BAB II KERANGKA TEORITIS

A. Landasan Teori

1. Kriptografi

Menurut Nurdin (2017), kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan

Dari sumber ahli Nurdin (2017), definisi terbaru menyatakan bahwa kriptografi merupakan ilmu mengenai teknik untuk mengirimkan pesan secara rahasia

Setelah digabungkan dari para ahli, Dengan demikian kesimpulan yang didapatkan, Menurut Nurdin (2017), kriptografi adalah suatu ilmu sekaligus seni yang memiliki tujuan untuk menjaga keamanan sebuah pesan

a. Istilah dan Konsep dalam Kriptografi

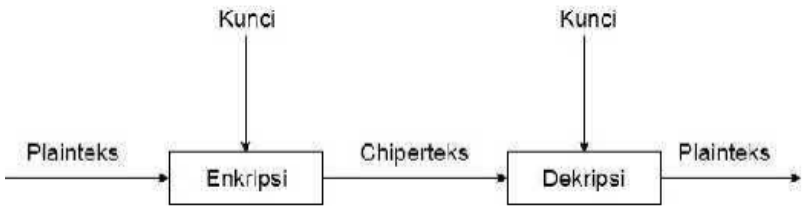
Kriptografi menurut sumber ahli (Munir, 2004) diantaranya sebagai berikut:

1) Plaintext dan Ciphertext Plaintext (pesan)
   Adalah pesan yang dikirim dan dapat dibaca atau disebut dengan Ciphertext
2) Peserta Komunikasi
   dibagi atas beberapa entitas.
   Entitas pertama adalah pengirim. Seseorang yang mengirim suatu pesan atau komunikasi, Lalu yang Entitas kedua adalah penerima. Seorang yang menerima pesan atau komunikasi
3) Enkripsi dan Dekripsi
   Sebuah kejadian dimana ketika Plaintext diubah menjadi CipherText itu bisa disebut juga dengan enkripsi
4) Kriptanalis dan Kriptologi
   Dalam pengertiannya Kriptanalis adalah seseorang yang membuat plaintext menjadi ciphertext tanpa memerlukan kunci , sedangkan Kriptologi adalah studi pembelajaran tentang Kriptanals dan Kriptografi

b. Jenis-Jenis Kriptografi

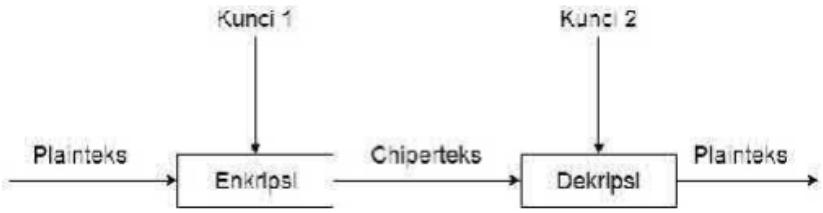
Jenis kunci yang ada di Kriptografi, Menurut Munir (2004) terdapat dua macam kriptografi, yaitu kriptografi simetri dan kriptografi asimetri.

1) Kriptografi simetri,adalah kunci yang digunakan sama dengan deskripsi



Gambar 2.1. Kriptografi Simetri (Munir, 2004)

2) Kriptografi asimetri, adalah yang digunakan berbeda kunci



Gambar 2.2. Kriptografi Asimetri (Munir, 2004)

c. Informasi

Menurut Ahli Tata Sutabri(2016). menyatakan bahwa Informasi bagaikan darah dalam tubuh organisasi. Bisa diartikan juga sebagai penentu dalam pilihan

d. Data

Data itu sendiri dapat diartikan sebagai kumpulan fakta, dimana banyak catatan kejadian nyata dijadikan dalam suatu tumpukan berkas

e. Keamanan Data dan File

Menurut Hendrayudi, “File Merupakan media tempat penyimpanan kumpulan data.”

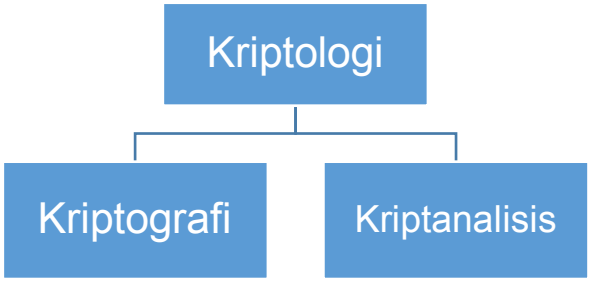
Berbeda dengan Menurut McLeod (PEARSON) “File merpukan data yang saling terhubung.”

Sedangkan menurut Edi S. Mulyanta yang mengatakan, “File merupakan data yang berurutan.”

f. Komponen Sistem Kriptografi

Pada dasarnya komponen kriptografi terdiri dari beberapa komponen antara lain Ariyus (2008), :

1) Enkripsi : proses dimana pesan akan di buat kode yang dirahasiakan sehingga membuat rahasia
2) Dekripsi : berbeda dengan Enkripsi, Deskripsi itu adalah proses dimana memecahkan kode yang dirahasiakan oleh proses enkripsi
3) Kunci : kode yang digunakan untuk merahasiakan file
4) Ciphertext :suatu pesan (arti) yang telah melalui proses enkripsi.
5) Plaintext :suatu text asli
6) Pesan : data informasi berupa (kertas, *storage*, dsb) yang dikirimkan.
7) Cryptanalysis dan Cryptology : Cryptanalysis merupakan ilmu yang mempelajari dalam pengkodean suatu pengamanan data



Gambar 2.3 Kriptografi dan Kriptanalisis adalah cabang bidang ilmu Kriptologi

Sumber : Ariyus (2008).

g. Encoding dan Decoding

Menurut Danesi (2013) pengkodean atau penyandian (*encoding*) merupakan sebuah proses konversi informasi menjadi data dan dikirim ke pengawas. Sedangakan (*decoding)* adalah proses kebalikannya, proses konversi data menjadi informasi yang dikirim oleh pengawas

h. Microsoft Visual Studio (VB.net)

Dalam penelitian ini tool aplikasi yang digunakan adalah Microsoft Visual Studio 2010, karena Visual Studio 2010 pada dasarnya adalah sebuah bahasa pemrograman komputer, dimana pengertian dari bahasa pemrograman itu adalah perintah-perintah atau instruksi yang dimengerti oleh komputer untuk melakukan tugas-tugas tertentu.

i. Ujian Sekolah

Menurut sumber Ahli Mardapi (2015: 1), Ujian adalah sebuah bentuk dalam mengukur nilai seseorang dari hasil pembelajaran

B. Metode Caesar Cipher

Menurut Sumber Ahli Ade Candrad (2015), Caesar cipher merupakan salah satu Algoritma yang sudah tua sangat tua, dimana teknik dengan teknik subtitusi.

Contoh Kasus Caesar cipher

Dalam hal ini kuncinya adalah pergeseran huruf (yaitu 3). Susunan alphabet setelah digeser sejauh 3 huruf sehingga membentuk sebuah table substitusi sebagai berikut:

Alfabet Biasa: 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

Alfabet Sandi: 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

Untuk memecahkan sandi tersebut gunakan cara sebaliknya. Contoh penyandian sebuah pesan adalah sebagai berikut.

Teks Terang : MAKAN

Teks Sandi : OCMCP

Jadi dengan mengkodekan setiap huruf alfabet dengan integer : ‘A’= 0 , ‘B’= 1,…, ‘Z’= 25, sehingga membuat pergeseran pada hurufnya

$C = E (P) = (P + 3) \bmod 26$

Dikarenakan bentuk jumlah Alfabet sendiri berjumlah 26 maka akan diubah sebagai berikuti :

$P = D (C) = (C - 3) \bmod 26$

Dapat diperhatikan bahwa jika fungsi D adalah balikan (invers) dari fungsi E, yaitu :

$D (C) = E^{-1} (P)$

Salah satu contohnya adalah ROT13 dimana jumlah huruf posisinya 13 dan dapat diartikan dengan sebuah gambar.Maka hal ini dapat dituliskan sebagai:

C = ROT13 (M)

Untuk mengembalikan kembali ke bentuk semulanya dilakukan proses

enkripsi ROT13 dua kali.

M = ROT13 (ROT13 (M))

Tabel 2.1 Caesar Cipher

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

Cara agar menyembunyikan rasa amarah kita kepada salah satu orang dan tidak dapat diketahui oleh setiap orang maka dengan menggunakan ROT13 (Orang yang ingin membaca makian kita harus melakukan konversi ROT13 sendiri menurut Apriani Mega, Seftyanto Donny, (2012).

C. Tinjauan Pustaka

Pada penelitian sebelumnya sudah banyak dilakukan pada kasus yang sama namun dengan metode yang berbeda sebagai bahan pertimbangan pada penelitian ini dan untuk mengetahui perbedaan pada penelitian sebelumnya dengan penelitian yang akan dilakukan. Berikut adalah penelitian yang pernah dilakukan sebelumnya :

1. **Menurut Rifkie Primartha 2011, dalam penelitian yang berjudul "Penerapan Enkripsi dan Dekripsi File Menggunakan Algoritma Data Encryption Standard (DES)",**

   Mengungkapkan Bahwa Kriptografi dapat mengamankan data rahasia maupun informasi penting, dapat di implementasikan dengan teknolgi terbaru seperti ATM dan Mobile Banking.

   Adapun perbedaan di penelitian yang dilakukan adalah Caesar Cipher sendiri merupakan teknik Subtitusi

2. **Menurut I Gede Agus Budiawan 2008, dalam penelitian yang berjudul "Aplikasi Pengamanan Data Menggunakan Algoritma RC4",**

   Mengungkapkan Bahwa Kriptografi menggunakan sebuah kunci Symmetric-Key dan Asymmetric-Key. Kunci Symmetric sendiri adalah kunci yang diunakan pada enkripsi maupun deskripsi. Berbeda dengan Asymmetric-Key yang sama sekali menggunakan kunci yang berbeda dalam emkripsi maupun deskripsi

   Adapun perbedaan penelitian yang dilakukan adalah RC4 menggunakan kunci dari 1 sampai 256 byte sedangkan Caesar cipher hanya 1 sampai 64 byte saja

3. **Menurut Erwin Gunadhi, Agung Sudrajat 2016, dalam penelitian yang berjudul "Pengamanan Data Rekam Medis Pasien Menggunakan Algortitma Kriptografi VIGENERE CHIPER",**

   Mengungkapkan bahwa kriptografi Vigènere cipher merupakan teknik dimana pengaman data yang dapat pada rekam medis. Kunci nya sendiri dalam bentuk numeric (yaitu, a=0, b=1, c=2, d=3, e=5…, z=25). huruf kunci c(=2) menyatakan huruf-huruf plainteks digeser sebanyak 2 huruf ke kanan (dari susunan alfabetnya), sedangkan Caesar Cpher ke arah biner saja..

4. **Menurut Henny Wandani, Muhammad Andri Budiman 2015, dalam penelitian yang berjudul "Implementasi Sistem Kemanan Data Dengan Menggunakan Teknik Steganografi *End Of File (EOF)* dan Rabin *Public Key Cryptosystem"*,**

   Mengungkapkan bahwa proses enkripsi data memiliki jumlah maksimum yaitu hanya 24 digit angka, setelah itu, akan di muat dalam sebuah data gambar yang berukuran minimum 25x25. Selanjutnya, akan dilakkan ekstraksi algoritma Rabin Public Key dan teknik steganografi yang digunakan adalah metode End of File

Adapun perbedaan dari penelitian ini adalah dimana Caesar Cipher menggunakan sistem Substitusi

5. **Menurut Susanto 2017, dalam penelitian yang berjudul "Implementasi Keamanan Data Menggunakan Algoritma Blowfish Pada Sistem Informasi Koperasi Rias",**
   Mengungkapkan pBahwa Database adalah sebuah tempat penyimpanan. Dengan menggunakan MySQL, sistem informasi koperasi RIAS pada database dapat di enkripsi serta diartikan dalam bahasa umum
   Adapun perbedaan dengan penelitan ini dimana proses caesar chiper hanya menggunakan sistem pengkodean lama
6. **Menurut Susanto, Andrianto Tri Susilo 2018, dalam penelitian yang berjudul "Penerapan Algoritma Asimetris RSA Untuk Keamanan Data Pada Aplikasi Penjualan CV. SINERGI COMPUTER LUBUKLINGGAU Berbasis Web",**
   Mengungkapkan Bahwa. Dalam pengaman Database. Penerapan algoritma kriptografi RSA menjadi solusi yang baik pada sistem penjualan yang akan dibangun CV
   Adapun perbedaan yang dilakukan adalah sistem pengamanan data dari kode maupun kunci nya berbeda
7. **Menurut Muhammad Fahmi Ridho 2017, dalam penelitian yang berjudul "Perancangan Aplikasi Keamanan Data Dengan Algoritma SERPENT",**
   Mengungkapkan bahwa dalam sitem Database yang menyimpan data penting Penerapan algoritma kriptografi RSA menjadi solusi yang baik
   Adapun perbedaan yang dilakukan adalah Algoritma caesar cipher hanya subtitusi
8. **Menurut Muhammad Zulham, Helmi Kurniawan, Iwan Fitrianto Rahmad 2014 , dalam penelitian yang berjudul "Perancangan Aplikasi Keamanan Data Dengan Email menggunakan Algoritma Enkripsi RC6 Berbasis Android",**
   Mengungkapkan Bahwa RC6 dengan basis android sangat aman dalam proses pengamanan data

   Adapun perbedaan yang dilakukan adalah Algoritma RC6 menggunakan 4 register dan lebih rumit, berbeda dengan Caesar cipher yang lebih sederhana
9. **Menurut Semuil Tjiharjadi, Marvin Chandra Wijaya 2009, dalam penilitian yang berjudul "Pengamanan Data Menggunakan Metode Enkripsi Simetri Dengan Algoritma FEAL",**
   Mengungkapkan bahwa dalam mengamankan sebuah data yang sangat penting dibutuhkan suatu sistem. FEAL merupakansalah satu solusi terbaiknya
   Adapun perbedaan yang dilakukan adalah Algoritma Caesar chipher lebih sederhana
10. **Menurut Munawar 2012, dalam penelitian yang berjudul "Perancangan Algoritma Sistem Keamanan Data Menggunakan Metode Kriptografi Asimetris",**

Mengungkapkan bahwa implementasi ilmu kriptografi sangat dibutuhkan dalam ilmu komputer untuk mengamankan data serta infomasi yang sangat penting

Adapun perbedaan yang dilakukan adalah Algoritma Caesar cipher lebih sederhana

Tabel 2.2 Tijauan pustaka

No	Nama Peneliti	Jurnal Peneliti	Permasalahan	Kontribusi
1.	**Rifkie Primartha 2011,**	**"Penerapan Enkripsi dan Dekripsi File Menggunakan Algoritma Data Encryption Standard (DES)",**	Mengungkapkan Bahwa Kriptografi dapat mengamankan data rahasia maupun informasi penting, dapat di implementasikan dengan teknolgi terbaru seperti ATM dan Mobile Banking.	penelitian yang dilakukan adalah blok 64-bit dan kunci 56 bit. DES terdiri dari seri 16-putaran substitusi dan permutasi. sedangkani penelitian yang dilakukan adalah Caesar Cipher sendiri merupakan teknik Subtitusi
2.	**I Gede Agus Budiawan 2008,**	**"Aplikasi Pengamanan Data Menggunakan Algoritma RC4",**	Kriptografi menggunakan sebuah kunci Symmetric-Key dan Asymmetric-Key. Kunci Symmetric sendiri adalah kunci yang	penelitian yang dilakukan adalah RC4 menggunakan kunci dari 1 sampai 256 byte yang digunakan untuk menginisialisasikan tabel sepanjang

No	Nama Peneliti	Jurnal Peneliti	Permasalahan	Kontribusi
			diunakan pada enkripsi maupun deskripsi. Berbeda dengan Asymmetric-Key yang sama sekali menggunakan kunci yang berbeda dalam emkripsi maupun deskripsi	256 byte .
3.	**Erwin Gunadhi, Agung Sudrajat 2016,**	**"Pengamanan Data Rekam Medis Pasien Menggunakan Algortitma Kriptografi VIGENERE CHIPER",**	Mengungkapkan bahwa kriptografi Vigènere cipher merupakan teknik dimana pengaman data yang dapat pada rekam medis. Kunci nya sendiri dalam bentuk numeric (yaitu, a=0, b=1, c=2, d=3, e=5…, z=25). huruf kunci c(=2) menyatakan huruf-huruf plainteks digeser	pada rekam medis. Kunci nya sendiri dalam bentuk numeric (yaitu, a=0, b=1, c=2, d=3, e=5…, z=25). huruf kunci c(=2) menyatakan huruf-huruf plainteks digeser sebanyak 2 huruf ke kanan (dari susunan alfabetnya)

No	Nama Peneliti	Jurnal Peneliti	Permasalahan	Kontribusi
			sebanyak 2 huruf ke kanan (dari susunan alfabetnya)	
4.	**Henny Wandani, Muhammad Andri Budiman 2015,**	**"Implementasi Sistem Kemanan Data Dengan Menggunakan Teknik Steganografi *End Of File (EOF)* dan Rabin *Public Key Cryptosystem"*,**	Mengungkapkan bahwa proses enkripsi data memiliki jumlah maksimum yaitu hanya 24 digit angka, setelah itu, akan di muat dalam sebuah data gambar yang berukuran minimum 25x25. Selanjutnya, akan dilakkan ekstraksi algoritma Rabin Public Key dan teknik steganografi yang digunakan adalah metode End of File	Adapun perbedaan dari penelitian ini adalah dimana Caesar Cipher menggunakan sistem Substitusi
5.	**Susanto 2017,**	"**Implementasi Keamanan Data**	Mengungkapkan pBahwa	Adapun perbedaan

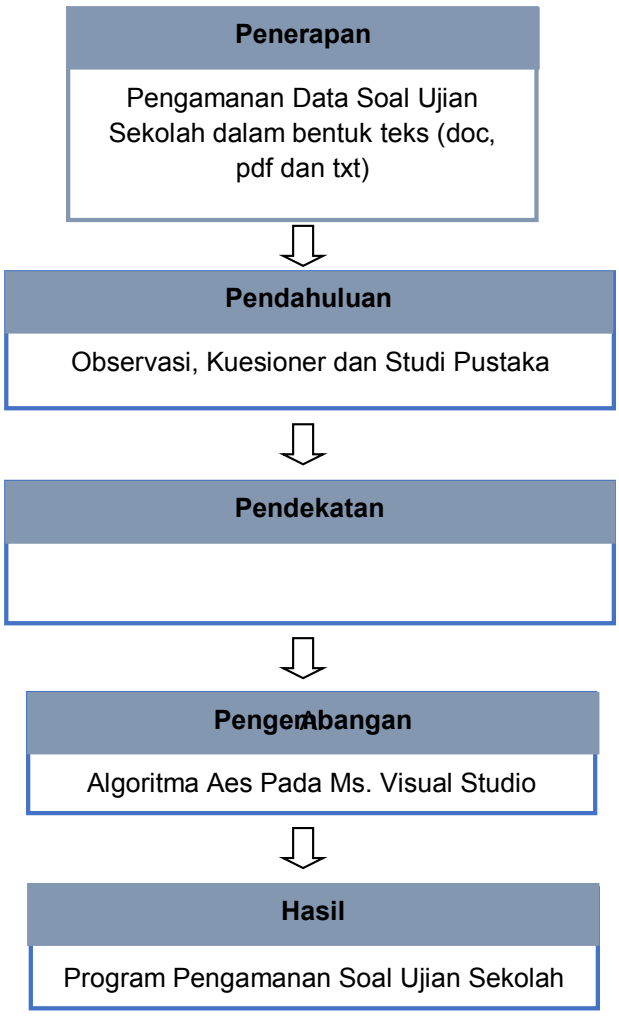
No	Nama Peneliti	Jurnal Peneliti	Permasalahan	Kontribusi
		Menggunakan Algoritma Blowfish Pada Sistem Informasi Koperasi Rias",	Database adalah sebuah tempat penyimpanan. Dengan menggunakan MySQL, sistem informasi koperasi RIAS pada database dapat di enkripsi serta diartikan dalam bahasa umum.	dengan penelitan ini dimana proses caesar chiper hanya menggunakan sistem pengkodean lama
6.	**Susanto, Andrianto Tri Susilo 2018,** .	**"Penerapan Algoritma Asimetris RSA Untuk Keamanan Data Pada Aplikasi Penjualan CV. SINERGI COMPUTER LUBUKLINGGAU Berbasis Web",**	Mengungkapkan Bahwa. Dalam pengaman Database. Penerapan algoritma kriptografi RSA menjadi solusi yang baik pada sistem penjualan yang akan dibangun CV	Adapun perbedaan yang dilakukan adalah sistem pengamanan data dari kode maupun kunci nya berbeda
7.	**Muhammad Fahmi Ridho 2017,**	"**Perancangan Aplikasi Keamanan Data Dengan Algoritma**	Mengungkapkan bahwa dalam sitem Database yang	Adapun perbedaan yang dilakukan adalah Algoritma

No	Nama Peneliti	Jurnal Peneliti	Permasalahan	Kontribusi
		SERPENT”,	menyimpan data penting Penerapan algoritma kriptografi RSA menjadi solusi yang baik	caesar cipher hanya subtitusi
8.	**Muhammad Zulham, Helmi Kurniawan, Iwan Fitrianto Rahmad, 2014**	**“Perancangan Aplikasi Keamanan Data Dengan Email menggunakan Algoritma Enkripsi RC6 Berbasis Android**	Mengungkapkan Bahwa RC6 dengan basis android sangat aman dalam proses pengamanan data	Adapun perbedaan yang dilakukan adalah Algoritma RC6 menggunakan 4 register dan lebih rumit, berbeda dengan Caesar cipher yang lebih sederhana
9.	**Semuil Tjiharjadi, Marvin Chandra 2009**	**“Pengamanan Data Menggunakan Metode Enkripsi Simetri Dengan Algoritma FEAL”**	Mengungkapkan bahwa dalam mengamankan sebuah data yang sangat penting dibutuhkan suatu sistem. FEAL merupakansalah satu solusi	Adapun perbedaan yang dilakukan adalah Algoritma Caesar chipher lebih sederhana

No	Nama Peneliti	Jurnal Peneliti	Permasalahan	Kontribusi
			terbaiknya	
10.	**Menurut Munawar 2012,**	**"Perancangan Algoritma Sistem Keamanan Data Menggunakan Metode Kriptografi Asimetris",**	Mengungkapkan bahwa implementasi ilmu kriptografi sangat dibutuhkan dalam ilmu komputer untuk mengamankan data serta infomasi yang sangat penting	Adapun perbedaan yang dilakukan adalah Algoritma Caesar cipher lebih sederhana

D. KERANGKA PEMIKIRAN

Kerangka pemikiran untuk pemecahan permasalahan dalam penelitian ini dapat digambarkan pada gambar 2.4



Gambar 2.4 Kerangka Pemikiran Penelitian

Penjelasan tentang kerangka pemikiran pada penelitian ini adalah :

1. Penerapan untuk menetapkan tujuan penelitian yang dilakukan.
2. Pendahuluan dengan Observasi, Kuesioner dan Studi Pustaka sebagai referensi dan teori yang digunakan dalam penelitian.
3. Pendekatan merupakan algoritma yang digunakan dalam proses penelitian.
4. Pengembangan sebagai pengembangan dan perancangan algoritma dengan software yang digunakan dalam penelitian.
5. Hasil Melakukan evaluasi terhadap aplikasi kriptografi yang dikembangkan.

E. HIPOTESIS

Berdasarkan permasalahan yang dihadapi yaitu kurang optimal dan belum aman dalam pengamanan data ujian sekolah pada saat penyimpanan data ujian, maka perlu adanya suatu cara untuk mengatasi permasalahan tersebut, diantaranya adalah metode *Caesar Chiper* dapat digunakan untuk Enkripsi. Berdasarkan dari pengungkapan penulis, maka dapat ditetapkan hipotesis metode *Caesar Chiper* diduga dapat mengoptimalkan dalam pengamanan data ujian.