

ABSTRAK

IMPLEMENTASI ENKRIPSI DAN DEKRIPSI DENGAN METODE RC4 UNTUK PENGAMANAN DATA SISTEM INFORMASI

Oleh

Uli Sholihah Saragih

Pada tahun 2015, Sistem Informasi Kegiatan Dosen (SIKSEN) Jurusan Ilmu Komputer Unila mengalami penyerangan data (*hack*) yang mengakibatkan data kegiatan dosen tidak dapat muncul di sistem informasi tersebut. Penyerangan data yang terjadi adalah salah satu akibat dari kurangnya keamanan data pada Sistem Informasi Jurusan Ilmu Komputer. Salah satu cara untuk mengamankan data adalah dengan menggunakan teknik kriptografi. Kriptografi merupakan cara yang dilakukan dengan menyandikan pesan asli menjadi pesan acak yang sulit dipahami. Didalam kriptografi terdapat dua proses utama yaitu enkripsi dan dekripsi. Enkripsi merupakan mengubah pesan asli menjadi pesan sandi, sedangkan dekripsi adalah proses pengembalian dari pesan sandi ke pesan aslinya. Metode yang dipakai adalah metode *Rivest Code 4* (RC4) karena metode ini merupakan salah satu metode yang hasil penyandian (*ciphertext*) memiliki ukuran panjang karakter yang sama dengan pesan aslinya (*plaintext*). Metode ini terdiri dari tiga tahap utama yaitu KSA (*Key Scheduling Algorithm*), PRGA (*Pseudo Random Generation Algorithm*) dan proses XOR. Data yang digunakan dalam penelitian ini adalah data mahasiswa Jurusan Ilmu Komputer Unila yang berjumlah 970 data mahasiswa yang terdiri dari 25 kolom data. Pengujian dilakukan dengan menguji apakah jumlah karakter pesan asli sama dengan pesan sandinya dan berapa banyak data yang berhasil dienkripsi dan didekripsi. Hasil pengujian didapatkan bahwa 970 data berhasil dienkripsi dan 970 data berhasil didekripsi dengan jumlah karakter yang sama antara pesan asli dan pesan sandi.

Keyword: RC4, Enkripsi, Dekripsi, Kriptografi, *Database*

ABSTRACT

IMPLEMENTASI ENKRIPSI DAN DEKRIPSI DENGAN METODE RC4 UNTUK PENGAMANAN DATA SISTEM INFORMASI

Oleh

Uli Sholihah Saragih

In 2015, Lecturer Activity Information System (SIKSEN) Department of Computer Science Unila experiencing data attacks (hack) which resulted in data lecturer activities can not appear in the information system. Attacking the data that occurred is one result of the lack of data security in Information Systems Computer Science Department. One way to secure data is to use cryptographic techniques. Cryptography is the way it does by encoding the original message into an elusive random message. In cryptography there are two main processes namely encryption and decryption. Encryption represents converting the original message into a password message, while decryption is the process of returning the password message to the original message. The method used is Rivest Code 4 (RC4) because this method is one of the methods that the encoding result (ciphertext) has the same character length as the original message (plaintext). This method consists of three main stages: KSA (Key Scheduling Algorithm), PRGA (Pseudo Random Generation Algorithm) and XOR process. The data used in this study is the data of Unila Computer Science students, amounting to 970 student data consisting of 25 columns of data. Testing is done by testing whether the number of original message characters is the same as the password and how much data is successfully encrypted and decrypted. The test results obtained that 970 data successfully encrypted and 970 data successfully decrypted with the same number of characters between the original message and password.

Keyword: RC4, Encryption, Decryption, Cryptography, Database