dekripsi symetris key	60
Tabel IV.3 – Enkripsi asyemetris key.....	61
Tabel IV.4 – Dekripsi asyemetris key.....	61
Tabel IV.5 – Tes panjang password terhadap enkripsi symetris key.....	62
Tabel IV.6 – Tes panjang password terhadap dekripsi symetris key.....	62
Tabel IV.7 – Rasio perbandingan hasil enkripsi dan dekripsi	63
Tabel IV.8 – Tes CRC check pada dekripsi SEAL <i>symetris</i> dan <i>asyemetris</i>	63