BAB II
TINJAUAN PUSTAKA DAN LANDASAN TEORI

2.1 Tinjauan Pustaka

Pada penelitian ini digunakan referensi sebagai pendukung dari penelitian yang akan dilakukan. Adapun beberapa penelitian terdahulu yang berkaitan dengan kriptografi *Playfair Cipher* sebagai berikut.

Penelitian pertama yaitu penelitian yang dilakukan oleh Sartika Dewi Br. Surbakti pada tahun 2017 yang berjudul "Implementasi Algoritma *Playfair Cipher* pada Penyandian Data". Dalam penelitian tersebut, dilakukan enkripsi dan dekripsi dengan *Playfair Cipher* biasa yaitu dengan kunci berukuran 25 karakter yang merupakan huruf alfabet kecuali huruf J yang disusun dalam bujur sangkar berukuran 5×5. Hasil yang diperoleh dari penelitian ini adalah algoritma *Playfair Cipher* hanya dapat menyandikan pesan *plaintext* yang berisi huruf alfabet saja dan untuk melakukan proses enkripsinya harus menghilangkan huruf J [7].

Penelitian kedua yaitu penelitian yang dilakukan oleh Rivalri Kristianto Hondro pada tahun 2020 dengan judul "Modifikasi *Platform* Kunci Algoritma *Playfair* Untuk Meningkatkan Nilai *Confusion* Pada *Ciphertext*". Dalam penelitian tersebut, dilakukan modifikasi pada tabel kunci yang digunakan untuk proses enkripsi dan dekripsi yaitu dengan menggunakan tabel bujur sangkar berukuran 8×8. Tabel kunci berisi karakter huruf alfabet, karakter angka dan penambahan karakter simbol. Hasil *ciphertext* lebih bervariasi tetapi proses enkripsi masih dilakukan per karakter [8].

Penelitian ketiga yaitu penelitian yang dilakukan oleh Ratna Wati Simbolon pada tahun 2016 dengan judul "Pengamanan Transkrip Nilai Mahasiswa menggunakan Kriptografi *Playfair Cipher* dan Steganografi dengan Teknik *Least Significant Bit* (LSB)". Dalam penelitian tersebut, dilakukan enkripsi dengan *Playfair Cipher* dengan kunci berjumlah 36 yang merupakan kombinasi alfabet sebanyak 26 huruf dan angka sebanyak 10 (rentang 0 sampai 9) yang disusun dalam matriks

berukuran 6 × 6. Pesan asli yaitu transkrip nilai mahasiswa dengan 8 karakter dari NPM mahasiswa, gabungan sesmester mata kuliah, kode mata kuliah, dan nilai. Setelah proses enkripsi, *ciphertext* yang dihasilkan di konversi ke dalam bentuk kode *American Standard Code for Information Interchange* (ASCII) yang terdiri dari 8 bit biner untuk dapat diimplementasikan ke wadah (*cover image*) yang digunakan dengan metode *The Least Significant Bit* (LSB). Penerapan kode ASCII membuat hasil enkripsi semakin sulit untuk dimengerti oleh pihak ketiga sebab frekuensi kemunculan huruf di dalam *ciphertext* menjadi datar. Tetapi proses enkripsi masih dilakukan per karakter [9].

Penelitian keempat yaitu penelitian yang dilakukan oleh Ahmad Tantoni dan Mohammad Taufan Asri Zaen pada tahun 2018 yang berjudul "Implementasi *Double Caesar Cipher* Menggunakan ASCII". Dalam penelitian tersebut, pesan di enkripsi dengan algoritma *Double Caesar Cipher* yaitu proses enkripsi dilakukan dua kali dengan dua kali menginputkan angka pergeseran menggunakan modulus 256 dan penggunaan tabel ASCII (*American Standard Code for Information Interchange*). Penelitian ini menghasilkan hasil *ciphertext* yang lebih banyak dibanding dengan hanya menggunakan huruf alfabet. Hal tersebut dikarenakan pada huruf alfabet digunakan mod 26 yang hanya akan memunculkan sebanyak 26 huruf alfabet sedangkan pada tabel ASCII digunakan mod 256 yang akan memunculkan sebanyak 256 karakter kombinasi antara huruf, angka ataupun simbol. Pesan *ciphertext* yang dihasilkan lebih rumit karena terdapat simbol-simbol dari kode ASCII yang sulit dipahami. Tetapi proses enkripsi masih dilakukan per karakter. [6]. Rangkuman dari penelitian terdahulu dapat dilihat pada Tabel 2.1.

Tabel 2.1 Tinjauan pustaka

No	Nama Peneliti	Judul	Metode	Hasil
1.	Sartika Dewi Br. Surbakti	Implementasi Algoritma Playfair Cipher pada	Menggunakan algoritma *Playfair Cipher* klasik yang biasa	Algoritma *Playfair Cipher* hanya dapat menyandikan pesan *plaintext* yang berisi

No	Nama Peneliti	Judul	Metode	Hasil
		Penyandian Data	dengan kunci berukuran 25 karakter alfabet selain huruf J.	huruf alfabet saja dan untuk melakukan proses enkripsinya harus menghilangkan huruf J.
2.	Rivalri Kristianto Hondro	Modifikasi *Platform* Kunci Algoritma *Playfair* Untuk Meningkatkan Nilai *Confusion* Pada *Ciphertext*	Algoritma *Playfair Cipher* dengan kunci berukuran 8×8. Tabel kunci berisi karakter huruf alfabet, karakter angka dan penambahan karakter simbol.	Hasil *ciphertext* lebih bervariasi tetapi proses enkripsi masih dilakukan per karakter.
3.	Ratna Wati Simbolon	Pengamanan Transkrip Nilai Mahasiswa menggunakan Kriptografi *Playfair Cipher* dan Steganografi dengan Teknik *Least Significant Bit* (LSB)	Menggunakan algoritma *Playfair Cipher* dengan tabel matriks 6x6 yang merupakan gabungan 26 huruf alfabet dan 10 angka (0 sampai 9). Saat penanaman bit dengan metode LSB *ciphertext* hasil enkripsi di konversi ke dalam	Penerapan kode ASCII membuat hasil enkripsi semakin sulit untuk dimengerti oleh pihak ketiga sebab frekuensi kemunculan huruf di dalam *ciphertext* menjadi datar. Tetapi proses enkripsi masih dilakukan per karakter.

No	Nama Peneliti	Judul	Metode	Hasil
			kode ASCII lalu ke dalam bentuk biner.	
4.	Ahmad Tantoni dan Mohammad Taufan Asri Zaen	Implementasi *Double Caesar Cipher* Menggunakan ASCII	Menggunakan algoritma *Double Caesar Cipher*, proses enkripsi dilakukan dua kali dengan dua kali menginputkan angka pergeseran, dengan modulus 256	Pesan *ciphertext* yang dihasilkan lebih rumit karena terdapat simbol-simbol dari kode ASCII yang sulit dipahami. Tetapi proses enkripsi masih dilakukan per karakter.

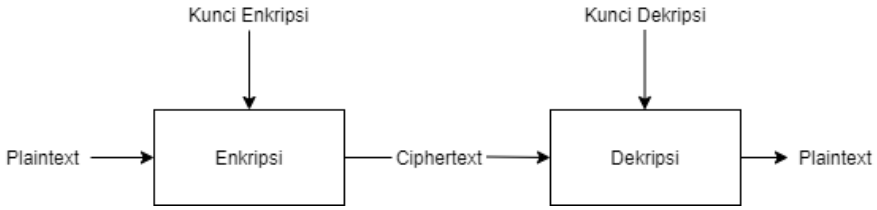
Pada penelitian ini, pesan asli akan terlebih dahulu diubah ke dalam bentuk ASCII. Selanjutnya nilai desimal per karakter diubah dalam bentuk biner yang panjanganya 8 bit yang akan dipartisi menjadi dua pasang 4-bit-substring. Lalu dilakukan enkripsi pada tiap partisi dengan *Playfair Cipher* dengan kunci angka biner 4 bit hasil permutasi angka 0 sampai 15 yang disusun dalam tabel kunci 4 × 4. Lalu tiap 4-bit-substring *ciphertext* disatukan kembali menjadi biner 8 bit dan nilai desimal dari 8 bit biner tersebut di konversi ke karakter ASCII.

2.2 Landasan Teori

2.2.1 Kriptografi

Kriptografi berasal dari dua kata dalam bahasa Yunani "*cryptos*" yang berarti rahasia dan "*gráphein*" yang berarti tulisan. Secara umum, kriptografi merupakan ilmu dan seni yang digunakan untuk menjaga kerahasiaan sebuah informasi [10].

Dalam kriptografi, pesan akan dikimkan dengan bentuk *ciphertext* atau pesan yang tidak dapat dipahami. Untuk mendapatkan *ciphertext*, dilakukan proses enkripsi pada pesan asli atau *plaintext* dan untuk mendapatkan *plaintext* kembali dilakukan proses dekripsi. Kedua proses tersebut menggunakan kunci yang hanya diketahui oleh pengirim dan penerima pesan tersebut. Ilustrasi kedua proses tersebut dapat dilihat pada Gambar 2.1.



Gambar 2.1 Proses enkripsi dan dekripsi

2.2.2 Kriptografi Klasik *Cipher* Subtitusi

Algoritma kriptografi klasik merupakan kriptografi yang pada proses enkripsi dan dekripsinya menggunakan kunci simetris, artinya kunci yang digunakan saat proses enkripsi dan dekripsi sama [3]. Contoh teknik dalam kriptografi klasik, yaitu substistusi dan transposisi. Teknik subsitusi dilakukan dengan cara mengganti satu atau sekumpulan huruf pada *plaintext* tanpa mengubah urutannya. Sedangkan teknik transposisi dilakukan dengan cara memindahkan posisi huruf atau blok *plaintext* berdasarkan aturan yang ditentukan [10].

Algoritma kriptografi yang termasuk dalam teknik substitusi adalah kriptografi *Caesar*. Algoritma *Caesar Cipher* menggunakan operasi modulus. Huruf-huruf diubah menjadi angka, A = 0, B = 1, sampai Z = 25 [6]. Kunci merupakan nilai pergeseran karater.

Secara matematis dituliskan dengan persamaan berikut :

$$\text{Enkripsi} \longrightarrow C = E(P) = (P + k)\ mod\ 26$$

$$\text{Deksripsi} \longrightarrow P = D(C) = (C - k)\ mod\ 26$$

Langkah dalam algoritma ini sebagai berikut :

1. Menentukan besar nilai pergeseran karakter *ciphertext* dari *plaintext*.
2. Menukar karakter pada *plaintext* menjadi *ciphertext* sesuai dengan pergeseran yang telah ditentukan.

Misal ditentukan nilai pergeseran = 3, maka dihasilkan substitusi huruf yaitu huruf A menjadi huruf D, huruf B menjadi huruf E, dan seterusnya. Hal tersebut digambarkan dalam Tabel 2.2.

Tabel 2.2 Substitusi huruf *Caesar Cipher*

Plaintext	A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Ciphertext	D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

Contoh penyandian pesan menggunakan Algoritma *Caesar Cipher* dengan nilai pergeseran = 3 sebagai berikut :

Plaintext : NAMA SAYA LATISYA

Ciphertext : QDPD VDBD ODWLVBD

2.2.3 Kriptografi Klasik Cipher Transposisi

Cipher Transposisi yaitu algoritma kriptografi yang dilakukan dengan cara memutasikan karakter-karakter *plaintext*, yaitu dengan mengubah susunan urutan karakter pesan. *Ciphertext* didapat dari susunan *plaintext* yang sudah diubah posisinya [11].

Berikut merupakan salah satu contoh proses algoritma *Cipher* Transposisi.

Plaintext : NAMA SAYA LATISYA

Dipilih kunci sebesar 5 sehingga *plaintext* akan disusun kedalam kolom yang panjangnya 5.

N A M A S

A Y A L A

T I S Y A

Untuk mendapatkan *ciphertext* baca susunan huruf secara vertical sehingga dihasilkan *ciphertext* :

NATAYIMASALYSAA ⟶ tanpa spasi

NATA YIMA SALY SAA ⟶ bentuk pengelompokkan 4 huruf

Pengelompokkan *ciphertext* kedalam x huruf bertujuan untuk menyulitkan kripanalisis dalam memecahkan *ciphertext.* Pada contoh ini dipilih pengelompokkan kedalam 4 huruf.

Untuk proses dekripsi, bagi panjang *ciphertext* dengan kunci. Panjang *ciphertext* yaitu 15 huruf dan kunci yang digunakan yaitu 5. Sehingga didapat kunci yang digunakan untuk dekripsi sebesar 3 sehingga *ciphertext* akan disusun kedalam kolom yang panjangnya 3.

N	A	T
A	Y	I
M	A	S
A	L	Y
S	A	A

Untuk mendapatkan *plaintext* baca susunan huruf secara vertical sehingga dihasilkan *ciphertext* :

NAMASAYALATISYA ⟶ tanpa spasi

NAMA SAYA LATISYA ⟶ susunan *plaintext* yang benar

2.2.4 Playfair Cipher

Playfair Cipher ditemukan oleh Sir Charles Wheatstone (1802-1875) pada tahun 1854 dan dipopulerkan oleh Baron Lyon Playfair (1819-1898). Algoritma *Playfair Cipher* merupakan suatu algoritma kriptografi klasik yang mengenkripsi pasangan huruf (bigram). Kunci yang digunakan yaitu 25 buah huruf (kecuali huruf J) yang disusun didalam bujursangkar berukuran 5×5. Kemungkinan kuncinya sebanyak $25!$ [5].

Berikut merupakan salah satu contoh proses algoritma *Playfair Cipher.*

Kunci : INFORMATIKA ITERA

Plaintext : SUKA BACA BUKU KRIPTOGRAFI

Kunci yang digunakan harus diekstrak terlebih dahulu dengan membuang huruf yang berulang dan jika terdapat huruf J maka ganti dengan huruf I. Pada kunci INFORMATIKAITERA, kunci yang sudah diekstrak yaitu INFORMATKE.
Selanjutnya tambahkan huruf yang belum ada (kecuali J) secara berurutan. Sehingga kunci menjadi INFORMATKEBCDGHLPQSUVWXYZ.
Masukan huruf-huruf kunci kedalam bujur sangkar, susunan kunci seperti pada Tabel 2.3.

Tabel 2.3 Tabel kunci

I	N	F	O	R
M	A	T	K	E
B	C	D	G	H
L	P	Q	S	U
V	W	X	Y	Z

Pesan atau *plaintext* yang akan dienkripsi diatur terlebih dahulu sebagai berikut

1. Ganti huruf J dengan I (bila ada)
2. Kelompokkan pesan dalam pasangan huruf (bigram).
3. Jika ada pasangan huruf yang sama, sisipkan X diantaranya.
4. Jika jumlah huruf ganjil,tambahkan huruf X di akhir.

Plaintext : SUKA BACA BUKU KRIPTOGRAFI
Bigram : SU KA BA CA BU KU KR IP TO GR AF IX

Algoritma enkripsi:

1. Jika dua huruf berada pada baris kunci yang sama maka tiap huruf diganti dengan huruf dikanannya seperti pada Tabel 2.4. Substitusi bersifat siklik, artinya jika huruf berada pada bagian paling kanan tabel kunci, maka huruf substitusinya adalah huruf paling kiri pada baris yang sama.
   Biagram : SU
   Ciphertext : UL

Tabel 2.4 Enkripsi pada bigram sama baris

I	N	F	O	R
M	A	T	K	E
B	C	D	G	H
L	P	Q	S	U
V	W	X	Y	Z

2. Jika dua huruf berada pada kolom kunci yang sama maka tiap huruf diganti dengan huruf dibawahnya seperti pada Tabel 2.5. Substitusi bersifat siklik, artinya jika huruf berada pada bagian paling bawah tabel kunci, maka huruf substitusinya adalah huruf paling atas pada kolom yang sama [12].

   Biagram : CA

   Ciphertext : PC

Tabel 2.5 Enkripi pada bigram sama kolom

I	N	F	O	R
M	A	T	K	E
B	C	D	G	H
L	P	Q	S	U
V	W	X	Y	Z

3. Jika dua huruf tidak pada baris yang sama atau kolom yang sama, maka:
   - Huruf pertama diganti dengan huruf pada perpotongan baris huruf pertama dengan kolom huruf kedua.
   - Huruf kedua diganti dengan huruf pada titik sudut keempat dari persegi panjang yang dibentuk dari tiga huruf yang digunakan sebelumnya. Seperti pada Tabel 2.6.

     Biagram : KR

     Ciphertext : EO

Tabel 2.6 Enkripsi pada bigram tidak sama baris dan kolom

I	N	F	O	R
M	A	T	K	E
B	C	D	G	H
L	P	Q	S	U
V	W	X	Y	Z

Lakukan langkah tersebut pada semua bigram sehingga untuk contoh penyelesaian dengan :

Plaintext : SUKA BACA BUKU KRIPTOGRAFI

Kunci : INFORMATIKA ITERA

Didapat *ciphertex*t : UL ET CM PC HL ES EO NL KF HO TN FV