ABSTRAK

Kriptografi adalah teknik pengamanan informasi yang dilakukan dengan cara mengubah pesan menggunakan suatu metode enkripsi sehingga tidak dapat dibaca secara langsung oleh pihak yang tidak berhak. *Block cipher* merupakan salah satu algoritma kriptografi yang menggunakan kumpulan bit dengan panjang tetap untuk mengenkripsi pesan. Metode enkripsi kriptografi *block cipher* pada dasarnya dilakukan dengan cara melakukan pertukaran kode bit pesan sehingga membentuk suatu pesan baru yang tidak dapat dibaca (*ciphertext*). Penelitian dilakukan dengan tujuan merancang kriptografi *block cipher* baru yang merepresentasikan ciri khas pola peta administrasi kalimantan barat dalam pertukaran kode bitnya. Perancangan kriptografi dilakukan dengan mengacu kepada algoritma kriptografi *block cipher Advance Encryption Standard (AES)* yang ditetapkan oleh *National Institute of Standard and Technology (NIST)* sebagai standar pengamanan informasi di dunia. Algoritma kriptografi yang dirancang juga menggunakan substitusi box (S-Box) dinamis yang dibangkitkan dengan kunci sehingga berbeda dengan S-box statis *AES*. Pengujian terhadap performa algoritma kriptografi menunjukkan hasil yang baik. Hasil pengujian *avalance effect* mendapatkan nilai rata-rata 50,524%. Simulasi waktu enkripsi per 500 blok data rata-rata membutuhkan waktu 3,514 detik. Analisa serangan *brute force* menunjukkan waktu yang diperlukan untuk melakukan *exhaustive search* memerlukan $1{,}341\ x\ 10^{152}$ detik atau setara $4{,}252\ x\ 10^{144}$ tahun. Algoritma kriptografi yang dihasilkan dapat bekerja dengan baik dalam 5 mode operasi block cipher yang direkomendasikan oleh *NIST* yaitu *Electronic Code Book (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB), Output Feedback (OFB),* dan *Counter (CTR)*. Penelitian juga mengimplementasikan algoritma kriptografi ke dalam sebuah aplikasi surat elektronik berbasis web.

Kata kunci: *block cipher*, kalimantan barat, *advance encryption standard*, s-box dinamis, aplikasi surat elektronik

ABSTRACT

Cryptography is a way of securing information by changing messages using an encryption method so that unauthorized parties cannot read them directly. Block cipher is a cryptographic algorithm that uses a fixed length set of bits to encrypt messages. The method of block cipher cryptographic encryption is basically done by converting the message bit code so that it forms a new message that cannot be read called ciphertext. This research was conducted with the aim of designing a new block cipher cryptography that represents the characteristics of the West Kalimantan administrative map pattern in exchanging its bit code. The design of cryptography is carried out by referring to the block cipher cryptographic algorithm Advance Encryption Standard (AES) set by the National Institute of Standards and Technology (NIST) as the standard for information security in the world. The designed cryptographic algorithm also uses a dynamic substitution box (S-Box) which is designed with a key so that it is different from the static AES S-box. The test performance of cryptographic algorithms shows good results. Avalance effect test results get an average value of 50.524%. Encryption simulation time per 500 data blocks on average takes 3.514 seconds. Brute force attack analysis shows that the time needed to perform exhaustive search requires $1.341\ x\ 10^{152}$ seconds or the equivalent of $4.252\ x\ 10^{144}$ years. The designed cryptographic algorithm can work well in the 5 block cipher operating modes recommended by NIST, namely Electronic Code Book (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB), Output Feedback (OFB), and Counter (CTR). This research also implements designed cryptographic algorithms into a electronic mail web-based application.

Keywords : block cipher, west kalimantan, advance encryption standard, dynamic s-box, electronic mail application