ABSTRAK

Dalam dunia internet tidak ada yang benar-benar aman. Selalu saja ada celah dalam setiap aplikasi yang dibuat. Untuk memininalisir serangan dapat menggunakan enkripsi pada data ketika data tersebut dikirimkan. Salah satu algoritma kriptografi yang cukup populer adalah algoritma RSA, dinamakan (Rivest-Shamir-Addlemen), sesuai dengan nama penemunya.

Pada tugas akhir ini ini akan dibahas penerapan RSA pada protokol SSL *(Secure Socket Layer)* dalam autentikasi website. SSL merupakan protokol yang digunakan untuk browsing web secara aman. SSL memiliki banyak fitur yang digunakan pada setiap transaksi client-server.

Aplikasi ini menambah tingkat keamanan di sisi server dengan pertama-tama mengenkripsi *plaintext password* menggunakan RSA sebelum kemudian di konvesi menjadi bentuk *hash* MD5. Teknik ini mencegah para *hacker* mendapatkan *plaintext* dari password dengan menggunakan teknik *brute force* atau melihat table. Aplikasi ini dibangun dengan *JavaScript* pada sisi *client* dan PHP pada sisi *server.*

Kata kunci :*SSL, RSA, MD5, Autentikasi, Kriptografi*

ABSTRACT

In the Internet world there is no truly safe. There is always security flaws in any applications that are made. Attacks can be minimized by encrypting the data while transmitted. One popular cryptographic algorithms is RSA, named by its inventors, namely Rivest-Shamir-Addleman. The algorithm by its nature, is an asymmetric algorithm. It uses public key encryption.

In this final project will be discussed about implementation of RSA on (Secure Socket Layer) protocol in the website authentication. SSL is a protocol used for secure web browsing. It has many security features which are included in every client-server transaction.

This application increases security level on the server side by first encrypting plaintext used for password using RSA before it is converted into its MD5 hash. This technique prevents hackers to reveal the plaintext of the password by using brute force methods or table's look up. The application is developed using JavaScript in client side and PHP in server side.

Keywords: *SSL, RSA, MD5,Authentication, Cryptography*

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR ISTILAH

Nama Istilah	Definisi	Halaman pertama kali muncul
Enkripsi	proses mengamankan suatu informasi dengan membuat informasi tersebut tidak dapat dibaca tanpa bantuan pengetahuan khusus	vi
Algoritma	merupakan kumpulan perintah untuk menyelesaikan suatu masalah. Perintah-perintah ini dapat diterjemahkan secara bertahap dari awal hingga akhir	vi
Kriptografi	ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data	vi
Protocol	sebuah aturan atau standar yang mengatur atau mengijinkan terjadinya hubungan, komunikasi, dan perpindahan data antara dua atau lebih titik komputer	vi
Username	Identitas unik yang diberikan kepada user yang berhak mengakses suatu sistem	vi
Autentikasi	berhubungan dengan identifikasi/pengenalan, baik secara kesatuan sistem maupun informasi itu sendiri. Dua pihak yang saling berkomunikasi harus saling memperkenalkan diri. Informasi yang dikirimkan melalui kanal harus diautentikasi keaslian, isi datanya, waktu pengiriman, dan lain-lain	vi
Website	sebutan bagi sekelompok halaman web (*web page*), yang umumnya merupakan bagian dari suatu nama domain (*domain name*) atau subdomain di *World Wide Web* (WWW) di Internet	vi
Hacker	istilah teknologi informasi dalam bahasa Inggris yang mengacu kepada peretas yang secara etis menunjukkan suatu kelemahan dalam sebuah sistem komputer	vi
Brute force	sebuah teknik serangan terhadap sebuah sistem keamanan komputer yang menggunakan percobaan terhadap semua kunci yang mungkin	vi
Server	sebuah sistem komputer yang menyediakan jenis layanan tertentu dalam sebuah jaringan komputer	vi
Plaintext	teks informasi yang merupakan masukan bagi suatu algoritma enkripsi; sedangkan keluarannya disebut teks tersandi atau teks sandi (*ciphertext*)	vi

Hash	merupakan suatu metode yang secara langsung mengakses *record-record* dalam suatu tabel dengan melakukan transformasi aritmatik pada *key* yang menjadi alamat dalam tabel tersebut. *Key* merupakan suatu input dari pemakai di mana pada umumnya berupa nilai atau string karakter.	vi
Login	proses untuk mengakses komputer dengan memasukkan identitas dari akun pengguna dan kata sandi guna mendapatkan hak akses menggunakan sumber daya komputer tujuan.	1
Database	kumpulan informasi yang disimpan di dalam komputer secara sistematik sehingga dapat diperiksa menggunakan suatu program komputer untuk memperoleh informasi dari basis data tersebut	1
Password	Kode unik yang diinputkan user untuk masuk kedalam suatu sistem	1
Dekripsi	Proses mengembalikan dari chipertext menjadi plaintext	2
Internet	sistem global dari seluruh jaringan komputer yang saling terhubung menggunakan standar Internet Protocol Suite (TCP/IP) untuk melayani miliaran pengguna di seluruh dunia.	13
IP Address	deretan angka biner antar 32-bit sampai 128-bit yang dipakai sebagai alamat identifikasi untuk tiap komputer host dalam jaringan Internet.	32