

# **APLIKASI CHATTING MENGGUNAKAN ALGORITMA KRIPTOGRAFI WAKE UNTUK CLIENT-SERVER**

**Syamsul Amin**

## **Abstrak**

Teknologi jaringan komputer membuat orang lebih mudah dan cepat untuk mendapat informasi. Aplikasi *Chatting* merupakan salah satu media yang digunakan untuk saling berbagi informasi. Adanya sistem enkripsi pada aplikasi *chatting* dapat membantu user dalam merahasiakan pesan. Solusi tersebut kita perlukan ilmu kriptografi. Dalam suatu jaringan komputer mudah saja terperangkap data penting diambil orang yang akan berbuat jahat maka informasi data harus di enkripsi. Dengan demikian pesan yang disampaikan akan sulit untuk dipecahkan *attacker*. Maka didapat suatu alternatif untuk menyelesaikan masalah ini yaitu membuat aplikasi *secure chat* menggunakan algoritma WAKE (*Word Auto Key Encryption*). Metode WAKE merupakan salah satu algoritma *stream cipher* yang digunakan secara komersial. Tujuannya untuk mendesain sistem enkripsi yang berkeamanan tinggi. Dengan demikian pesan yang dikirim berupa *ciphertext* kemampuan untuk mengamankan pesan informasi sangat rahasia. Pengiriman kunci dan ronde diperlukan jalur data yang aman berupa VPN (*Virtual Private Network*). Hasil dari uji pengujian keamanan aplikasi menunjukkan bahwa percakapan *chat* yang sudah diamankan dengan algoritma WAKE tidak dapat terbaca sehingga memberikan keamanan lebih.

**Kata Kunci:** Aplikasi *chatting*, *Client-Server*, Protokol, Algoritma WAKE

# **APPLICATIONS CHATTING USING A CRYPTOGRAPHIC ALGORITHM WAKE FOR CLIENT-SERVER**

**Syamsul Amin**

## **Abstract**

Computer network technology make people easier and faster to obtain information. Applications Chat is one of the media that is used to share information. The existence of the stem encryption on application chat can help the user in the secret message. The solution we need the science of Cryptography. In a computer network simply trapped data pentingdiambil people will do evil then the information must be in data encryption. The message thus delivered will be difficult to solve attacker. Then obtained an alternative to solve the problem is to make the application secure chat using WAKE algorithm (Word Auto Key Encryption). Method of WAKE algorithm is one stream cipher that is used commercially. His goal was to design a high secure encryption system. Thus messages sent in the form of ciphertext capability to secure the message information is very confidential. Key shipping and round needed a secure data path in the form of a VPN (Virtual Private Network). The result of the test application security testing showed that the chat conversation that is already secured with WAKE algorithm can not be read so as to provide more security.

**Keyword:** Applications chatting, Client-Server, Protocol, Algorithm WAKE