MODIFIKASI ALGORITMA BLOCK CIPHER DENGAN PENGELOMPOKAN PLAINTEKS MENGGUNAKAN *K-MEANS CLUSTERING*

Nova Yastika Putri (14117073)

Pembimbing Utama : Angga Wijaya, S.Si., M.Si.

ABSTRAK

Seiring perkembangan teknologi sangat mudah jika ingin bertukar informasi. Namun, dengan kemudahan yang dirasakan, tentunya memiliki resiko yaitu berupa keamanan pesan yang belum tentu terjaga. Salah satu yang sering terjadi adalah pencurian informasi, sehingga teknik untuk mengamankan informasi juga perlu ditingkatkan salah satunya dengan kriptografi.

Terdapat dua jenis kriptografi, yaitu kriptografi klasik dan kriptografi modern. Algoritma *block cipher* merupakan metode kriptografi modern yang tidak terlalu rumit. Karena itu, dirasa perlu untuk dilakukan modifikasi pada algoritma ini dengan tujuan untuk menghasilkan kunci yang lebih beragam, dan menjadikan algoritma dengan kunci yang sulit untuk diterka.

Pada penelitian ini akan dilakukan modifikasi yang menggunakan konsep dasar dari algoritma *block cipher*, yang mana setelah *plaintext* dikonversi menjadi biner (0 atau 1) maka bit-bit tersebut akan dipartisi sesuai ukuran yang diinginkan. Bit *plaintext* yang telah dipartisi akan dikelompokkan menggunakan *K-means Clustering.* Setelah *plaintext* dikelompokan, maka akan dibangun sebuah kunci random yang mana akan berbeda untuk setiap anggota dalam satu cluster dan akan sama jika berbeda *cluster*.

Hasil dari penelitian ini *plaintext* berhasil dienkripsi menjadi *ciphertext* dan pada pengujian *recovery ciphertext* terbukti dapat didekripsi kembali menjadi pesan awal atau *plaintext.* Pada pengujian analisis frekuensi didapat nilai variansi untuk *plaintext* sebesar 1230.7231822696233 dan nilai variansi untuk *ciphertext* sebesar 4329.023153795 dengan pengelompokan *plaintext* ke dalam 30 *cluster*

serta nilai variansi untuk *ciphertext* sebesar 4487.07153121513 dengan pengelompokan *plaintext* ke dalam 120 *cluster*. Dari hasil pengelompokan yang dilakukan pada pengujian analisis frekuensi, dilakukan perhitungan *silhouette coefisien* terhadap hasil pengelompokan dengan menggunakan 30 *cluster* dan 120 *cluster*. Hasilnya, nilai *silhouette coefisien* dari pengelompokan 120 *cluster* jauh lebih baik yaitu sebesar 0.7511408435874822 dengan kategori *strong structure*, dibandingkan nilai *silhouette coefisien* dari pengelompokan 30 *cluster* hanya bernilai sebesar 0.37023451881692465 dengan kategori *weak structure*.

Selain pengujian di atas, dilakukan pula pengujian perbandingan algoritma antara algoritma *block cipher* modifikasi dengan algoritma *block cipher* sederhana yang dilakukan dengan pengecekan pola kunci, hasil menunjukan bahwa kunci yang dihasilkan dari Modifikasi Algoritma *Block Cipher* dengan Pengelompokan *Plaintext* Menggunakan *K-Means Clustering* terbukti lebih beragam dibandingkan Algoritma *Block Cipher* sederhana.

Kata kunci : Keamanan informasi, Kriptografi, Enkripsi, Dekripsi, *Block Cipher*.

MODIFICATION OF BLOCK CIPHER ALGORITHMS

WITH PLAINTEKS GROUPING USING K-MEANS CLUSTERING

Nova Yastika Putri (14117073)

Pembimbing Utama : Angga Wijaya, S.Si., M.Si.

ABSTRACT

Along with the development of technology is very easy if you want to exchange information. However, with the ease felt, of course, has the risk of security messages that are not necessarily maintained. One that often occurs is the theft of information, so the technique to secure information also needs to be improved one of them with cryptography.

There are two types of cryptography: classical cryptography and modern cryptography. Block cipher algorithms are a modern cryptographic method that is not too complicated. Therefore, it is necessary to make modifications to this algorithm with the aim to produce a more diverse key, and make the algorithm with a key that is difficult to guess.

In this research will be made modifications that use the basic concept of the block cipher algorithm, which after plaintext is converted into binary (0 or 1) then the bits will be partitioned according to the desired size. The plaintext bits that have been partitioned will be grouped using K-means Clustering. After the plaintext is grouped, it will be built a random key which will be different for each member in one cluster and will be the same if different clusters.

The results of this study plaintext successfully encrypted into ciphertext and on recovery test ciphertext proved to be decryptable back into the initial message or plaintext. In the frequency analysis test obtained a variance value for plaintext of 1230.7231822696233 and a variance value for ciphertext of 4329.023153795 with the grouping of plaintext into 30 clusters as well as the variance value for ciphertext of 4487.07153121513 with the grouping of plaintext into 120 clusters.

From the results of grouping conducted in frequency analysis testing, the calculation of silhouette coefficiencies was carried out on the results of grouping using 30 clusters and 120 clusters. As a result, the silhouette coefficiency value of the grouping of 120 clusters is much better at 0.7511408435874822 with the strong structure category, compared to the silhouette coefficiency value of the grouping of 30 clusters is only worth 0.37023451881692465 with the weak structure category.

In addition to the above tests, algorithm comparison tests were also conducted between modified block cipher algorithms and simple block cipher algorithms conducted by checking key patterns, the results showed that the key resulting from the Block Cipher Algorithm Modification with Plaintext Grouping Using K-Means Clustering proved to be more diverse than the simple Block Cipher Algorithm.

***Keywords** : Information security, Cryptography, Encryption, Decryption, Block Cipher.*