BAB I

PENDAHULUAN

1.1 Latar Belakang

Seiring perkembangan teknologi sangat mudah jika ingin bertukar informasi, telah banyak media yang dapat digunakan untuk melakukan hal tersebut. Namun dengan kemudahan yang dirasakan, tentunya memiliki resiko yaitu berupa keamanan pesan yang belum tentu terjaga, karena semakin berkembangnya teknologi sudah tentu semakin banyak pula teknik untuk melakukan pencurian informasi yang berakibat informasi tersebut sampai kepada pihak yang tidak berkepentingan [1],[2]. Sehingga teknik untuk mengamankan informasi juga perlu ditingkatkan salah satunya dengan kriptografi yang mana merupakan algoritma pengkodean untuk menjamin kerahasiaan dan pengubahan informasi yang dilakukan secara ilegal untuk disalahgunakan oleh pihak tertentu yang tentunya dapat merugikan [4],[11].

Dalam kriptografi terdapat dua proses untuk menjamin kerahasiaan pesan, yaitu enkripsi dan dekripsi. Enkripsi adalah proses untuk mengubah *plaintext* (pesan awal) menjadi *ciphertext* (pesan setelah dikodekan), sedangkan Dekripsi adalah proses untuk mengubah *ciphertex*t menjadi *plaintext* [3],[14]. Dengan dilakukan nya proses tersebut maka pesan akan berubah dari pesan terbuka menjadi pesan rahasia, pesan ini akan dapat dimengerti kembali atau terbuka jika kunci enkripsi diketahui [4],[5].

Kriptografi sendiri terdiri dari dua jenis, yaitu kriptografi klasik dan kriptografi modern. Kedua nya memiliki fungsi yang sama yaitu untuk mengenkripsi dan mendekripsi pesan, untuk kriptografi modern beroperasi pada mode bit (0 atau 1). Algoritma *block cipher* merupakan salah satu metode kriptografi modern yang tidak terlalu rumit, karena kunci yang digunakan pada saat enkripsi dan dekripsi adalah kunci yang sama. Namun, algoritma ini tetap dinilai cukup baik dalam mengkodekan pesan dan cukup sulit untuk diterka oleh beberapa orang [3]. Algoritma ini memproses pesan atau *plaintext* berupa bit yang dalam proses enkripsi dan

dekripsi nya akan di XOR kan dengan kunci, pada algoritma *block cipher* panjang kunci akan sama dengan panjang blok pesan, dan kunci merupakan bilangan acak [5],[6].

Pada penelitian ini akan dilakukan modifikasi pada algoritma *block cipher*. Modifikasi yang akan dilakukan adalah setelah *plaintext* di konversi menjadi biner (0 atau 1) maka bit-bit tersebut akan di partisi sesuai ukuran yang diinginkan hal ini diambil dari konsep dasar *block cipher* [1],[3]. Bit *plaintext* yang telah dipartisi akan dikelompokkan menggunakan *K-means Clustering*. *K-means Clustering* adalah sebuah metode pengelompokan data menjadi beberapa *cluster*, yang mana data dikelompokan berdasarkan hasil operasi *Euclidean Distance* yang merupakan perhitungan jarak dari dua buah titik (variabel x dan y) [8]. Pada penelitian ini jarak *Euclidean Distance* dihitung berdasarkan frekuensi biner 1 untuk variabel x, dan nilai perubahan setiap biner dari *plaintext* untuk variabel y. Setelah *plaintext* dikelompokan, maka akan di bangun sebuah kunci *random* yang mana akan berbeda untuk setiap anggota dalam satu *cluster* dan akan sama jika berbeda *cluster*. Ini berfungsi untuk menghilangkan hubungan atau kemiripan hasil *ciphertext* dari *plaintext* yang terdapat di dalam satu *cluster*, sehingga dapat meningkatkan keamanan informasi, karena semakin acak *keystream* yang dihasilkan maka akan semakin sulit informasi tersebut untuk dipecahkan [6]. Setelah itu, kunci akan dibangkitkan sepanjang blok *plaintext*, yang mana ini merupakan konsep dasar dari *block cipher.*

1.2 Rumusan Masalah

Berdasarkan latar belakang penelitian, terdapat beberapa rumusan masalah, yaitu :

1. Apakah *plaintext* yang memiliki kemiripan dapat dikelompokan?
2. Apakah modifikasi algoritma ini dapat menghasilkan kunci yang lebih beragam sehingga mengurangi hubungan antar *ciphertext* yang *plaintext*nya memiliki kemiripan?
3. Apakah terdapat karakter tertentu yang mendominasi *ciphertext*?

1.3 Tujuan Penelitian

Tujuan yang ingin dicapai dari penelitian ini adalah

1. Melakukan modifikasi pada Algoritma *Block Cipher* dengan mengelompokan *plaintext* menggunakan *K-Means Clustering.*
2. Menghasilkan kunci yang lebih beragam berdasarkan hasil *clustering* sehingga mengurangi hubungan antar *ciphertext* yang *plaintext* nya memiliki kemiripan.
3. Melakukan analisis frekuensi untuk menentukan karakter yang mendominasi *ciphertext* dan memiliki hubungan dengan karakter yang juga mendominasi *plaintext.*

1.4 BatasanMasalah

Batasan masalah dari penelitian ini adalah

1. Kode ASCII yang tidak dapat dicetak akan dituliskan dalam bentuk desimal dan dengan awalan dan akhiran berupa spasi. Contohnya karakter *null* ditulis menjadi*spasi*0*spasi*
2. Karakter spasi akan ditulis seperti karakter yang tidak bisa dicetak, yaitu menjadi*spasi*32*spasi*

1.5 Manfaat Penelitian

Manfaat dari penelitian ini adalah

1. Meningkatkan keamanan enkripsi pesan dengan kunci yang lebih beragam.
2. Mengurangi hubungan antar *ciphertext* yang *plaintext* nya memiliki kemiripan.

1.6 SistematikaPenulisan

Sistematika penulisan yang digunakan pada penelitian ini adalah

1. Bab I Pendahuluan

   Bab ini menjelaskan tentang latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, dan

sistematika penulisan.

2. Bab II Tinjauan Pustaka dan Landasan Teori

   Bab ini menjelaskan tentang tinjauan pustaka dan landasan teori yang menjadi acuan dalam penelitian ini.

3. Bab III Metodologi Penelitian

   Bab ini berisikan tentang analisis permasalahan dan rancangan yang akan dilakukan dalam penelitian ini,yaitu rancangan algoritma, rancangan implementasi, dan rancangan pengujian.

4. Bab IV Hasil dan Pembahasan

   Bab ini menjelaskan proses implementasi dan pengujian terhadap hasil yang telah didapat.

5. Bab V Kesimpulan dan Saran

   Bab ini berisi kesimpulan penelitian yang telah dicapai dan saran terhadap penelitian lanjutan yang mungkin akan dilakukan.