

Implementasi Algoritma Enkripsi *DES* Untuk Aplikasi *Mobile Chat* Pada OS Android

Zhomi Fero Anista
(07.04.111.00177)

Pembimbing 1 : Cucun Very Angkoso,S.T.,M.T
Pembimbing 2 : Ari Kusumaningsih,S.T.,M.T

ABSTRAK

Pengiriman informasi melalui jaringan elektronik dalam permasalahan ini adalah *chatting* dengan media *server* memiliki kerentanan dalam keamanan data yang dikirimkan . Layanan tersebut diketahui memiliki beberapa kelemahan, yaitu kelemahan terhadap masalah keamanan sistem. Kelemahan itu dikarenakan data yang dikirim kedalam *server* menggunakan koneksi dengan jaringan global sehingga lebih rentan terhadap serangan *hacker*.

Pada penelitian ini untuk menjamin keamanan dan kerahasiaan informasi pada komunikasi yang menggunakan jaringan *IP mobile*, dilakukan proses enkripsi dan dekripsi terhadap informasi yang akan dikirimkan. Enkripsi dilakukan pada saat pengiriman dengan cara mengkonversi informasi asli menjadi informasi yang terenkripsi sedangkan dekripsi dilakukan pada saat penerimaan dengan cara mengkonversi informasi terenkripsi menjadi informasi asli. Jadi informasi yang dikirimkan selama proses pengiriman adalah data informasi yang terenkripsi, sehingga informasi asli tidak dapat diketahui oleh pihak yang tidak berhak. Informasi asli hanya dapat diketahui oleh penerima dengan menggunakan kunci rahasia.

Penggunaan algoritma enkripsi *Data Encryption Standard (DES)* merupakan upaya untuk mencegah kebocoran data *chat* ke pihak lain. Sehingga dalam menggunakan aplikasi *chat* tidak dikhawatirkan terjadinya kebocoran informasi pribadi. Karena berdasarkan hasil uji coba terbukti bahwa cipherteks yang dihasilkan telah sesuai dengan hasil perhitungan menggunakan algoritma enkripsi *DES* dan telah diuji menggunakan beberapa aplikasi *DES test vector*.

Kata kunci: *Data Encryption Standard, Client-Server, chat*

ABSTRACT

Transmission of information through electronic networks in meaning of chat with the server media has vulnerability security of the data being transmitted. These services are known has several drawbacks and the weakness of the security system issues. Because the data is sent into the server using a global network has vulnerable to hacker's attacks. to ensure the security and confidentiality of information on communication using mobile IP networks, We are using encryption for the information being transmitted. The Encryption is performed at the time of Transmission by converting the original information into encrypted information. decryption is done by the time when reconvertng the encrypted information being original information. So the information is encrypted during the process of sending the data, so that the original information cannot be known by unauthorized parties. Original information can only be known by the receiver using a secret key. Using Data Encryption Standard (DES) algorithm is an attempt to prevent data leakage from chat to the other party. So when using this chat application we no need to worry about the leakage of chat information. Because based on the test results, proved that the output of the cyphertext is match with the results of the DES encryption algorithm manual calculations. And has been tested using several DES test vectors applications.

Keywords: *Data Encryption Standard, Client-Server, chat*