ABSTRAK

Web merupakan suatu aplikasi menyediakan layanan yang memungkinkan pengguna untuk mengakses suatu informasi. Keamanan sebuah data dalam aplikasi sangatlah penting keberadaannya sehingga kita harus memberikan prioritas. Karena pada saat ini pencurian informasi atau data sudah banyak dilakukan, maka dari itu berbagai cara dilakukan untuk memberikan keamanan. Salah satu cara yang dapat dilakukan untuk keamanan suatu data adalah melakukan enkripsi dengan menggunakan suatu algoritma, baik dilakukan enkripsi untuk jalur transfer data atau hanya untuk enkripsi data.

Pada penelitian ini akan dibahas penerapan RSA pada sistem autentikasi website yang menggunakan protokol *Secure Socket Layer* (SSL) sebagai jalur yang aman antara *client-server*. RSA merupakan salah satu algoritma kriptografi asimetris yang menggunakan sepasang kunci, yaitu kunci publik dan kunci pribadi. Panjang kunci dapat diatur, dimana semakin panjang bit pembentukan kunci maka semakin sukar untuk dipecahkan karena sulitnya memfaktorkan dua bilangan yang sangat besar.

Aplikasi ini menambah tingkat keamanan di sisi server dengan pertama-tama mengenkripsi *plaintext username* dan *password* menjadi *ciphertext* menggunakan RSA. Teknik ini mencegah para *hacker* mendapatkan *plaintext* dari password dengan menggunakan teknik *brute force*.

Kata kunci : *SSL, RSA, Kriptografi*

ABSTRACT

Web is an application providing a service that allows users to access the information. Security of data in an application is important given that we should give priority. Because at this time stealing information or data has been done, and therefore different methods are used to provide security. One way to do for the security of an encryption of data is using an algorithm, not only encryption for grid of data transfer, but also for data encryption.

This research will be discussed about the implementation of RSA on the website authentication system that uses Secure Socket Layer protocol (SSL) as a safe path between the client-server. RSA is a cryptography algorithm that uses an asymmetric key pair, the public key and private key. Key length can be set, in which the key bit length of the formation of the more difficult to solve because of the difficulty of factoring two large numbers.

This added level of security applications on the server by first encrypt the plaintext into ciphertext for example username and password using RSA. This technique prevents hackers from getting plaintext password using brute force techniques.

Keywords: *Cryptography, SSL, RSA*

DAFTAR ISI

PRAKATA i
ABSTRAK iii
ABSTRACT iv
DAFTAR GAMBAR vii
DAFTAR TABEL ix
DAFTAR SIMBOL x
DAFTAR LAMPIRAN xi
BAB I PENDAHULUAN 1
1.1 Latar Belakang 1
1.2 Rumusan Masalah 2
1.3 Batasan Masalah 2
1.4 Tujuan 2
1.5 Sistematika Pembahasan 3
BAB II LANDASAN TEORI 4
2.1 Pengenalan Kriptografi 4
2.2 Algoritma Kriptografi 5
2.2.1 Algoritma Simetris 5
2.2.2 Algoritma Asimetris 6
2.3 Algoritma Rivest-Shamir-Adleman (RSA) 6
2.2.1 Serangan-Serangan di RSA 10
2.2.2 Keamanan Algoritma RSA 11
2.4 Secure Socket Layer (SSL) 12
2.5 Cara Kerja SSL 12
2.6 Web *Server* Apache 13
2.7 *Flowchart* 14
2.8 Wireshark 15
2.9 Ettercap 18
BAB III ANALISIS DAN PERANCANGAN 21
3.1 Analisis Masalah 21
3.1.1 Gambaran Umum Sistem 21

3.2 Proses Kerja 23
3.3 Arsitektur Sistem Jaringan 24
3.4 Perancangan Perangkat Lunak 24
3.4.1 Proses pada Pesan 26
3.4.2 Proses Enkripsi Pesan 27
3.4.3 Proses Dekripsi Pesan 28
3.5 Spesifikasi Sistem 29
3.5.1 Spesifikasi Perangkat Keras (*Hardware*) pada *Server* 29
3.5.2 Spesifikasi Perangkat Keras (*Hardware*) pada *Client* 29
3.5.3 Spesifikasi Perangkat Lunak (*Software*) pada *Server* 30
3.5.4 Spesifikasi Perangkat Lunak (*Software*) pada *Client* 30
BAB IV PENGEMBANGAN PERANGKAT LUNAK 31
4.1 Implementasi Sistem 31
4.1.1 Instalasi Web *Server* 31
4.1.2 Konfigurasi Web *Server* 32
4.1.3 Konfigurasi Database 34
4.1.4 HTML Script dan Java Script 35
BAB V TESTING DAN PENGUJIAN 43
5.1 Rencana Pengujian 43
5.1.1 Pelaksanaan Pengujian Sistem Autentikasi 44
BAB VI KESIMPULAN DAN SARAN 50
6.1 Kesimpulan 50
6.2 Saran 50
DAFTAR PUSTAKA 51

DAFTAR GAMBAR

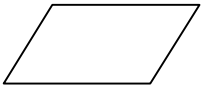
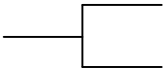
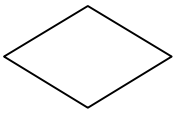
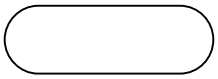
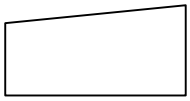
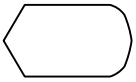
Gambar 2.1 Enkripsi dan Dekripsi [Munir 2006:15].....5
Gambar 2.2 Prosedur Kerja Algoritma Simetris [Munir 2006:17].....5
Gambar 2.3 Prosedur Kerja Algoritma Simetris [Munir 2006:23].....6
Gambar 2.4 Algoritma RSA [Schneier 1995:389] 8
Gambar 2.5 Taxonomy of Potential Attact on RSA [Stallings 2003:203].....10
Gambar 2.6 Cara kerja SSL [Stephen 2000:38] 12
Gambar 2.7 Option interface 16
Gambar 2.8 Capture interface.....16
Gambar 2.9 Paket data Wireshark 17
Gambar 2.10 Follow TCP Stream 17
Gambar 2.11 Sniffing username dan password.....17
Gambar 2.12 Tampilan awal Ettercap 19
Gambar 2.13 Tampilan network interface 19
Gambar 2.14 ARP poisoning.....19
Gambar 2.15 Koneksi pada Ettercap 20
Gambar 2.16 Sniffing username dan password.....20
Gambar 3.1 Flowchart proses kerja 23
Gambar 3.2 Arsitektur sistem jaringan yang akan dirancang 24
Gambar 3.3 Tahap pembangunan sistem 25
Gambar 3.4 Proses yang terjadi pada teks 26
Gambar 3.5 Proses enkripsi pada sisi client.....27
Gambar 3.6 Proses dekripsi pada sisi server 28
Gambar 4.1 Instalasi XAMPP 1.7.3 31
Gambar 4.2 XAMPP 1.7.3 setup 32
Gambar 4.3 XAMPP 1.7.3 control panel 32
Gambar 4.4 Sertifikat SSL 32
Gambar 4.5 Konfigurasi file httpd-ssl.conf.....33
Gambar 4.6 Konfigurasi file httpd-vhost.conf 33
Gambar 4.7 Jendela autentikasi pada database.....34
Gambar 4.8 Query membuat tabel.....34

Gambar 4.9 Query tabel user.....35
Gambar 4.10 Isi tabel user.....35
Gambar 4.11 Alur enkripsi pada web browser.....35
Gambar 4.12 Proses enkripsi.....36
Gambar 4.13 Kode program jika berhasil login.....37
Gambar 4.14 Kode program jika berhasil login.....38
Gambar 4.15 Proses dekripsi.....39
Gambar 4.16 Proses pencocokan dengan database.....40
Gambar 4.17 Koneksi dengan database.....41
Gambar 4.18 Proses logout.....41
Gambar 4.19 Halaman login pada client.....42
Gambar 4.20 Halaman berhasil login pada client.....42
Gambar 5.1 Hasil pengujian sistem autentikasi.....44
Gambar 5.2 Monitoring Wireshark dengan username “308080008”.....46
Gambar 5.3 Monitoring Ettercap dengan username “308080008”.....47
Gambar 5.4 Monitoring Wireshark dengan username “308080009”.....47
Gambar 5.5 Monitoring Ettercap dengan username “308080009”.....48
Gambar 5.6 Monitoring Wireshark dengan username “308080010”.....48
Gambar 5.7 Monitoring Ettercap dengan username “308080010”.....49
Gambar 5.8 Monitoring SSL.....49

DAFTAR TABEL

Tabel 3.1 Perangkat keras di sisi *server*.....29
Tabel 3.2 Perangkat keras di sisi *client*.....30
Tabel 3.3 Perangkat lunak di sisi *server* 30
Tabel 3.4 Perangkat lunak di sisi *client* 30
Tabel 5.1 Hasil pengujian sistem autentikasi 45

DAFTAR SIMBOL

Simbol	**Keterangan**
Proses 	Merepresentasikan operasi.
Input/Output 	Merepresentasikan *input* data atau *output* data yang diproses atau informasi
Anak Panah 	Merepresentasikan alur kerja
Penjelasan 	Digunakan untuk komentar tambahan
Keputusan 	Keputusan dalam program.
Terminal points 	Awal/akhir *flowchart*
Manual Input 	*Input* yang dimasukkan secara manual dari *keyboard*.
Display 	*Output* yang ditampilkan pada terminal

DAFTAR LAMPIRAN

Surat Keterangan Penelitian A.1
Riwayat Hidup Penulis A.2