BAB I
PENDAHULUAN

1.1 Latar Belakang

Pada era teknologi seperti sekarang ini, pertukaran informasi melalui internet sudah menjadi hal yang biasa dilakukan. Hal tersebut menjadikan keamanan informasi sebagai hal yang sangat penting karena dalam proses pengiriman data seringkali terjadi penyadapan atau pencurian informasi oleh pihak yang tidak berhak. Oleh karena itu, dalam proses pengiriman atau penerimaan informasi dibutuhkan suatu sistem keamanan yang dapat menjaga kerahasiaan pesan atau informasi agar tidak disalahgunakan oleh pihak lain. Salah satu cara pengamanan tersebut adalah dengan menerapkan kriptografi.

Kriptografi adalah ilmu dan seni yang digunakan untuk menjaga keamanan pesan. Dalam penerapannya pesan yang dikirim diubah kedalam bentuk sandi, sandi tersebut hanya bisa dibaca atau dikembalikan dengan kunci (*key*) tertentu. Kunci tersebut hanya diketahui oleh orang yang berhak atas pesan tersebut [1].

Algoritma kriptografi merupakan langkah-Iangkah logis dalam menyembunyikan pesan dari orang-orang yang tidak berhak atas pesan tersebut. Dalam algoritma kriptografi ada beberapa istilah atau terminologi yang perlu diketahui yaitu *plaintext, ciphertext*, enkripsi dan dekripsi. *Plaintext* (pesan) merupakan data atau informasi asli biasanya berupa pesan teks yang mudah dipahami. *Ciphertext* merupakan pesan yang sudah disandikan dan tidak dapat dimengerti agar isi pesan tidak dapat dipahami oleh pihak yang tidak berkepentingan. Enkripsi merupakan proses penyandian pesan dari *plaintext* ke *ciphertext*, sedangkan dekripsi merupakan proses pengembalian pesan dari *ciphertext* ke *plaintext* [2].

Secara umum, model yang digunakan dalam kriptografi klasik dikelompokkan menjadi dua yaitu substitusi dan transposisi [3]. Algoritma dalam kriptografi yang termasuk dalam kriptografi klasik model subtitusi salah satunya adalah algoritma *Playfair Cipher*. *Playfair Cipher* merupakan salah satu algoritma kriptografi

klasik yang termasuk ke dalam *polygram cipher*. *Polygram cipher* adalah cipher substitusi yang menggunakan beberapa huruf dalam proses penyandiannya. Poligram dengan dua huruf disebut bigram, tiga huruf disebut trigram dan seterusnya [4]. Dalam algoritma *Playfair Cipher*, *plaintext* diubah menjadi bentuk pasangan huruf / bigram. Proses enkripsi dan dekripsi dilakukan pada bigram tersebut. Kunci yang digunakan adalah 25 huruf (semua huruf abjad kecuali huruf J) yang disusun di dalam bujursangkar berukuran 5×5. Kemungkinan kunci *Playfair Cipher* adalah sebanyak 25! [5].

Pada penelitian ini, digunakan string biner yang disusun dalam blok berbentuk bujur sangkar. String biner tersebut merepresentasikan bilangan dari 0 sampai $x^2 - 1$, dimana x adalah bilangan bulat yang menyatakan panjang sisi bujur sangkar tersebut. Penyusunan string biner disusun secara acak sehingga susunan tersebut merupakan permutasi string biner sebanyak $x^2 - 1$ atau sebanyak jumlah blok dalam bujur sangkar. Isi dari setiap blok berupa string biner yang panjangnya sebanyak n. Setiap bit string biner memiliki 2 kemungkinan yaitu 0 atau 1 sehingga banyaknya kemungkinan string dalam blok adalah 2^n. Akibatnya diperoleh persamaan sebagai berikut :

$$2^n = x^2$$

Dengan

n = bilangan bulat yang menyatakan panjang string biner dari isi setiap blok

x = bilangan bulat yang menyatakan panjang sisi bujur sangkar

Berikut ini Tabel 1.1 yang merupakan tabel penentuan nilai persamaan n dan x yang bersesuaian

Tabel 1.1 Persamaan nilai x dan n

n	2^n	$2^n = x^2$	x	Keterangan
n = 1	$2^1 = 2$	$2 = x^2$	1.4142135624	Tidak ada x bilangan bulat yang memenuhi

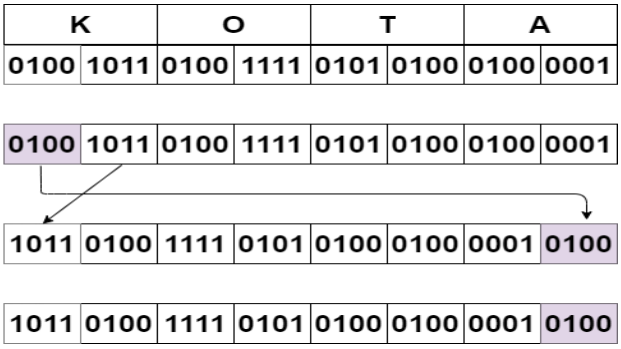
n	2^n	$2^n = x^2$	x	**Keterangan**
n = 2	$2^2 = 4$	$4 = x^2$	2	Nilai n dan x memenuhi persamaan
n = 3	$2^3 = 8$	$8 = x^2$	2,8284271247	Tidak ada x bilangan bulat yang memenuhi
n = 4	$2^4 = 16$	$16 = x^2$	4	Nilai n dan x memenuhi persamaan
n = 5	$2^5 = 32$	$32 = x^2$	5,6568542495	Tidak ada x bilangan bulat yang memenuhi
n = 6	$2^6 = 64$	$64 = x^2$	8	Nilai n dan x memenuhi persamaan
n = 7	$2^7 = 128$	$128 = x^2$	11,313708499	Tidak ada x bilangan bulat yang memenuhi
n = 8	$2^8 = 256$	$256 = x^2$	16	Nilai n dan x memenuhi persamaan
n = 9	$2^9 = 512$	$512 = x^2$	22,627416998	Tidak ada x bilangan bulat yang memenuhi
n = 10	$2^{10} = 1024$	$1024 = x^2$	32	Nilai n dan x memenuhi persamaan

Jika menggunakan nilai n = 2 dan x = 2, maka kemungkinan kunci yang bisa digunakan hanya sebanyak $2^n! = 2^2! = 24$. Banyaknya kemungkinan kunci ini jumlahnya lebih sedikit daripada *Caesar Cipher* yang memiliki kemungkinan kunci sebanyak 26. Padahal *Caesar Cipher* merupakan algoritma kriptografi yang sederhana yang biasa digunakan sebagai contoh dasar algoritma kriptografi subtitusi.

Dalam penelitian ini dipilih $n = 4$ dan x = 4. Oleh karena itu, terdapat 16 blok dalam bujur sangkar dan isi setiap blok merupakan string biner yang merepresentasikan bilangan desimal dari 0 sampai 15.

Pesan teks akan direpresentasikan sebagai kode ASCII. Kode ASCII (*American Standard Code for Information Interchange*) merupakan suatu standar internasional dalam kode huruf dan simbol seperti *Hex* dan *Unicode* tetapi ASCII lebih bersifat *universal*. Jumlah kode ASCII adalah 255 kode. Untuk keperluan manipulasi kode ASCII dibagi menjadi dua, untuk manipulasi teks digunakan kode ASCII 0 sampai 127 dan untuk manipulasi grafik digunakan kode ASCII 128 sampai 255 [6].

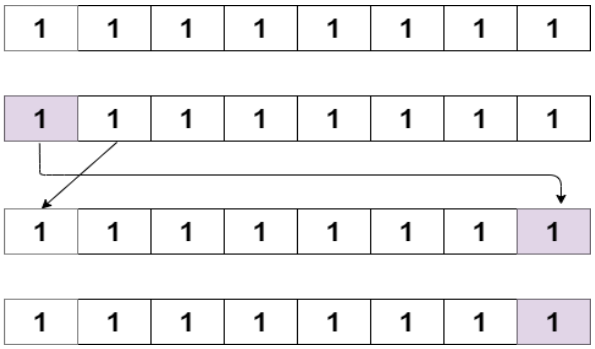
Jumlah bit biner dari setiap kode ASCII terdiri dari 8 bit. *Plaintext* diubah terlebih dahulu kedalam kode ASCII. Berikutnya kode ASCII diubah menjadi string biner. Lalu dipartisi menjadi dua bagian. Sehingga terdapat dua bagian yang masing-masing terdiri dari 4 bit. Pada string biner *plaintext* dilakukan pergeseran (*shift*) 4 bit ke kiri sehingga 4 bit paling kiri akan dipidahkan ke ujung paling kanan. Proses pergeseran (*shift*) diilustrasikan pada Gambar 1.1.



Gambar 1.1 *Shift* pada *plaintext*

Pergeseran (*shift*) tersebut bertujuan agar dua buah 4-bit-substring tidak dienkripsi ke dua buah 4-bit-substring yang sama. Pada 4-bit-substring *plaintext* yang berada di posisi genap, *shift* 1 bit paling kiri ke ujung kanan bagian dari substring tersebut. Hal tersebut bertujuan mengurangi kemungkinan adanya dua buah 4-bit-substring yang sama. Sehingga dihasilkan 8 bit string biner yang merupakan gabungan dari 4-bit-substring kedua huruf pertama dengan 4-bit-substring pertama huruf selanjutnya. Setiap 8 bit string biner tersebut akan dienkripsi dengan kunci yang sebelumnya sudah ditentukan. Pada proses enkripsi jika terdapat pasangan 4-bit-substring yang sama maka hasil enkripsinya tetap / tidak berubah.

Kemungkinan terdapat pasangan 4-bit-substring yang sama hanya sebanyak dua macam yaitu 0000 0000 dan 1111 1111 karena pada 4-bit-substring kedua dilakukan *shift* 1 bit paling kiri akan menghasilkan susunan string yang sama atau tidak berubah seperti pada Gambar 1.2.



Gambar 1.2 *Shift* pada string biner seragam

Setelah dilakukan enkripsi, 8 bit string biner tersebut di konversi kembali ke kode ASCII. Pesan yang sudah dienkripsi akan membuat analisis frekuensi menjadi sangat sulit karena kemunculan huruf-huruf dalam *ciphertext* menjadi lebih beragam sehingga menghasilkan hasil enkripsi yang unik dan lebih sulit diterjemahkan.

1.2 Rumusan Masalah

Berdasarkan latar belakang, rumusan masalah dapat dirumuskan sebagai berikut:

1. Bagaimana implementasi algoritma *Playfair Cipher* untuk enkripsi pesan teks ASCII - Biner?
2. Bagaimana hasil *ciphertext* yang dihasilkan dari algoritma *Playfair Cipher* dengan koversi ASCII – Biner?
3. Bagaimana pengujian hasil implementasi algoritma *Playfair Cipher* untuk enkripsi pesan teks ASCII – Biner?

1.3 Tujuan Penelitian

Tujuan penelitian adalah sebagai berikut :

1. Menerapkan konsep algoritma *Playfair Cipher* untuk enkripsi pesan teks ASCII – Biner.
2. Menghasilkan *ciphertext* yang lebih beragam yaitu berupa kode ASCII
3. Melakukan pengujian hasil implementasi algoritma *Playfair Cipher* untuk enkripsi pesan teks ASCII – Biner.

1.4 Batasan Masalah

Dalam penelitian ini terdapat batasan masalah sebagai berikut :

1. Kunci yang digunakan dalam algoritma *Playfair Cipher* pada penelitian ini berasal dari permutasi string biner yang merepresentasikan bilangan desimal dari 0 sampai 15.
2. Dalam penelitian ini dipilih $n = 4$ dan $x = 4$ yang memenuhi persamaan $2^n = x^2$.
3. Pada karakter ASCII yang memiliki blok *plaintext* dengan string biner 0000 0000 dan 1111 1111 hasil enkripsi akan tetap/tidak berubah.
4. Karakter ASCII yang tidak dapat dicetak akan ditampilkan dalam bentuk heksadesimal dari kode ASCII tersebut, dengan diberi awalan dan akhiran berupa spasi. Contoh : [spasi]0x1[spasi], [spasi]0xFF[spasi].
5. Karakter spasi akan ditampilkan seperti karakter yang tidak bisa dicetak. Contoh : [spasi]0x20[spasi].

1.5 Manfaat Penelitian

Manfaat yang diharapkan dari penelitian ini adalah sebagai berikut :

1. Meningkatkan keamanan enkripsi pesan pada algoritma *Playfair Cipher*.
2. Pesan asli atau *plaintext* dapat berisi karakter ASCII seperti angka, spasi dan karakter ASCII lainnya, sehingga huruf J tidak perlu dihilangkan seperti algoritma *Playfair Cipher* sebelumnya.