BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi saat ini sudah jadi hal penting untuk dimanfaatkan, sehingga diperlukan sarana dan prasarana yang dapat mencukupi kebutuhan akan informasi tersebut. Timbulnya berbagai informasi tersebut mendorong manusia untuk mencapai dan mengembangkan teknik-teknik baru agar pengolahan data dapat dilaksanakan dengan cepat, akurat, dan efisien. Salah satunya adalah melakukan pemilihan kepala desa dengan memanfaatkan teknologi. Pemilihan kepala desa di Kecamatan Barus, Kabupaten Tapanuli Tengah banyak dilakukan dengan cara coblos lembar kertas suara, kemudian memasukkan kertas suara tersebut kedalam kotak suara yang tersedia. Setelah tahapan pemungutan selesai akan dilanjutkan ke perhitungan suara. Proses pemilihan kepala desa tersebut sering terjadi kesalahan yang disebabkan oleh *human error*, yakni pemilih salah dalam pencoblosan lembar kertas suara, sehingga banyak kertas suara yang rusak dan dinyatakan tidak sah. Proses perhitungan suara masih dilakukan dengan cara manual, hal ini menyebabkan perhitungan menjadi lambat karena proses tersebut harus meghitung satu persatu lembar kertas suara. Adanya permasalahan tersebut membuat proses pemilihan kepala desa menjadi tidak efektif. Untuk itu, dibutuhkan sebuah sistem yang dapat mengatasi permasalahan tersebut.

Dengan adanya permasalahan di atas, penulis mencoba membangun sebuah sistem pemilihan kepala desa dengan menggunakan *e-voting* (*electronic voting*).

Dimana *e-voting* merupakan penggunaan teknologi komputer dalam melaksanakan pemilihan dan penghitungan suara (Sany, 2021).

Prosedur pemungutan suara yang digunakan dalam istilah *e-voting* memungkinkan pemilih untuk memberikan suara yang aman, rahasia, dan terjamin melalui sistem elektronik (Abba et al., 2017).

Langkah-langkah untuk memastikan keamanan dan kerahasiaan data tersebut dapat dilakukan dengan menggunakan algoritma kriptografi. Algoritma kriptografi melakukan dua fungsi yaitu enkripsi dan dekripsi. Salah satu algoritma enkripsi yang dapat digunakan untuk menjaga keamanan dan kerahasiaan data adalah *vigenere cipher*.

Menurut (Pramudya et al., 2021) *vigenere cipher* merupakan hasil dari penyederhanaan sandi substitusi polialfabetik dan terdiri dari beberapa bagian sandi *caesar* dengan proses pergeseran nilai yang berbeda dengan menambahkan angka kata kunci dan angka pesan lalu dimoduluskan dengan 26 dan hasilnya yang berupa angka tersebut dirubah ke dalam huruf untuk mendapatkan huruf yang tersandi (Lukman Sholeh & Ali Muharom, 2016).

Algoritma *vigenere cipher* menggunakan sebuah kunci pada saat melakukan enkripsi dan dekripsi. Oleh karena itu, untuk menghindari adanya pendistribusian kunci serta sebagai model keamanan data voting dengan keamanan ganda, maka algoritma *vigenere cipher* ini akan dibantu dengan skema *three pass protocol*.

Three pass protocol memungkinkan satu pihak untuk mengirim pesan dengan aman ke pihak lain tanpa bertukar atau mendistribusikan kunci enkripsi. Disebut dengan *three pass protocol* karena terdapat tiga pertukaran untuk

mengotentikasi pengirim dan penerima dari protokol pertama (Oktaviana & Utama Siahaan, 2016).

Maka berdasarkan latar belakang masalah yang sudah diuraikan, penulis melakukan penelitian dengan judul "KEAMANAN DATA HASIL *E-VOTING* PEMILIHAN KEPALA DESA DENGAN ALGORITMA *VIGENERE CIPHER* PERTUKARAN KUNCI *THREE PASS PROTOCOL* PADA KECAMATAN BARUS KABUPATEN TAPANULI TENGAH".

1.2 Rumusan Masalah

Berdasarkan uraian latar belakang diatas, rumusan masalah dalam penelitian ini adalah sebagai berikut:

1. Belum adanya aplikasi pemilihan kepala desa di Kecamatan Barus, Kabupaten Tapanuli Tengah.
2. Bagaimana menerapkan algoritma *vigenere cipher* dan *three pass protocol* dalam melakukan pengamanan data *e-voting* yang aman, rahasia dan terjamin?

1.3 Batasan Masalah

Agar pembahasan lebih terarah dan sesuai dengan judul tugas skripsi yang telah ditentukan, penulis hanya membahas pokok-pokok bahasan sebagai berikut:

1. Aplikasi yang dibangun merupakan aplikasi berbasis web.
2. Pembuatan aplikasi menggunakan bahasa pemrograman PHP dan

menggunakan *database server* MySQL.

3. Perancangan aplikasi *e-voting* pemilihan kepala desa hanya pada Kecamatan Barus di Kabupaten Tapanuli Tengah.
4. 3 kunci yang digunakan pada *three pass protocol* merupakan kunci statis bukan kunci dinamis.

1.4 Tujuan dan Manfaat Penelitian

1.4.1 Tujuan Penelitian

Tujuan yang ingin dicapai dalam penelitian tugas skripsi ini adalah:

1. Untuk mengetahui bagaimana membuat aplikasi yang mampu yang dapat melakukan sistem *e-voting* pemilihan kepala desa di Kecamatan Barus, Kabupaten Tapanuli Tengah.
2. Untuk mengetahui bagaimana menerapkan algoritma *vigenere cipher* dan *three pass protocol* dalam melakukan pengamanan data *e-voting* yang aman, rahasia dan terjamin.

1.4.2 Manfaat Penelitian

Adapun manfaat penelitian ini adalah sebagai berikut:

1. Dapat menghasilkan aplikasi yang mampu yang dapat melakukan sistem *e-voting* pemilihan kepala desa di Kecamatan Barus, Kabupaten Tapanuli Tengah.
2. Membantu Kecamatan Barus, Kabupaten Tapanuli Tengah dalam mendukung tujuan menuju *E-Governance*.
3. Tugas skripsi ini dapat menambah referensi dalam bidang pengamanan data

serta sistem *e-voting*

1.5 Metodologi Penelitian

Metodologi penelitian yang digunakan pada penelitian ini adalah:

1. Studi Kepustakaan

Pada tahap ini dilakukan studi kepustakaan yaitu proses mengumpulkan informasi dengan melakukan pengumpulan, mempelajari, dan membaca berbagai bahan referensi yang berkaitan dengan aplikasi, *e-voting*, serta algoritma *vigenere cipher*. Adapun literatur yang digunakan meliputi buku, artikel, *paper*, jurnal, makalah, internet dan sumber lainnya.

2. Analisis dan Perancangan

Pada tahap ini dilakukan analisis spesifikasi aplikasi dan melakukan perancangan aplikasi, seperti perancangan proses dan antarmuka yang meliputi desain database, sketsa, dan lain sebagainya.

3. Pengkodean

Pada tahap ini dilakukan pengkodean aplikasi sesuai dengan analisis spesifikasi dan perancangan yang telah ditentukan.

4. Pengujian Aplikasi

Pada tahap ini dilakukan pengujian terhadap aplikasi yang telah dibangun, dan tingkat keakuratan dari sistem aplikasi yang telah dibuat.

5. Penyusunan Laporan

Pada tahap ini dilakukan penulisan dokumentasi dan laporan dari aplikasi yang dikembangkan.

1.6 Sistematika Penulisan

Sistematika penulisan tugas skripsi ini dibagi atas beberapa bab, di mana masing-masing bab dibagi atas beberapa sub agar mempermudah penjelasan mengenai penelitian yang dilakukan dan mempermudah pembaca dalam memahami isi penelitian. Adapun sistematika penulisan tugas skripsi ini adalah sebagai berikut:

BAB 1 PENDAHULUAN

Pendahuluan berisi tentang latar belakang masalah, rumusan masalah, tujuan, manfaat, batasan masalah, metodologi penelitian dan sistematika penulisan dalam pembuatan tugas skripsi.

BAB 2 TINJAUAN PUSTAKA

Bab ini berisi teori-teori pengetahuan dasar yang di peroleh dari studi kepustakaan atau literatur dan dokumentasi *internet* yang digunakan untuk memahami permasalahan yang dibahas pada penelitian ini. Teori–teori pengetahuan dasar yang disajikan antara lain tentang aplikasi, *e-voting*, serta algoritma *vigenere cipher*.

BAB 3 METODE PENELITIAN

Bab ini menguraikan tahapan-tahapan sistematis yang digunakan untuk melakukan kajian penelitian. Tahapan-tahapan tersebut merupakan kerangka yang dijadikan pedoman penelitian untuk mencapai tujuan yang telah ditetapkan. Tahapan tersebut dimulai

dari waktu dan tempat penelitian serta alat dan bahan yang digunakan dalam aplikasi *e-voting* pemilihan kepala desa di Kecamatan Barus, Kabupaten Tapanuli Tengah.

BAB 4 HASIL DAN PEMBAHASAN

Bab ini berisi tentang hasil dan pembahasan dari aplikasi *e-voting* pemilihan kepala desa di Kecamatan Barus, Kabupaten Tapanuli Tengah yang telah dibuat.

BAB 5 KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan dari keseluruhan uraian bab–bab penulisan skripsi dan saran yang diajukan untuk pengembangan lebih lanjut.

BAB II

TINJAUAN PUSTAKA

2.1 Pengertian Aplikasi

Menurut (Maimunah et al., 2017) Aplikasi merupakan program yang dikembangkan untuk memenuhi kebutuhan pengguna dalam menjalankan pekerjaan tertentu. Sedangkan menurut (Fauzi Siregar et al., 2018) "aplikasi adalah alat terapan yang difungsikan secara khusus dan terpadu sesuai kemampuan yang dimilikinya aplikasi merupakan suatu perangkat komputer yang siap pakai bagi *user*".

2.2 Pengertian Web

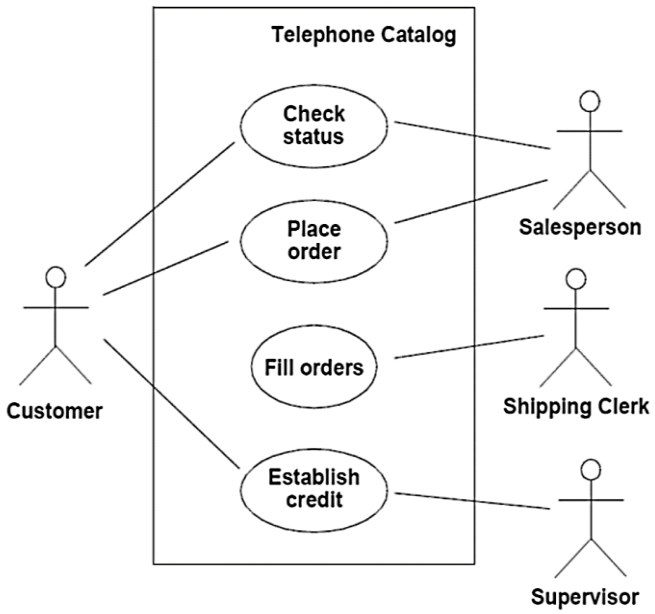
Menurut Rohi Abdulloh dalam (Ibnu Sa'ad, 2020), *website* atau web adalah sekumpulan halaman yang terdiri dari beberapa halaman yang berisi informasi berupa teks, gambar, video, audio, dan data digital animasi lainnya yang disediakan melalui koneksi internet. Pada dasarnya *website* adalah halaman yang dapat diakses oleh browser dan berisi informasi yang dapat memberikan informasi yang berguna bagi pengguna.

2.3 UML (*Unified Modeling Language*)

UML (*Unified Modeling Language*) merupakan bahasa pemodelan perangkat lunak yang telah distandarisasi sebagai media penulisan untuk cetak biru (*blueprints*) perangkat lunak. UML dapat digunakan untuk visualisasi, spesifikasi, konstruksi dan beberapa dokumentasi sistem yang ada dalam perangkat lunak. UML digunakan untuk membantu *programmer* atau *developer*

dalam membuat dan membangun *software* atau perangkat lunak (Sumiati et al., 2021). Berdasarkan penjelasan (Mulyani, 2016) dalam bukunya yang berjudul *Metode Analisis dan Perancangan Sistem*, diagram yang didefinisikan oleh UML (*Unified Modeling Language*) diantaranya adalah sebagai berikut:

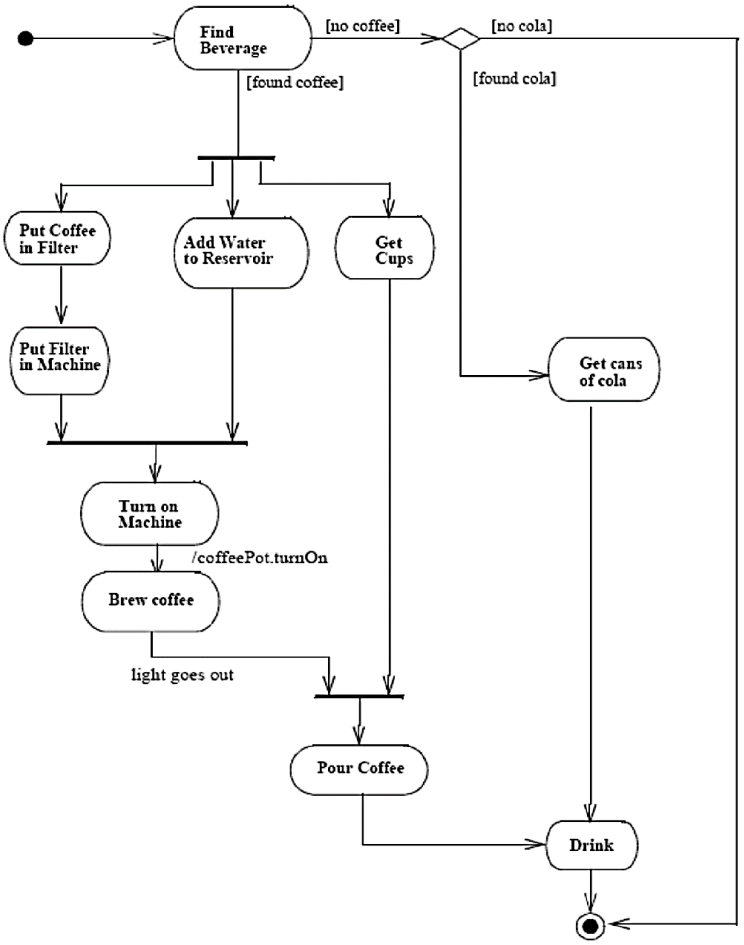
a. *Use Case Diagram*



Gambar 2.1 Contoh *Use Case Diagram*

Use case diagram merupakan diagram yang menggambarkan dan mewakili aktor, *use cases*, dan *dependencies* dari sebuah proyek. Tujuan dari diagram ini adalah untuk menggambarkan konsep hubungan antara sistem dan dunia luar.

b. *Activity Diagram*



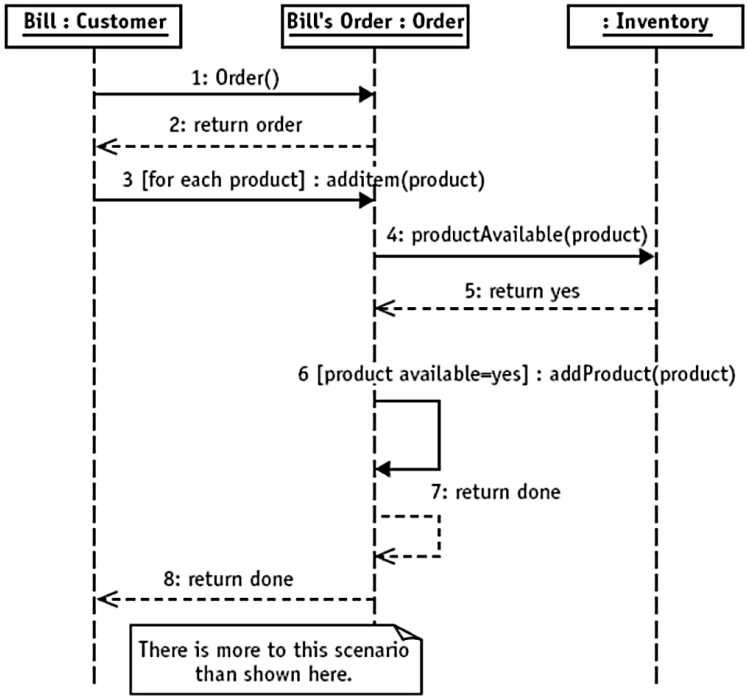
Gambar 2.2 Contoh *Activity Diagram*

Activity diagram sangat mirip dengan *flowchart*. Perbedaannya adalah *activity diagram* dapat mencabangkan aktivitas. *Activity diagram* juga memungkinkan untuk mempartisi aktivitas antar aktor. *Activity diagram* adalah diagram UML yang digunakan untuk menggambarkan aliran aktivitas dalam suatu proses. *Activity diagram* memungkinkan orang yang menjalankan proses untuk memilih urutan proses yang akan dilakukan. Dengan kata lain, diagram hanya menyebutkan seperangkat aturan dasar yang harus diikuti. Hal ini penting untuk pemodelan bisnis karena proses sering berjalan secara paralel. Dan juga berguna

dalam algoritma paralel di mana urutan independen dapat dieksekusi secara paralel.

c. *Sequence Diagram*

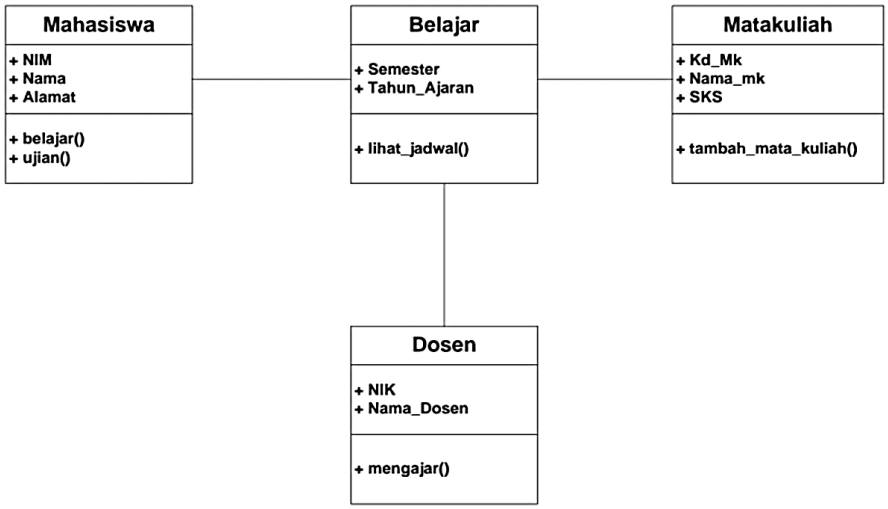
Sequence diagram adalah diagram yang menggambarkan interaksi antara beberapa objek dalam kurun waktu tertentu.



Gambar 2.3 Contoh *Sequence Diagram*

d. *Class Diagram*

Class diagram adalah keadaan suatu sistem yang jika dilakukan proses instansiasi (proses membuat objek dari kelas) akan menghasilkan objek, serta kelas merupakan inti dari pengembangan perancangan berbasis objek. *Class diagram* juga menunjukkan properti dan operasi kelas, serta batasan yang ada pada hubungan antar objek tersebut.

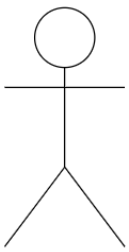
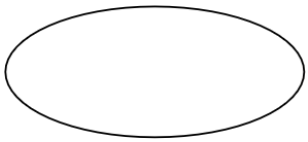


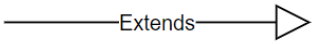
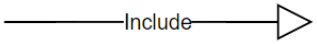
Gambar 2.4 Contoh *Class Diagram*

2.4 Daftar Simbol Diagram

a. *Use Case Diagram*

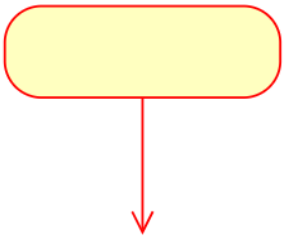
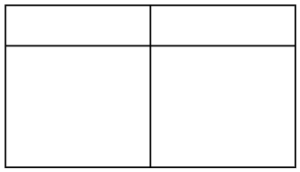
Tabel 2.1 Tabel Daftar Simbol *Use Case Diagram* (Maharani, 2018)

Simbol	Nama	Keterangan
	Actor	Menspesifikasikan himpunan peran ketika berinteraksi dengan sistem usulan.
	Use Case	Deskripsi dari urutan aksi – aksi yang ditampilkan sistem, dan mewakili sebagian besar sistem sacara fungsional.

	Sistem	Menggambarkan ruang lingkup sistem.
	Asosiasi	Menghubungkan aktor dengan use case yang berinteraksi.
	Ekstend	Relasi yang menggambarkan bahwa sebuah use case (sub use case) bisa berdiri sendiri atau bisa berjalan tanpa menjalankan main use case terlebih dahulu.
	Include	Relasi yang menggambarkan bahwa sebuah use case (sub use case) harus menjalankan use case lain terlebih dahulu sebelum menjalankan fungsinya.

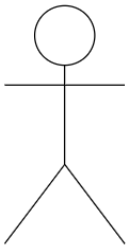
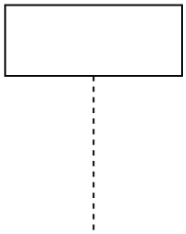
b. *Activity Diagram*

Tabel 2.2 Tabel Daftar Simbol *Activity Diagram* (Maharani, 2018)

Simbol	Nama	Keterangan
	Start Poin	Merupakan awal penelusuran. Sebuah activity diagram selalu dimulai dengan start poin
	End Point	Merupakan akhir dari penelusuran. Sebuah activity diagram selalu diakhiri dengan End Point
	Activities	Activity menggambarkan proses, disisi dengan kata kerja atau merupakan state dari sistem yang mencerminkan eksekusi dari suatu aksi.
	Swimline Style	Sebuah cara untuk mengelompokan activity berdasarkan actor. Actor bisa ditulis dengan nama actor.

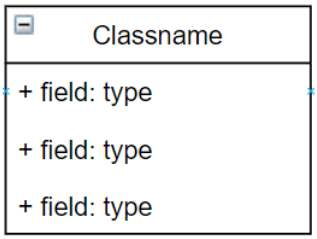
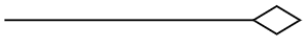
c. Sequence Diagram

Tabel 2.3 Tabel Daftar Simbol *Sequence Diagram* (Maharani, 2018)

Simbol	Nama	Keterangan
	Actor	Menspesifikasikan himpunan peran ketika berinteraksi dengan sistem usulan
	Object Lifeline	Menyatakan hidup uatu object dalam basis waktu
	Activation	Menyatakan object dalam keadaan aktif dan berinteraksi
	Message	Pesan antar object, dan menggambarkan urutan kejadian
	Message return	Menyatakan arah kembali antara urutan kejadian

d. *Class Diagram*

Tabel 2.4 Tabel Daftar Simbol *Class Diagram* (Maharani, 2018)

Simbol	Nama	Keterangan
	Class	*Class diagram* ini terdiri dari nama kelas, atribut kelas, dan metode / *operation* (fungsi yang dimiliki suatu kelas)
	Asosiasi	Menyatakan hubungan statis antar *class*, dan di simbolkan dengan garis tegas saja.
	Agregasi	Hubungan yang menyatakan terdiri atas, dimana *class* yang satu merupakan bagian dari *class* lain, namun kedua *class* ini dapat berdiri sendiri.
	Komposisi	Bentuk khusus dari agragasi dimana *class* yang menjadi bagian, baru dapat dibuat setelah *class* yang menjadi *whole* dibuat.

2.5 *E-Voting*

Electronic Voting (*E-Voting*) merupakan penggunaan teknologi komputer dalam melaksanakan pemilihan dan penghitungan suara (Sany, 2021).

Menurut (Prananda et al., 2017) *Electronic Voting* (*E-Voting*) merupakan bagian dari *electronic government* dengan hubungan G2C (*Government to Citizen*), Perkembangan ilmu pengetahuan dan teknologi (IPTEK) yang sudah selayaknya dapat dimanfaatkan untuk memajukan dan memudahkan aktivitas kebutuhan manusia.

2.6 Kriptografi

Kriptografi berasal dari bahasa Yunani, yakni *kripto* dan *grafia*, *Kripto* berarti *secret* (rahasia) dan *grafia* berarti *writing* (tulisan). Secara istilah, kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan yang dikirim dari satu tempat ke tempat lain. Dalam perkembangannya, kriptografi juga digunakan untuk mengidentifikasi keaslian pesan menggunakan tanda tangan digital dan pesan menggunakan sidik jari digital (*fingerprint*) (Mukhtar, 2018).

Sedangkan menurut (Sidik, 2018), “kriptografi adalah seni dan ilmu dalam mengamankan pesan”. Pesan dalam dunia kriptografi disebut dengan *plaintext* atau *cleartext* sedangkan pesan yang telah dienkripsi disebut *ciphertext*. Proses penyamaran pesan dan menyembunyikan konten asli disebut enkripsi sedangkan proses mengubah teks terenkripsi kembali ke *plaintext* disebut dengan dekripsi.

2.6.1 *Database*

Secara konseptual, *database* adalah kumpulan data yang membentuk satu atau lebih *file* yang berhubungan dengan langkah tertentu untuk membentuk data atau informasi baru atau dapat diartikan sebagai kumpulan data yang saling berhubungan yang diatur menurut skema atau struktur tertentu (Apryliyana et al., 2021).

Sedangkan menurut (Sunarya et al., 2018) *database* adalah adalah tempat yang berisi kumpulan data dan prosedur yang diatur dengan bantuan komputer untuk akses yang mudah dan cepat.

2.7 *Vigenere Cipher*

Menurut (Pramudya et al., 2021) *vigenere cipher* merupakan hasil dari penyederhanaan sandi substitusi polialfabetik dan terdiri dari beberapa bagian sandi *caesar* dengan proses pergeseran nilai yang berbeda. Huruf yang akan disandikan disesuaikan dengan angka, a = 0, b = 1, c = 2, …, z = 25. Kemudian tambahkan angka kata kunci dan angka pesan. Lalu hasilnya dimoduluskan dengan 26, dan hasilnya yang berupa angka tersebut dirubah ke dalam huruf untuk mendapatkan huruf yang tersandi (Lukman Sholeh & Ali Muharom, 2016).

Dalam melakukan enkripsi dan dekripsi, algoritma *vigenere cipher* dirumuskan kedalam persamaan (2.1) dan (2.2) (Musla et al., 2021).

$$C_i = (P_i + K_i)\ Mod\ 26 \quad \text{.....} \quad (2.1)$$

$$P_i = (C_i - K_i)\ Mod\ 26 \quad \text{.....} \quad (2.2)$$

Keterangan:

C_i = Nilai *ciphertext*

P_i = Nilai *plaintext*

K_i = Nilai Kunci (*key*)

Mod 26 = Modulus 26 karakter

2.7.1 Contoh Perhitungan dengan Menggunakan Algoritma *Vigenere Cipher*

Pada contoh perhitungan ini, akan dilakukan proses enkripsi dan dekripsi dengan menggunakan algoritma *vigenere cipher*. Berikut merupakan variabel yang digunakan pada contoh kasus perhitungan ini sebelum dilakukan enkripsi dan dekripsi:

Plaintext (P) = aprizaldi isnan simamora

Key (K) = good

Tabel 2.5 Tabel Posisi Alfabet

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**
0	1	2	3	4	5	6	7	8	9	10	11	12
N	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
13	14	15	16	17	18	19	20	21	22	23	24	25

1. Enkripsi

Untuk memasangkan kunci pada *plaintext* yang akan dienkripsi, maka dilakukan pemasangan *plaintext* dengan *key* yang akan digunakan.

Tabel 2.6 Tabel Pasangan *Plaintext* dengan *Key*

P	a	p	r	i	z	a	l	d	i		i	s	n	a	n		s	i	m	a	m	o	r	a
K	g	o	o	d	g	o	o	d	g		o	o	d	g	o		o	d	g	o	o	d	g	o

Dari hasil pemasangan tersebut kemudian dilakukan pencarian data alfabet pada setiap huruf yang terdapat pada *plainrext*.

P	**a**	**p**	**r**	**i**	**z**	**a**	**l**	**d**	**i**	**i**	**s**	**n**	**a**	**n**
P_i	0	15	17	8	25	0	11	3	8	8	18	13	0	13
K	**g**	**o**	**o**	**d**	**g**	**o**	**o**	**d**	**g**	**o**	**o**	**d**	**g**	**o**
K_i	6	14	14	3	6	14	14	3	6	14	14	3	6	14

P	**s**	**i**	**m**	**a**	**m**	**o**	**r**	**a**
P_i	18	8	12	0	12	14	17	0
K	**o**	**d**	**g**	**o**	**o**	**d**	**g**	**o**
K_i	14	3	6	14	14	3	6	14

Setelah masing-masing nilai *plaintext* dan nilai *key* diperoleh, maka nilai *ciphertext* dapat dihitung dengan menggunakan persamaan (2.1). Berikut merupakan perhitungan nilai *ciphertext* pada setiap huruf *plaintext* dan *key*-nya.

$C_1 = (P_1 + K_1) \bmod 26$

$C_1 = (0 + 6) \bmod 26$

$C_1 = 6 \bmod 26$

$C_1 = 6$

$C_2 = (P_2 + K_2) \bmod 26$

$C_2 = (15 + 14) \bmod 26$

$C_2 = 29 \bmod 26$

$C_2 = 3$

$C_3 = (P_3 + K_3) \bmod 26$

$C_3 = (17 + 14) \bmod 26$

$C_3 = 31 \bmod 26$

$C_3 = 5$

$C_4 = (P_4 + K_4) \bmod 26$

$C_4 = (8 + 3) \bmod 26$

$C_4 = 11 \bmod 26$

$C_4 = 11$

$C_5 = (P_5 + K_5) \bmod 26$

$C_5 = (25 + 6) \bmod 26$

$C_5 = 31 \bmod 26$

$C_5 = 5$

$C_6 = (P_6 + K_6) \bmod 26$

$C_6 = (0 + 14) \bmod 26$

$C_6 = 14 \bmod 26$

$C_6 = 14$

$C_7 = (P_7 + K_7) \bmod 26$ | $C_8 = (P_8 + K_8) \bmod 26$ | $C_9 = (P_9 + K_9) \bmod 26$

$C_7 = (11 + 14) \bmod 26$ | $C_8 = (3 + 3) \bmod 26$ | $C_9 = (8 + 6) \bmod 26$

$C_7 = 25 \bmod 26$ | $C_8 = 6 \bmod 26$ | $C_9 = 14 \bmod 26$

$C_7 = 25$ | $C_8 = 6$ | $C_9 = 14$

$C_{10} = (P_{10} + K_{10}) \bmod 26$ | $C_{11} = (P_{11} + K_{11}) \bmod 26$ | $C_{12} = (P_{12} + K_{12}) \bmod 26$

$C_{10} = (8 + 14) \bmod 26$ | $C_{11} = (18 + 14) \bmod 26$ | $C_{12} = (13 + 3) \bmod 26$

$C_{10} = 22 \bmod 26$ | $C_{11} = 32 \bmod 26$ | $C_{12} = 16 \bmod 26$

$C_{10} = 22$ | $C_{11} = 6$ | $C_{12} = 16$

$C_{13} = (P_{13} + K_{13}) \bmod 26$ | $C_{14} = (P_{14} + K_{14}) \bmod 26$ | $C_{15} = (P_{15} + K_{15}) \bmod 26$

$C_{13} = (0 + 6) \bmod 26$ | $C_{14} = (13 + 14) \bmod 26$ | $C_{15} = (18 + 14) \bmod 26$

$C_{13} = 6 \bmod 26$ | $C_{14} = 27 \bmod 26$ | $C_{15} = 32 \bmod 26$

$C_{13} = 6$ | $C_{14} = 1$ | $C_{15} = 6$

$C_{16} = (P_{16} + K_{16}) \bmod 26$ | $C_{17} = (P_{17} + K_{17}) \bmod 26$ | $C_{18} = (P_{18} + K_{18}) \bmod 26$

$C_{16} = (8 + 3) \bmod 26$ | $C_{17} = (12 + 6) \bmod 26$ | $C_{18} = (0 + 14) \bmod 26$

$C_{16} = 11 \bmod 26$ | $C_{17} = 18 \bmod 26$ | $C_{18} = 14 \bmod 26$

$C_{16} = 11$ | $C_{17} = 18$ | $C_{18} = 14$

$C_{19} = (P_{19} + K_{19}) \bmod 26$ | $C_{20} = (P_{20} + K_{20}) \bmod 26$ | $C_{21} = (P_{21} + K_{21}) \bmod 26$

$C_{19} = (12 + 14) \bmod 26$ | $C_{20} = (14 + 3) \bmod 26$ | $C_{21} = (17 + 6) \bmod 26$

$C_{19} = 26 \bmod 26$ | $C_{20} = 17 \bmod 26$ | $C_{21} = 23 \bmod 26$

$C_{19} = 0$ | $C_{20} = 17$ | $C_{21} = 23$

$C_{22} = (P_{22} + K_{22}) \bmod 26$

$C_{22} = (0 + 14) \bmod 26$

$C_{22} = 14 \bmod 26$

$C_{22} = 14$

Sehingga diperoleh nilai *ciphertext* dan *ciphertext*-nya adalah sebagai berikut:

C_i	**6**	**3**	**5**	**11**	5	**14**	**25**	**6**	**14**		**22**	**6**	16	**6**	**1**
C	g	d	f	l	f	o	z	g	o		w	g	q	g	b

C_i	**6**	**11**	**18**	**14**	**0**	**17**	**23**	**14**
C	g	l	s	o	a	r	x	o

Maka, hasil dari enkripsi *plaintext* “aprizaldi isnan simamora” dengan kunci “good” adalah “gdflfozgo wgqgb glsoarxo”.

2. Dekripsi

Pada tahap dekripsi ini, akan dicoba melakukan dekripsi dari hasil enkripsi yang telah dilakukan. Maka:

Ciphertext (C) = gdflfozgo wgqgb glsoarxo

Key (K) = good

Tabel 2.7 Tabel Pasangan *Ciphertext* dengan *Key*

C	g	d	f	l	f	o	z	g	o		w	g	q	g	b		g	l	s	o	a	r	x	o

K	g	o	o	d	g	o	o	d	g		o	o	d	g	o		o	d	g	o	o	d	g	o

Dari hasil pemasangan tersebut kemudian dilakukan pencarian data alfabet pada setiap huruf yang terdapat pada *ciphertext*.

C	**g**	**d**	**f**	**l**	**f**	**o**	**z**	**g**	**o**		**w**	**g**	**q**	**g**	**b**
C_i	6	3	5	11	5	14	25	6	14		22	6	16	6	1
K	**g**	**o**	**o**	**d**	**g**	**o**	**o**	**d**	**g**		**o**	**o**	**d**	**g**	**o**
K_i	6	14	14	3	6	14	14	3	6		14	14	3	6	14

C	**g**	**l**	**s**	**o**	**a**	**r**	**x**	**o**
C_i	6	11	18	14	0	17	23	14
K	**o**	**d**	**g**	**o**	**o**	**d**	**g**	**o**
K_i	14	3	6	14	14	3	6	14

Setelah masing-masing nilai *ciphertext* dan nilai *key* diperoleh, maka nilai *plaintext* dapat dihitung dengan menggunakan persamaan (2.2). Berikut merupakan perhitungan nilai *plaintext* pada setiap huruf *ciphertext* dan *key*-nya.

$P_1 = (C_1 - K_1) \bmod 26$

$P_1 = (6 - 6) \bmod 26$

$P_1 = 0 \bmod 26$

$P_1 = 0$

$P_2 = (C_2 - K_2) \bmod 26$

$P_2 = (3 - 14) \bmod 26$

$P_2 = -11 \bmod 26$

$P_2 = 15$

$P_3 = (C_3 - K_3) \bmod 26$

$P_4 = (C_4 - K_4) \bmod 26$

$P_3 = (5 - 14) \bmod 26$

$P_3 = -9 \bmod 26$

$P_3 = 17$

$P_4 = (11 - 3) \bmod 26$

$P_4 = 8 \bmod 26$

$P_4 = 8$

$P_5 = (C_5 - K_5) \bmod 26$

$P_5 = (5 - 6) \bmod 26$

$P_5 = -1 \bmod 26$

$P_5 = 25$

$P_6 = (C_6 - K_6) \bmod 26$

$P_6 = (14 - 14) \bmod 26$

$P_6 = 0 \bmod 26$

$P_6 = 0$

$P_7 = (C_7 - K_7) \bmod 26$

$P_7 = (25 - 14) \bmod 26$

$P_7 = 11 \bmod 26$

$P_7 = 11$

$P_8 = (C_8 - K_8) \bmod 26$

$P_8 = (6 - 3) \bmod 26$

$P_8 = 3 \bmod 26$

$P_8 = 3$

$P_9 = (C_9 - K_9) \bmod 26$

$P_9 = (14 - 6) \bmod 26$

$P_9 = 8 \bmod 26$

$P_9 = 8$

$P_{10} = (C_{10} - K_{10}) \bmod 26$

$P_{10} = (22 - 14) \bmod 26$

$P_{10} = 8 \bmod 26$

$P_{10} = 8$

$P_{11} = (C_{11} - K_{11}) \bmod 26$

$P_{11} = (6 - 14) \bmod 26$

$P_{11} = -8 \bmod 26$

$P_{11} = 18$

$P_{12} = (C_{12} - K_{12}) \bmod 26$

$P_{12} = (16 - 3) \bmod 26$

$P_{12} = 13 \bmod 26$

$P_{12} = 13$

$P_{13} = (C_{13} - K_{13}) \bmod 26$

$P_{13} = (6 - 6) \bmod 26$

$P_{13} = 0 \bmod 26$

$P_{13} = 0$

$P_{14} = (C_{14} - K_{14}) \bmod 26$

$P_{14} = (1 - 14) \bmod 26$

$P_{14} = -13 \bmod 26$

$P_{14} = 13$

$P_{15} = (C_{15} - K_{15}) \bmod 26$

$P_{15} = (6 - 14) \bmod 26$

$P_{15} = -8 \bmod 26$

$P_{15} = 18$

$P_{16} = (C_{16} - K_{16}) \bmod 26$

$P_{16} = (11 - 3) \bmod 26$

$P_{16} = 8 \bmod 26$

$P_{16} = 8$

$P_{17} = (C_{17} - K_{17}) \bmod 26$

$P_{17} = (18 - 6) \bmod 26$

$P_{17} = 12 \bmod 26$

$P_{17} = 12$

$P_{18} = (C_{18} - K_{18}) \bmod 26$

$P_{18} = (14 - 14) \bmod 26$

$P_{18} = 0 \bmod 26$

$P_{18} = 0$

$P_{19} = (C_{19} - K_{19}) \bmod 26$

$P_{19} = (0 - 14) \bmod 26$

$P_{19} = -14 \bmod 26$

$P_{19} = 12$

$P_{20} = (C_{20} - K_{20}) \bmod 26$

$P_{20} = (17 - 3) \bmod 26$

$P_{20} = 14 \bmod 26$

$P_{20} = 14$

$P_{21} = (C_{21} - K_{21}) \bmod 26$

$P_{21} = (23 - 6) \bmod 26$

$P_{21} = 17 \bmod 26$

$P_{21} = 17$

$P_{22} = (C_{22} - K_{22}) \bmod 26$

$P_{22} = (14 - 14) \bmod 26$

$P_{22} = 0 \bmod 26$

$P_{22} = 0$

Sehingga diperoleh nilai *plaintext* dan *plaintext*-nya adalah sebagai berikut:

P_i	**0**	**15**	**17**	**8**	**25**	**0**	**11**	**3**	**8**		**8**	**18**	13	**0**	**13**
P	a	p	r	i	z	a	l	d	i		i	s	n	a	n

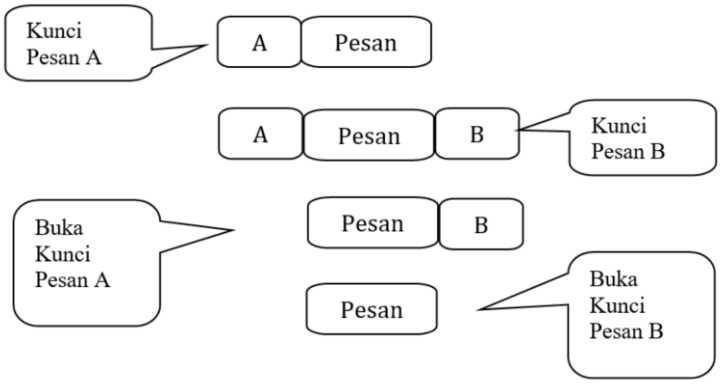
P_i	**18**	**8**	**12**	**0**	**12**	**14**	**17**	**0**
P	s	i	m	a	m	o	r	a

Maka, hasil dari dekripsi *ciphertext* “gdflfozgo wgqgb glsoarxo” dengan kunci “good” adalah “aprizaldi isnan simamora”.

2.8 *Three Pass Protocol*

Dikembangkan oleh Adi Shamir sekitar tahun 1980, konsep dasar dari *three pass protocol* adalah setiap pihak memiliki kunci enkripsi atau *private key* dan *private decryption* (Oktaviana & Utama Siahaan, 2016). *Three pass protocol* memungkinkan satu pihak untuk mengirim pesan dengan aman ke pihak lain tanpa bertukar atau mendistribusikan kunci enkripsi. Disebut dengan *three pass protocol* karena terdapat tiga pertukaran untuk mengotentikasi pengirim dan penerima dari protokol pertama (Oktaviana & Utama Siahaan, 2016).

Sedangkan menurut (Khasanah et al., 2020) *three pass protocol* adalah konsep pengiriman informasi yang memungkinkan pengirim mengirim pesan dengan aman ke penerima menggunakan kunci si pengirim dan penerima mendekripsi pesan terenkripsi menggunakan kunci si penerima.



Gambar 2.5 Gambaran Skema *Three Pass Protocol* (Sulaiman et al., 2020)

Dengan menerapkan *three pass protocol*, privasi dapat dicapai tanpa distribusi lanjutan dari kunci rahasia (*secret key*) yang menjamin penerima tidak dapat merusak atau mengutak-atik pesan tetapi membiarkan penerima untuk membaca semua pesan yang telah dikirimkan.

2.9 Penelitian Terkait

1. (Oktaviana & Utama Siahaan, 2016)

Penelitian yang dilakukan oleh (Oktaviana & Utama Siahaan, 2016) adalah tentang *Three-Pass Protocol Implementation in Caesar Cipher Classic Cryptography* tahun 2016.

Metode Penelitian : *Three pass protocol* dengan menggunakan algoritma kriptografi *caesar cipher*

Hasil Penelitian : Hasil dari kombinasi algoritma kriptografi *caesar cipher* dan *three pass protocol* adalah mampu memastikan bahwa informasi yang dikirimkan aman.

Kesimpulan : Kombinasi enkripsi *caesar cipher* dengan *three pass protocol* menghasilkan *ciphertext* yang terjamin. Proses pengiriman data tidak perlu lagi membagikan kunci ke pengirim pesan. Kriptografi klasik yang dianggap rentan terhadap serangan masih bisa digunakan.

2. (Khasanah et al., 2020)

Penelitian yang dilakukan oleh (Khasanah et al., 2020) adalah tentang *Three-pass Protocol Scheme on Vigenere Cipher to Avoid Key Distribution* tahun 2020.

Metode Penelitian : *Three pass protocol* dengan menggunakan algoritma kriptografi *vigenere cipher*.

Hasil Penelitian : Dengan menerapkan algoritma *vigenere cipher* dan skema *three-pass protocol*, keamanan data menjadi lebih terjamin.

Kesimpulan : Skema *three pass protocol* bekerja dengan menggunakan dua kunci yang berbeda dalam proses enkripsi dan dekripsi. Pengirim dan penerima tidak perlu bertukar atau memberikan kunci untuk menggunakan algoritma *vigenere cipher*. Proses enkripsi dilakukan dengan menambahkan ASCII *plaintext* 1 dan *ciphertext* 1 dengan kunci 1. Proses dekripsi dilakukan dengan mengurangi ASCII *ciphertext* 2 dan *ciphertext* 3 dengan kunci 2. Algoritma yang digunakan pada pengirim dan penerima adalah algoritma

vigenere cipher karena algoritma ini adalah semacam algoritma kriptografi klasik, sehingga lebih mudah untuk menghitung skema *three pass protocol*.

3. (Sulaiman et al., 2020)

Penelitian yang dilakukan oleh (Sulaiman et al., 2020) adalah tentang *Three Pass Protocol untuk Keamanan Kunci Berbasis Base64 pada XOR Cipher* tahun 2020.

Metode Penelitian : *Three pass protocol* dengan menggunakan algoritma XOR *cipher* dan algoritma *encoding* dan *decoding* bit dalam teks yaitu Base 64.

Hasil Penelitian : Enkripsi Base64 dengan XOR *cipher* memiliki kelemahan pada skema *three pass protocol* karena proses enkripsi standar Base64 mudah diketahui orang lain.

Kesimpulan : Dengan menggunakan *three pass protocol* dapat menambahkan lapisan keamanan pada saat pertukaran kunci, sehingga sulit untuk mengetahui kuncinya. Karena sifat Base64 mudah di *encoding* dan *decoding* sehingga pengembangan lanjutan dapat menggunakan algoritma kriptografi pada saat pertukaran kunci *three pass protocol*.