

ABSTRAK

Penyandian sebuah informasi merupakan suatu hal yang harus diperhatikan. Masalah tersebut penting karena jika sebuah informasi dapat di akses oleh orang yang tidak berhak atau tidak bertanggung jawab, maka keakuratan informasi tersebut akan diragukan, bahkan akan menjadi sebuah informasi yang menyesatkan. Chatting adalah suatu program yang melibatkan koneksi internet untuk saling bertukar pesan antar satu orang dengan orang lain. Chatting adalah bentuk komunikasi yang paling efektif dan efisien sata ini. Kriptografi hadir untuk meningkatkan aspek penyandian pesan. Hal ini dilakukan dengan menyandikan pesan ke dalam bentuk yang tidak dapat dimengerti lagi maknanya. Merkle Hellman digunakan subset masalah untuk membuat Cryptosystem untuk mengenkripsi pesan, Superincreasing S ransel vektor diciptakan dan Properti superincreasing tersembunyi dengan membuat kedua vektor M oleh perkalian Modular dan permutasi, Vektor M adalah kunci umum cryptosystem dan S digunakan untuk mendekripsi pesan. Kelebihan algoritma ini adalah proses pendistribusian kunci pada media yang tidak aman seperti internet, tidak memerlukan kerahasiaan.

Kata Kunci : *Aplikasi Chatting, Penyandian, Algoritma Merkle Hellman.*

ABSTRACT

Encoding an information is something that must be considered. This problem is important because if an information can be accessed by people who are not entitled or not responsible, then the accuracy of the information will be doubted, even it will be a misleading information. Chatting is a program that involves an internet connection to exchange messages between one person with another person. Chatting is the most effective and efficient form of communication. Cryptography exists to improve aspects of message encoding. This is done by encoding the message into a form that cannot be understood anymore. Merkle Hellman used a subset of problems to create a Cryptosystem to encrypt messages, Superincreasing S vector backpacks were created and the hidden superincreasing property by creating both M vectors by Modular multiplication and permutation, Vector M is the cryptosystem's public key and S is used to decrypt messages. The advantage of this algorithm is that the process of distributing keys to insecure media such as the internet does not require confidentiality.

Keywords: *Chatting Application, Encoding, Merkle Hellman Algorithm.*