

SISTEM PENGKODEAN DATA PADA FILE TEKS PADA KEAMANAN INFORMASI DENGAN MENGGUNAKAN METODE SKIPJACK

Suprianto

STMIK Mardira Indonesia, Bandung 40235
supriaja@yahoo.com

Abstract

At this time the internet has become an important part of the IT world, with the number of Internet users began large corporations to private use this also makes the data traffic becomes very much. With the increasing number of traffic data is then began to appear are the people who want to know the data of others for the benefit of themselves, these people are called hacker. This can be prevented by encrypting a document or data to be transmitted so as to be read by unauthorized parties, there are several ways to encrypt the data, the authors chose the method of data encryption skipjack. This method is to encrypt a text file that is sourced from a network application examples Internet e - mail service and have 32 times the stage with the inclusion of the permutation formula and rule a, b rule that is part of the method, the method of data to be transmitted over the Internet is encrypted by sender. Then after I got to the receiver data is encrypted or decrypted the ciphertext back into plaintext data is original. Use of skipjack method with "Security Software Skipjack" made, the encryption and decryption process is proven to help maintain the validity of the information derived from the sender to the receiver.

Keywords: *Hacker, Skipjack Method, "Security Software Skipjack", Valid Information*

Abstrak

Pada saat ini internet telah menjadi bagian penting dalam dunia TI, dengan banyaknya pengguna internet dari mulai perusahaan besar hingga penggunaan pribadi hal ini juga membuat lalu lintas data menjadi sangat banyak. Dengan makin banyaknya lalu lintas data maka mulai bermunculan pula orang-orang yang ingin mengetahui data orang lain demi keuntungan diri sendiri, orang tersebut disebut *hacker*. Hal ini dapat dicegah dengan mengenkripsi dokumen atau data yang akan dikirimkan sehingga dapat dibaca oleh pihak yang tidak berkepentingan, ada beberapa cara untuk mengenkripsi data, penulis memilih enkripsi data dengan metode skipjack. Metode ini adalah mengenkripsi file text yang bersumber dari suatu aplikasi jaringan internet contoh e-mail service dan memiliki 32 kali tahapan dengan disertakannya rumus permutasi dan rule a, rule b yang merupakan bagian dari metode tersebut, dengan metode tersebut data yang akan dikirimkan melalui internet dienkripsi oleh *sender*. Kemudian setelah sampai kepada *receiver* data yang dienkripsi atau *ciphertext* didekripsi kan kembali menjadi data semula atau plaintext. Penggunaan metode skipjack dengan "Perangkat Lunak Keamanan *Skipjack*" yang dibuat, proses enkripsi dan dekripsi terbukti dapat membantu menjaga kevalidan informasi yang berasal dari *sender* ke *receive*.

Kata Kunci: *Hacker, Metode Skipjack, "Perangkat Lunak Keamanan Skipjack", Informasi Yang Valid*

DAFTAR PUSTAKA

- http://csrc.nist.gov/cryptoolkit/skipjack/penerbit_kota_tahun
<http://csrc.nist.gov/cryptoToolkit/skipjack/clarification.pdf>
- <http://www.austinlinks.com/crypto/skipjack.review.html>
- <http://www.faqs.org/rfcs/rfc2876.html>
- <http://www.kremlinencrypt.com/crypto/algorithms.html>
- <http://www.cs.technion.ac.il/~biham/Reports/SkipJack/>
- http://www.epic.org/crypto/clipper/skipjack_interim_review.html
- <http://www.mirror386.com/gnupg/contrib/do-not-use/skipjack.c>
- Pawling, J.(2000). Use of the KEA and SKIPJACK Algorithms in CMS rfc2876,
<http://www.ietf.org/rfc/>
- Jogiyanto, H.M, Analisis dan Desain, 1990.
- Pressman, Roger S.(1997). Rekayasa Perangkat Lunak, Andi Offset Yogyakarta.
- Yao Tung, Khoe. (1997), Teknologi Jaringan Intranet, Andi Offset Yogyakarta.
- W. Purbo, Onno (2000), TCP/IP Standar, Desain, dan Implementasi, PT. Gramedia, Jakarta.
- Subyantara, Didik (2004), Instalasi dan Konfigurasi Jaringan Microsoft Windows, PT. Elex Media Komputindo, Jakarta.