IMPLEMENTASI ALGORITMA CAMELLIA DENGAN KUNCI 128 BIT PADA ENKRIPSI DAN DEKRIPSI ISI PESAN *ELECTRONIC MAIL* (EMAIL)

ABSTRAK

Keamanan data dan informasi menjadi sesuatu yang sangat beharga di era globalisasi sekarang ini. Data dan informasi dapat dikirim dari *sender* ke *receiver* melalui media-media yang sangat praktis, instan, gratis, dan mudah didapatkan. Salah satu media yang bisa digunakan adalah email (*electronic mail*). Email merupakan layanan surat elektronik yang memudahkan pengguna untuk saling bertukar data dan informasi. Namun, pencurian data dan informasi makin marak terjadi belakangan ini. sehingga membuat pengguna khawatir akan kerahasian data dan informasi yang dimiliki. Pencurian data dan infrormasi yang sering terjadi dikarenakan banyak akun email yang digunakan untuk mendaftar diberbagai situs lainnya dengan menggunakan *password* yang sama. Ketika data akun email kita didapat dari pihak ketiga sehingga memudahakan para pencuri untuk beraksi. Oleh karena itu, diperlukan algoritma untuk mengamankan data dan informasi yang kita kirim melalui email. Salah satu algoritma yang bisa digunakan adalah algoritma camellia 128 bit. Alasan utama penggunaan algoritma ini, berdasarkan penelitian sebelumnya disimpulkan bahwa algoritma ini tahan terhadap cryptanalys terutama *differential attack*. Selain itu, algoritma ini juga memiliki keunggulan *high level of security, efficeincy on multiple platforms, future developments*. Hasil dari penelitian ini, menyimpulkan bahwa algoritma ini bisa diimpelementasi pada pesan email. Implementasi dilakukan saat penulisan email dengan mengubah isi pesan email yang akan dikirim menjadi chiperteks dalam bentuk blok-blok biner. Sedangkan implementasi dari dekripsi dengan menggunakan metode ini akan merubah chiperteks yang diterima dalam bentuk blok-blok biner menjadi plainteks dalam bentuk pesan email sebenarnya. Selain itu algoritma ini juga sangat memiliki performa yang baik dari segi waktu proses dan kecepatan enkripsi dan dekripsinya. Pada penelitian ini waktu proses enkripsi dan dekripsi sangat dipengaruhi oleh padding bit. Padding bit dilakukkan pada proses enrkipsi dimana blok plainteks kurang dari kelipatan 128 bit. Sedangkan pada proses dekripsi tidak dilakukan padding bit, hal ini dikarenakan chiperteks yang dihasilkan pada penelitian ini telah berupa blok-blok kelipatan 128 bit.

Kata kunci: *email, enkripsi, dekripsi, key, camellia 128 bit, padding bit.*

IMPLEMENTATION OF CAMELLIA ALGORITHM WITH KEY 128 BIT IN ENCRYPTION AND DECRYPTION ELCECTRONIC MAIL (EMAIL) MESSAGE

ABSTRACT

Data security and information can be one of the most valuable thing in this era. Data and information can be sent from the sender to receiver using some practical,instant, free, and available medias. One of the medias that can be used is email (electronic mail). Email is an electronic mail that can help user exchange data and information to each other. However, data and information theft is a growing phenomenon recently. It makes the user so worry over the data privacy and information loss. Data theft mostly happen because of there are many sites registered using the same email with the same password. So, when someone steal the email acount, it can be easier for him to do anything.therefore, the algoritm for securing data and informtion sent by email is necessarily needed. One of the algortm used is camelia 128 bit algorithm. The main reason why the researcher uses this algorithm is because it can bare the criptanalys attack especially differential attack. Beside that, this algorithm has a high level of scurity, efficiency on multiple platforms, future devolopments. The results of the research, it concluded that these algorithms can be diimpelementasi email messages. Implementation is done when writing emails by changing the contents of the email that will be sent as chiperteks in the form of blocks of binary . While the implementation of dekrispi using this method will change chiperteks received in the form of blocks of binary becomes planteks in the form of the actual email message . Besides this algorithm also has a very good performance in terms of processing time and speed of encryption and decryption . In this research, encryption and decryption process is strongly influenced by the padding bits. Padding bits on encryption process in which a block of plaintext is less than a multiple of 128 bits . While in the decryption process is not use padding bits, because chiperteks generated in this study was in the form on blocks multiple of 128 bits.

Keyword: *email, encryptioni, decryption, key, camellia 128 bi, padding bit..*