BAB II

TINJAUAN PUSTAKA

II.1. Penelitian Terdahulu

Berdasarkan penelitian yang dilakukan oleh (Hossain Biswas et al., 2019) mengenai *A systematic study on classical cryptographic cypher in order to design a smallest cipher*, Biswas, dkk menggunakan metode *Porta Cipher* untuk studi kerahasiaan data berbentuk teks.

Berdasarkan penelitian yang dilakukan oleh (Al-omari, 2018) mengenai ABJAD *Arabic-Based Encryption*, Omari menggunakan metode *Porta Cipher* untuk merahasiakan abjad arab.

Berdasarkan penelitian yang dilakukan oleh (Saraswat et al., 2016) mengenai *An Extended Hybridization of Vigenere and Caesar Cipher Techniques for Secure Communication*, Saraswat, dkk menggunakan metode *Porta Cipher* untuk kerahasiaan komunikasi berbentuk teks.

Berdasarkan penelitian yang dilakukan oleh (Rosdiana, 2018) mengenai Rancang Bangun Aplikasi Penyandian Data Text Menggunakan Algoritma *Diffie-Hellman* Dan Algoritma RC4, Alam, dkk menggunakan metode *Diffie-Hellman* untuk pertukaran kunci RC4.

Berdasarkan penelitian yang dilakukan oleh (Khairani et al., 2021) mengenai Pengkodean *Monoalphabetic* Menggunakan *Affine Cipher* dengan Kunci *Diffie-Hellman*, Khairani, dkk menggunakan metode *Diffie-Hellman* untuk pertukaran kunci *Affine Cipher*.

Berdasarkan penelitian yang dilakukan oleh (Nisa et al., 2020) mengenai Aplikasi Enkripsi Citra dan Teks Menggunakan Algoritma *Diffie-Hellman* dan *ElGamal*, Nisa, dkk menggunakan metode *Diffie-Hellman* untuk pertukaran kunci *ElGamal*.

II.2. Landasan Teori

Landasan teori peneliti kutip dari beberapa teori yang berkaitan dengan penelitian ini yaitu:

II.2.1. Aplikasi

Aplikasi merupakan suatu program komputer yang dapat digunakan pada berbagai perangkat elektronik, terutama pada komputer/laptop atau telepon seluler yang berbasis *android*. Aplikasi merupakan komponen yang berguna melakukan pengolahan data maupun kegiatan-kegiatan seperti pembuatan dokumen atau pengolahan data. (Nugraha et al., 2020).

II.2.2. Kriptografi

Kriptografi dapat didefinisikan sebagai seni maupun ilmu yang menghasilkan pesan yang rahasia. Sebuah pesan asli yang disebut sebagai plaintext disandikan menjadi pesan yang tersandi yang disebut sebagai ciphertext melalui proses enkripsi dan ciphertext dipulihkan menjadi plaintext kembali melalui proses dekripsi. Kriptografi memiliki beragam algoritma yang telah banyak digunakan sebagai keamanan untuk informasi. Algoritma kriptografi dikelompokkan ke dalam dua jenis yaitu algoritma kriptografi klasik dan

algoritma kriptografi modern. Dalam pengoperasiannya, algoritma kriptografi klasik bekerja menggunakan mode karakter sedangkan algoritma kriptografi modern bekerja menggunakan mode bit. (Yusfrizal, 2019).

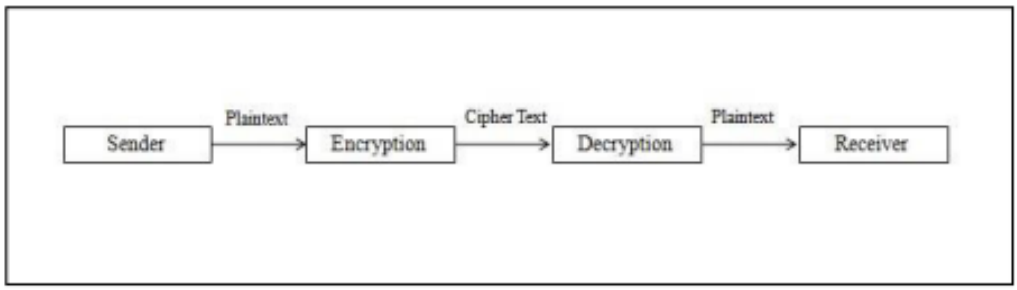
Kriptografi merupakan ilmu yang mempelajari penyandian pesan. Seiring berkembangnya zaman keamanan penyandian pesan menjadi sangat sensitif, karena banyak individu yang menyalahgunakan informasi untuk hal yang merugikan orang lain. Sehingga dibutuhkan ilmu penyandian pesan yang baik agar kerahasiaan pesan terjaga dengan aman. (Khairani et al., 2021).

Salah satu upaya pengamanan sistem informasi yang dapat dilakukan adalah kriptografi. Kriptografi sesungguhnya merupakan studi terhadap teknik matematis yang terkait dengan aspek keamanan suatu sistem informasi, antara lain seperti kerahasiaan, integritas data, keaslian, dan ketiadaan penyangkalan. Keempat aspek terserbut yang menjadi tujuan fundamental dari suatu sistem kriptografi.

1. Kerahasiaan Kerahasiaan adalah layanan yang digunakan untuk menjaga informasi dari setiap pihak yang tidak berwenang untuk mengaksesnya. Dengan demikian informasi hanya akan dapat diakses oleh pihak-pihak yang berhak saja.
2. Integritas Data (*Data Integrity*) Integritas data merupakan layanan yang bertujuan untuk mencegah terjadinya pengubahan informasi oleh pihak-pihak yang tidak berwenang. Untuk meyakinkan integritas data ini harus dipastikan agar sistem informasi mampu mendeteksi terjadinya manipulasi data.

Manipulasi data yang dimaksud meliputi penyisipan, penghapusan, maupun penggantian data.

3. Keaslian (*authentication*) Keaslian merupakan layanan yang terkait dengan pembuktian identifikasi terhadap pihak-pihak yang ingin mengakses sistem informasi (*entity authentication*) maupun pembuktian data dari sistem informasi itu sendiri (*data origin authentication*).
4. Ketiadaan Penyangkalan (*non-repudiation*) Ketiadaan penyangkalan merupakan layanan yang berfungsi untuk mencegah entitas yang berkomunikasi melakukan penyangkalan, yaitu pengiriman pesan menyangkal melakukan pengiriman atau penerima pesan menyangkal telah menerima pesan. (Alam & Pasaribu, 2019).

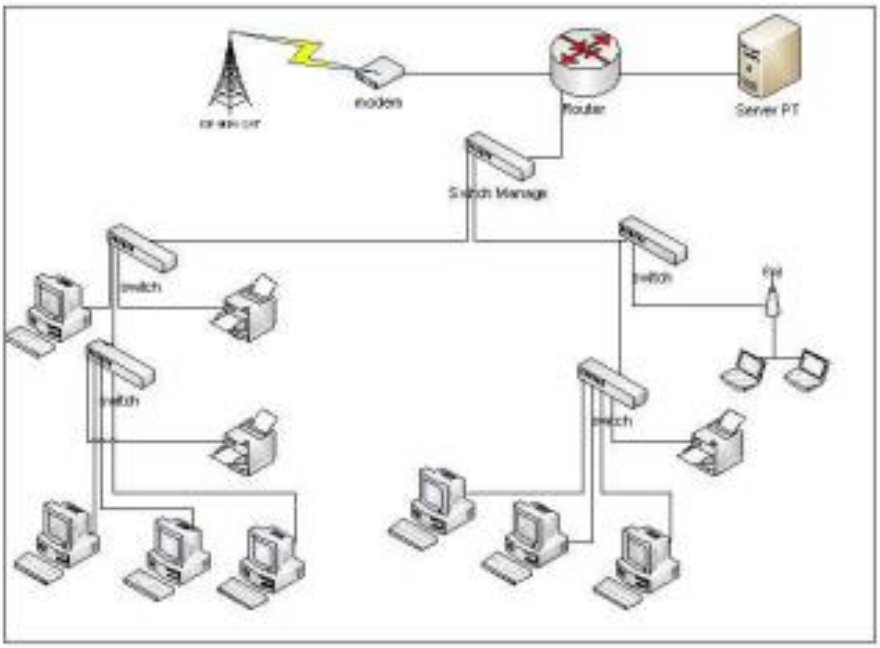


Gambar II.1. Konsep Kriptografi
(Sumber: (Alam & Pasaribu, 2019)**)**

II.2.3. Keamanan Jaringan

Keamanan jaringan merupakan suatu cara atau suatu sistem yang digunakan untuk memberikan proteksi atau perlindungan pada suatu jaringan agar terhindar dari berbagai ancaman luar yang mampu merusak jaringan dan pencurian data perusahaan. Jaringan komputer adalah sekumpulan komputer yang dapat saling berhubungan antara satu dengan lainnya dengan menggunakan media komunikasi, sehingga dapat saling berbagi data, informasi, program, dan

perangkat keras. Topologi jaringan komputer adalah suatu cara menghubungkan komputer yang satu dengan komputer lainnya sehingga membentuk jaringan. Cara yang saat ini banyak digunakan adalah bus, token ring dan star. Dalam suatu jaringan komputer jenis topologi yang dipilih akan mempengaruhi kecepatan komunikasi. Untuk itu maka perlu dicermati kelebihan/keuntungan dan kekurangan/kerugian dari masing-masing topologi berdasarkan karakteristiknya. (Nitra & Ryansyah, 2019).

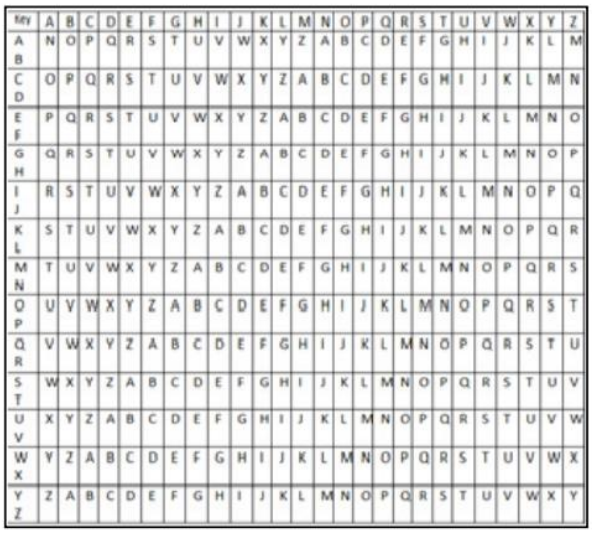


Gambar II.2. Topologi Jaringan
(Sumber: (Nitra & Ryansyah, 2019))

II.2.4. *Porta Cipher*

Porta Cipher adalah sandi substitusi polialfabetik. Dulu ditemukan oleh Giovanni Battista della Porta. Ini menggunakan 13 huruf secara timbal balik dan penyandiannya sama dengan menguraikan. Ini cukup kuat. Sandi Porta bisa menjadi rusak dengan cara yang sama seperti *Vigenere Cipher*. Dia diakui oleh ACA. (Hossain Biswas et al., 2019).

Teknik *cipher* porta mirip dengan teknik *cipher vigenere*; satu-satunya perbedaannya adalah ia menggunakan 13 pasang abjad sebagai kunci, alih-alih menggunakan semua 26 abjad secara individual. Lewat sini dua karakter kunci yang berbeda akan dapat menghasilkan teks terenkripsi yang sama untuk karakter teks biasa yang diberikan. Seperti tabel porta ditunjukkan pada gambar II.1. CALLMEATNINE plaintext menggunakan kunci ATTACK-ATTACK akan menghasilkan teks sandi PWHYAWNPJVBW dalam kasus ini.



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

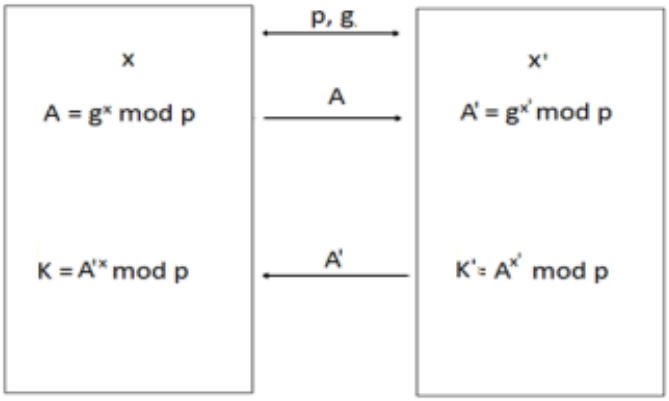
Gambar II.3. Porta Cipher
(Sumber: (Saraswat et al., 2016))

II.2.5. *Diffie Hellman*

Algoritma Pertukaran kunci *Diffie Hellman* (DH), diusulkan oleh Whitfield Diffie dan Martin Hellman pada tahun 1976, adalah skema algoritma asimetris yang pertama kali diterbitkan dalam literatur terbuka. penemuan ini juga dipengaruhi oleh karya Ralph Merkle. pertukaran kunci ini memberikan solusi praktis untuk masalah distribusi kunci, yaitu, memungkinkan dua pihak untuk mendapatkan kunci rahasia dengan berkomunikasi melalui saluran tidak aman. Kita dapat memberikan *public key* ke manapun tujuan yang kita inginkan, melalui

telepon, internet, *keyserver*, dan sebagainya. Kunci rahasia yang telah didistribusikan kemudian digunakan untuk enkripsi dan .Fungsi algoritma ini sendiri terbatas pada pertukaran nilai rahasia. (Alam & Pasaribu, 2019).

Jika p adalah bilangan prima dan g dan y adalah sembarang bilangan bulat, carilah x sedemikian sehingga g x = y (mod p). Secara umum algoritma *Diffie-Hellman* dapat digambarkan pada Gambar II.4.



Gambar II.4. *Diffie Hellman*
(Sumber: (Alam & Pasaribu, 2019))

II.2.6. Android

Android Software Development Kit (SDK) adalah sebuah alat untuk para pengembang aplikasi berbasis *Android*. Di dalam *android* SDK terdapat level API yang di dalamnya adalah alat perbaikan kesalahan program, pustaka-pustaka, *emulator*, dokumentasi, kode sumber serta tutorial. Level-level API tersebut adalah inisialisasi dari setiap *platform android* yang berisi paket dalam pengembangan aplikasi *Android*. Dengan adanya *android* SDK ini memudahkan para pengembang untuk menerapkan contoh kode sumber dari contoh aplikasi yang ada pada setiap API. (IVAN MAURITS, 2020).

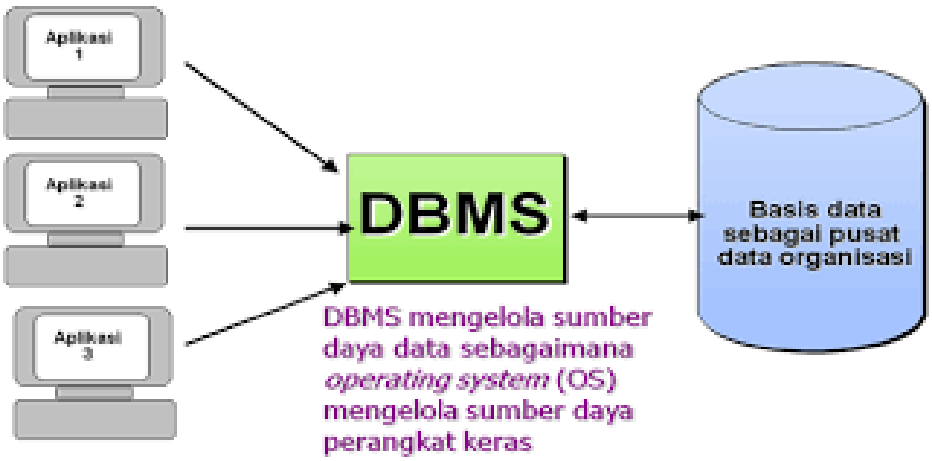
Berikut versi-versi *Android* yang telah dirilis hingga saaat ini:

1. Android 1.1
2. Android 1.5 (*Cupcake*)
3. Android 1.6 (*Donut*)
4. Android 2.0-2.1 (*Eclair*)
5. Android 2.2.3 (*Froyo*)
6. Android 2.3-2.3.7 (*Gingerbread*)
7. Android 3.0-3.2.6 (*Honeycomb*)
8. Android 4.0-4.0.4 (*Ice Cream Sandwich*)
9. Android 4.1-4.3.1 (*Jelly Bean*)
10. Android 4.4 (*KitKat*)
11. Android 5.0 (*Lollipop*)
12. Android 6.0 (*Marshmallow*)
13. Android 7.0 (*Nougat*)
14. Android 8.0 (*Oreo*)
15. Android 9.0 (*Pie*). (Nugraha et al., 2020).

II.2.7. Basis Data

Basis data adalah kumpulan informasi yang disimpan di dalam komputer secara sistematik sehingga dapat diperiksa menggunakan suatu program komputer untuk memperoleh informasi dari basis data tersebut. Basis data adalah representasi kumpulan fakta yang saling berhubungan disimpan secara bersama sedemikian rupa dan tanpa pengulangan (redudansi) yang tidak perlu, untuk memenuhi berbagai kebutuhan. Basis data merupakan sekumpulan informasi yang

saling berkaitan pada suatu subjek tertentu pada tujuan tertentu pula. Basis data adalah susunan *record* data operasional lengkap dari suatu organisasi atau perusahaan, yang diorganisir dan disimpan secara terintegrasi dengan menggunakan metode tertentu dalam komputer sehingga mampu memenuhi informasi yang optimal yang dibutuhkan oleh para pengguna. (Helmud, 2021).



Gambar II.5. Basis Data
(Sumber: (Helmud, 2021))

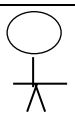
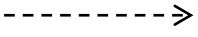
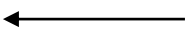
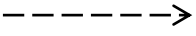
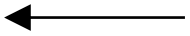
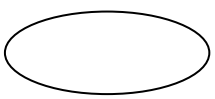
II.2.8. *Unified Modeling Language* (UML)

Unified Modeling Language (UML) adalah sebuah bahasa untuk menentukan, visualisasi, kontruksi, dan mendokumentasikan *artifact* (bagian dari informasi yang digunakan atau dihasilkan dalam suatu proses pembuatan perangkat lunak. *Artifact* dapat berupa model, deskripsi atau perangkat lunak) dari sistem perangkat lunak, seperti pada pemodelan bisnis dan sistem non perangkat lunak lainnya.

1. *Use Case Diagram*

Use Case Diargam merupakan pemodelan untuk melakukan (*behavior*) sistem informai yang akan dibuat. *Use case* digunakan untuk mengetahui fungsi apa saja yang ada di dalam sebuah sistem informasi dan siapa saja yang berhak menggunakan fungsi-fungsi itu. Berikut adalah simbol-simbol yang ada pada diagram *use case*. *Use case diagram* dapat digambarkan dengan sumber-sumber pada Tabel II.1.

Tabel II.1. Simbol *Use Case*

Notasi	Keterangan	Simbol
Actor	Menspesifikasikan himpunan peran yang pengguna mainkan ketika berinteraksi dengan *use case*.	
Depedency	Hubungan dimana perubahan yang terjadi pada suatu elemen mandiri (*independent*) akan mempengaruhi elemen yang bergantung padanya elemen yang tidak mandiri (*independent*).	
Generalization	Hubungan dimana objek anak (*descendent*) berbagi perilaku dan struktur data dari objek yang ada di atasnya objek induk (*ancestor*).	
Include	Menspesifikasikan bahwa *use case* sumber secara eksplisit.	
Extend	Menspesifikasikan bahwa *use case* target memperluas perilaku dari *use case* sumber pada suatu titik yang diberikan.	
Association	Apa yang mnghubungkan antara objek satu dengan objek lainnya.	
System	Menspesifikan paket yang menampilkan sistem secara terbatas.	
Use Case	Deskripsi dari urutan aksi-aksi yang ditampilkan sistem yang menghasilkan suatu hasil yang terukur bagi suatu *actor*.	
Collaboration	Interaksi aturan-aturan dan elemen lain yang bekerja sama untuk	

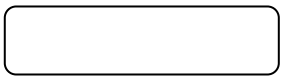
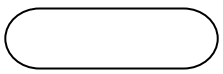
	menyediakan prilaku yang lebih besar dari jumlah dan elemen-elemennya (sinergi).	
Note	Elemen fisik yang eksis saat aplikasi dijalankan dan mencerminkan suatu sumber daya komputasi	

(Sumber: (Pitrawati dan Sanjaya, 2021))

2. Diagram Aktivitas (*Activity Diagram*)

Activity Diagram menggambarkan *workflow* (aliran kerja) atau aktivitas dari sebuah sistem atau proses bisnis atau menu yang ada pada perangkat lunak. Perlu diperhatikan bahwa diagram aktivitas menggambarkan aktivitas sistem bukan apa yang dilakukan aktor, jadi aktivitas yang dapat dilakukan oleh sistem. Berikut adalah simbol-simbol yang ada pada diagram aktivitas. *Activity diagram* dapat digambarkan dengan simbol-simbol seperti pada tabel II.2.

Tabel II.2. Simbol *Activity Diagram*

Notasi	Keterangan	Simbol
Activity	Memperlihatkan bagaimana masing-masing kelas antarmuka saling berinteraksi satu sama lain.	
Action	*State* dari sistem yang mencerminkan eksekusi dari suatu aksi.	
Initial Node	Bagaimana objek dibentuk atau diawali.	
Activity Final	Bagaimana objek dibentuk dan dihancurkan	
Fork Node	Satu aliran yang pada tahap tertentu berubah menjadi beberapa aliran	

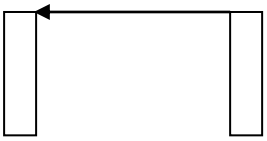
(Sumber: (Pitrawati dan Sanjaya, 2021))

3. Diagram Urutan (*Sequence Diagram*)

Sequence diagram menggambarkan interaksi antar objek di dalam dan di sekitar sistem (termasuk pengguna, *display*, dan sebagainya) berupa *message* yang

digambarkan terhadap waktu. *Sequence Diagram* dapat digambarkan dengan simbol-simbol seperti pada Tabel II.3.

Tabel II.3. Simbol *Sequence Diagram*

Nama	Keterangan	Gambar
Lifeline	Objek *entity*, antarmuka yang saling berinteraksi.	
Message	Spesifikasi dari komunikasi antar objek yang memuat informasi-informasi tentang aktifitas yang terjadi.	
Message	Spesifikasi dari komunikasi antar objek yang memuat informasi-informasi tentang aktifitas yang terjadi.	

(Sumber: (Pitrawati dan Sanjaya, 2021))