BAB I

PENDAHULUAN

I.1. Latar Belakang

MySQL merupakan *Relational Database Management System* (RDBMS) yang menggunakan bahasa SQL (*Structured Query Language*). MySQL ini adalah *database* yang bersifat, artinya bebas digunakan oleh siapa saja tanpa harus wajib mendapatkan lisensinya. MySQL juga merupakan *database* yang dapat diakses dari jalur manapun, baik dari *client* ataupun dari *server*. (Yunita dan Sunardi, 2017 : 60). Dengan kebebasan penggunaan ini yang menjadikan MySQL rentan terhadap pencuri data, MySQL hanya menerapkan keamanan berupa sandi untuk akses pengelolaan data sehingga tidak ada keamanan data pada isi basis datanya. Masalah yang bisa saja terjadi adalah adanya pihak dalam (pemegang akses data) merusak isi basis data karena tidak merasa puas dengan pendapatan dipekerjaannya atau pihak luar sebagai pencuri data untuk mendapatkan keuntungan.

Oleh karena itu peneliti merekomendasikan teknik kriptografi untuk merahasiakan isi dari basis data MySQL. Kriptografi berasal dari bahasa Yunani yaitu *kriptos* yang berarti tersembunyi dan *graphein* yang berarti tulisan, sehingga kriptografi diartikan sebagai ilmu yang digunakan untuk menyembunyikan pesan. Teknik ini sudah dikenal lebih dari 3000 tahun yang lalu dimana pertama kali digunakan oleh bangsa Sparta dari Yunani dalam bidang militer. (Sari, dkk, 2016 :

181). Dalam penggunaan kriptografi dibutuhkan sebuah metode untuk dapat mengubah isi pesan menjadi rahasia

Berdasarkan penelitian yang dilakukan oleh Sihombing (2019) mengenai Penerapan Algoritma Vernam Cipher (One Time) Untuk Pengamanan Login, Sihombing menyimpulkan bahwa aplikasi dapat mengacak dan menyembunyikan *file* dengan aman dan tidak menimbulkan kecurigaan pada pihak lain.

Berdasarkan penelitian yang dilakukan oleh Sutoyo, dkk (2019) mengenai Implementasi Super Enkripsi Algoritma One Time Pad (OTP) Dan Beaufort Cipher Untuk Mengamankan Data, Sutoyo, dkk menyimpulkan bahwa dengan menggunakan algoritma *one time pad* dan kombinasi algoritma *beaufortcipher* maka keamanan *file* teks menjadi bertambah.

Dari kedua penelitian terdahulu yang menggunakan meode *vernam cipher* untuk menyelesaikan masalah kerahasiaan data maka peneliti menggunakan metode *vernam cipher*. *Vernam cipher* merupakan algoritma kriptografi yang ditemukan oleh Mayor J. Maugborne dan G. Vernam. Algoritma Vernam *cipher* diadopsi dari *one time pad cipher*, dimana dalam hal ini karakter diganti dengan bit (0 atau 1). Dengan kata lain, *vernam cipher* merupakan versi lain dari *one-time pad cipher*. Algoritma kriptografi *vernam cipher* merupakan algoritma kriptografi berjenis *symmetric key*. Kunci yang digunakan untuk melakukan enkripsi dan dekripsi menggunakan kunci yang sama. Dalam melakukan proses enkripsi, algoritma vernam *cipher* menggunakan cara *stream cipher* dimana *cipher* berasal dari hasil operasi XOR antara bit *plainteks* dan *bit key*. (Juneidi, dkk, 2016 : 22). Namun dalam penggunaan *vernam cipher* terdapat kekurangan yaitu jika pesan

dan kunci yang digunakan bernilai sama, maka *vernam cipher* tidak dapat memberikan hasil, oleh karena itu peneliti menambahkan metode *caesar cipher* untuk menghindari terjadinya kekosongan hasil dari metode *vernam cipher*. *Caesar Cipher* merupakan salah satu jenis *cipher* substitusi yang membentuk *cipher* dengan cara melakukan penukaran satu karakter diganti dengan karakter yang berada di sejumlah digit sebelah kanan atau kirinya, tergantung arah pergeserannya. (Putri, dkk, 2019 : 87). Dengan adanya metode *vernam cipher* yang dikombinasikan dengan metode *caesar cipher* maka basis data MySQL mendapatkan kerahasiaan data yang lebih baik Berdasarkan latar belakang tersebut maka peneliti menyimpulkan judul **"Kerahasiaan Isi Teks Basis Data MySQL Menggunakan Metode Vernam Cipher Dan Caesar Cipher (Studi Kasus : Pelangi Toys)".**

I.2. Ruang lingkup Permasalahan

Ruang lingkup permasalahan yang dijabarkan untuk penelitian ini adalah sebagai berikut :

I.2.1. Identifikasi Masalah

Identifikasi masalah dari latar belakang yang telah dijelaskan adalah sebagai berikut :

1. Basis data MySQL rentan terhadap pencurian informasi.
2. Belum terdapat penerapan metode *vernam cipher* dan *caesar cipher* untuk merahasiakan isi teks basis data MySQL.
3. Diperlukan aplikasi yang dapat merahasiakan isi basis data MySQL.

I.2.2. Perumusan Masalah

Perumusan masalah pada penelitian ini yaitu :

1. Bagaimana agar basis data MySQL tidak rentan terhadap pencurian informasi ?
2. Bagaimana menerapkan metode *vernam cipher* dan *caesar cipher* untuk merahasiakan isi teks basis data MySQL ?
3. Bagaimana menghasilkan aplikasi Kerahasiaan Isi Teks Basis Data MySQL Menggunakan Metode *Vernam Cipher* Dan *Caesar Cipher* ?

I.2.3. Batasan Masalah

Batasan masalah yang terdapat pada penelitian ini berdasarkan latar belakang yang telah dijabarkan adalah sebagai berikut :

1. Aplikasi hanya untuk merahasiakan basis data MySQL.
2. Aplikasi hanya dapat berjalan pada sistem operasi *windows*.
3. *Input* aplikasi ini berupa teks isi basis data MySQL.
4. *Output* aplikasi ini berupa teks isi basis data MySQL yang terenkripsi.
5. Pembuatan Aplikasi ini menggunakan bahasa pemrograman Visual Basic 2010.
6. Perancangan Aplikasi ini menggunakan pemodelan UML.
7. Metode yang digunakan adalah *vernam cipher*.

I.3. Tujuan Dan Manfaat

I.3.1. Tujuan

Adapun tujuan penelitian ini adalah sebagai berikut :

1. Agar basis data MySQL tidak rentan terhadap pencurian informasi.

2. Menerapkan metode *vernam cipher* dan *caesar cipher* untuk merahasiakan isi teks basis data MySQL.
3. Menghasilkan aplikasi Kerahasiaan Isi Teks Basis Data MySQL Menggunakan Metode *Vernam Cipher* Dan *Caesar Cipher*.

I.3.2. Manfaat

Manfaat dari penelitian ini adalah sebagai berikut :

1. Isi teks *database* MySQL mendapatkan kerahasiaan data yang lebih baik.
2. Mengetahui dan memahami penerapan metode *vernam cipher* dan *caesar cipher* dalam merahasiakan isi teks basis data MySQL.
3. Mendapatkan wawasan dalam pembuatan perangkat lunak kriptografi.

BAB II

TINJAUAN PUSTAKA

II.1. Penelitian Terdahulu

Berdasarkan penelitian yang dilakukan oleh Aulia, dkk (2019) mengenai Penerapan Algoritma One Time Pad & Linear Congruential Generator Untuk Keamanan Pesan Teks, Aulia, dkk menyimpulkan bahwa tingkat kemanan pesan dapat dikatakan cukup karena menggunakan dua metode.

Berdasrkan penelitian yang dilakukan oleh Eka (2018), mengenai Implementasi Keamanan Data Menggunakan Algoritma *Vernam Cipher* Dan *Playfair Cipher*, Eka menyimpulkan bahwa plainteks yang diinputkan akan menjadi diacak sehingga tidak dapat dimengerti.

Berdasarkan penelitian yang dilakukan oleh Jumeidi, dkk (2016), mengenai Implementasi Algoritma Kriptografi *Vernam Cipher* Berbasais FPGA, Jumeidi, dkk menyimpulkan bahwa proses enkripsi dan dekripsi dilakukan dengan menggunakan implementasi sistem dari rancangan sistem yang sama.

Berdasarkan penelitian yang dilakukan oleh Sihombing (2019) mengenai Penerapan Algoritma Vernam Cipher (One Time) Untuk Pengamanan Login, Sihombing menyimpulkan bahwa aplikasi dapat mengacak dan menyembunyikan *file* dengan aman dan tidak menimbulkan kecurigaan pada pihak lain.

Berdasarkan penelitian yang dilakukan oleh Sutoyo, dkk (2019) mengenai Implementasi Super Enkripsi Algoritma One Time Pad (OTP) Dan Beaufort Cipher Untuk Mengamankan Data, Sutoyo, dkk menyimpulkan bahwa dengan

menggunakan algoritma *one time pad* dan kombinasi algoritma *beaufortcipher* maka keamanan *file* teks menjadi bertambah.

Berdasarkan penelitian yang dilakukan oleh Nataliana, dkk (2019) mengenai Rancang Bangun Sistem Keamanan RFID Tag menggunakan Metode Caesar Cipher pada Sistem Pembayaran Elektronik, Nataliana, dkk (2019) menyimpulkan bahwa Metode Ceasar Cipher dapat digunakan sebagai algoritma untuk proses enkripsi dan dekripsi dengan pemetaan nilai setiap karakter melalui tabel ASCII.

Berdasarkan penelitian yang dilakukan oleh Putri, dkk (2019) mengenai Penerapan Kriptografi Caesar Cipher Pada Fitur Chatting Sistem Informasi Freelance, Putri, dkk (2019) menyimpulkan bahwa metode *cipher* ini berjenis *cipher* substitusi, dimana setiap huruf pada *plaintext*nya digantikan dengan huruf lain yang tetap pada posisi *alphabet*, jadi kemungkinan dapat dipecahkan dengan cara *brute force attack*, suatu bentuk serangan yang dilakukan dengan mencoba-coba berbagai kemungkinan untuk menemukan kunci.

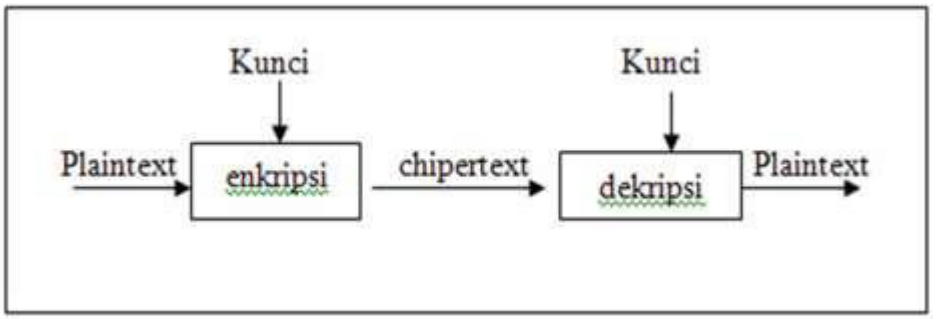
II.2. Landasan Teori

Beberapa landasan teori yang dikutip dari beberapa referensi penelitian yang berkaitan dengan penelitian ini yaitu :

II.2.1. Kriptografi

Kriptografi berasal dari bahasa Yunani yaitu *kriptos* yang berarti tersembunyi dan *graphein* yang berarti tulisan, sehingga kriptografi diartikan sebagai ilmu yang digunakan untuk menyembunyikan pesan. Teknik ini sudah

dikenal lebih dari 3000 tahun yang lalu dimana pertama kali digunakan oleh bangsa Sparta dari Yunani dalam bidang militer. (Sari, dkk, 2016 : 181).



Gambar II.1. Alur Kerja Kriptografi
(Sari, dkk, 2016 : 181)

Berdasarkan Gambar II.1, terdapat beberapa istilah penting untuk melakukan proses kriptografi. *Plaintext* yaitu data asli yang akan disandikan menjadi bentuk lain yang tidak diletahui oleh orang lain. Bentuk *plaintext* beraneka ragam berdasarkan media yang digunakan antara lain: teks, gambar, suara, video maupun IP protokol. Untuk mengubah menjadi bentuk lain plainteks memerlukan sebuah kunci. Kunci tersebut dapat berbentuk angka maupun tulisan. Media kriptografi yang dapat digunakan hingga saat ini dapat dibagi menjadi 5 yaitu teks, gambar, audio, video dan protokol IP**.** (Sari, dkk, 2016 : 181).

II.2.1.1. Tujuan Kriptografi

Secara umum terdapat 5 tujuan dilakukannya kriptografi, antara lain: (a) kerahasiaan yaitu informasi hanya dapat diakses oleh pihak yang berhak sehingga kerahasiaan harus dijaga; (b) otentikasi, dalam hal ini terdapat dua jenis otentikasi: otentikasi pesan berarti pesan yang diterima harus sama seperti pesan yang dikirimkam sedangkan otentikasi entitas *user* berarti pihak yang diajak berkomunikasi merupakan pihak yang benar-benar dikehendaki; (c) integritas

merupakan keaslian pesan yang dikirim, (d) anti penolakan merupakan bukti bahwa seseorang telah mengirimkan pesan, (e) ketersediaan yaitu adanya sumber daya dari sistem komputer untuk mengakses oleh pihak yang berhak pada saat dibutuhkan. (Sari, dkk, 2016 : 181).

II.2.1.2. Jenis-Jenis Kriptografi

Kriptografi berdasarkan jenis kunci yang digunakan dapat digolongkan menjadi 3 yaitu kriptografi kunci simetris, kriptografi kunci asimetris dan kriptografi kunci *hybrid* (gabungan dari simetris dan asimetris). Pertama, kriptografi kunci simetris yaitu kriptografi yang dalam operasi enkripsi dan dekripsnya menggunakan kunci yang sama, dikenal sebagai *private key*. Contoh kriptografi kunci simetris yaitu DES *(Data Encyption Standard)*, 3DES, IDEA, *Blowfish*, *Twofish*, *Shift Cipher*, *Hill Cipher*, *Vernam cipher* dan AES (*Advanced Encryption Standard*). Kedua, kriptografi kunci asimetris yaitu kriptografi yang dalam operasi enkripsi dan dekripsinya menggunakan 2 buah kunci berbeda yang disebut dengan kunci privat dan kunci publik. Contoh dari kriptografi kunci asimetris yaitu RSA (Riverst Shamir Adleman), DSA (*Digial Signature Algorithm*), ECC (*Elliptic Curve Cryptography*), DH (*Deffie Hellman*) dan El-Gamal. Ketiga, kriptografi kunci gabungan simetris dan asimetris yaitu kriptografi yang menggunakan model persetujuan dari kedua belah pihak baik pengirim maupun penerima, dimana *session key* digunakan untuk mengenkripsi percakapan maupun mengenkripsi pertukaran data yang terjadi. Dalam hal ini setiap *session key* hanya dapat digunakan satu kali saja sehingga untuk sesi selanjutnya harus dibuat *session key* yang baru. (Sari, dkk, 2019 : 182).

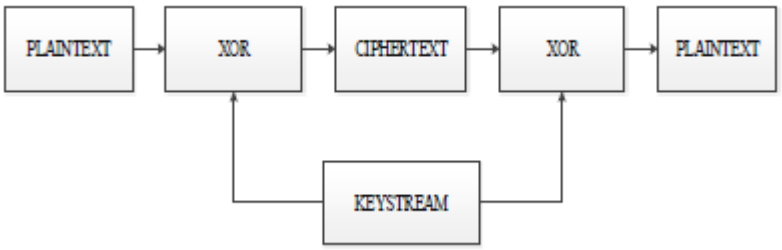
II.2.2. Kerahasiaan

Secrecy bermakna kerahasiaan atau privasi. Hal tersebut berarti setiap informasi yang dikirim atau diterima hanya dapat diakses oleh pihak yang berkepentingan. Enkripsi pesan bertujuan untuk tetap merahasiakan pesan sampai kepada penerima dengan aman. Selanjutnya pesan yang telah diterima akan didekripsi oleh penerima dengan algoritma yang telah disepakati dan kunci yang telah dikirimkan dengan jalur yang lebih aman. (Sutoyo, dkk : 2019 : 3).

II.2.3. Metode *One Time Pad* (*Vernam Cipher*)

Vernam cipher merupakan algoritma kriptografi yang ditemukan oleh Mayor J. Maugborne dan G. Vernam. Algoritma Vernam *cipher* diadopsi dari *one time pad cipher*, dimana dalam hal ini karakter diganti dengan bit (0 atau 1). Dengan kata lain, vernam *cipher* merupakan versi lain dari *one-time pad cipher*. Algoritma kriptografi vernam *cipher* merupakan algoritma kriptografi berjenis *symmetric key*. Kunci yang digunakan untuk melakukan enkripsi dan dekripsi menggunakan kunci yang sama. Dalam melakukan proses enkripsi, algoritma vernam *cipher* menggunakan cara *stream cipher* dimana *cipher* berasal dari hasil operasi XOR antara bit *plainteks* dan *bit key*.

Pada *cipher* aliran, bit hanya mempunyai dua buah nilai, sehingga proses enkripsi hanya menyebabkan dua keadaan pada bit tersebut, yaitu berubah atau tidak berubah. Dua keadaan tersebut ditentukan oleh kunci enkripsi yang disebut dengan aliran-bit-kunci (*keystream*). Secara sederhana proses enkripsi dan dekripsi algoritma vernam *cipher* dapat adalah pada Gambar II.2.



Gambar II.2. Proses Enkripsi Dan Dekripsi Algoritma Kriptografi *Vernam Cipher*
(Juneidi, dkk, 2016 : 22)

II.2.4. *Caesar Cipher*

Ceasar Cipher adalah sebuah metode enkripsi paling pertama ditemukan dan digunakan oleh Julius Ceasar dan tentaranya pada saat terjadi perang Gaul tahun 50 SM. Cara kerja dari algoritma ini ialah dengan memanfaatkan proses substitusi ke dalam sebuah surat, kalimat atau kumpulan kata-kata sehingga terbentuk sebuah kumpulan huruf yang tidak dapat dimengerti oleh siapapun.

Caesar Cipher merupakan salah satu jenis *cipher* substitusi yang membentuk *cipher* dengan cara melakukan penukaran satu karakter diganti dengan karakter yang berada di sejumlah digit sebelah kanan atau kirinya, tergantung arah pergeserannya. (Putri, dkk, 2019 : 87).

a. Persamaan Enkripsi

Persamaan enkripsi untuk mengubah pesan asli menjadi pesan rahasia menggunakan rumus sebagai berikut :

$$\mathbf{C_x = P_x + K \bmod 26}$$

b. Persamaan Dekripsi

Persamaan dekripsi untuk mengubah pesan asli menjadi pesan rahasia menggunakan rumus sebagai berikut :

$P_x = C_x$ - K mod 26

Dengan C_x adalah nilai desimal karakter ciphertext (data terenkripsi) ke-i, Px adalah nilai desimal karakter plaintext (data asli) ke-i, k adalah nilai desimal karakter key (kunci) ke-i dan mod 26 adalah modulus dari jumlah karakter alfabet yaitu 26. (Nataliana, dkk, 2019 : 429).

II.2.5. *Visual Basic* 2010

Visual basic 2010 adalah inkarnasi dari bahasa Visual Basic yang sangat populer dan telah dilengkapi dengan fitur serta fungsi yang setara dengan bahasa tingkat tinggi lainnya seperti C++. *Visual Basic* dapat digunakan untuk membuat aplikasi *Windows*, *mobile*, *web*, dan *office* yang kompleks dengan menggunakan kode yang anda tulis, atau kode yang telah ditulis oleh orang lain dan kemudian dimasukkan ke dalam program. (Putri dan Putra, 2018 : 52).

II.2.6. MySQL

MySQL merupakan *Relational Database Management System* (RDBMS) yang menggunakan bahasa SQL (*Structured Query Language*). MySQL ini adalah *database* yang bersifat, artinya bebas digunakan oleh siapa saja tanpa harus wajib mendapatkan lisensinya. MySQL juga merupakan *database* ini dapat diakses dari jalur manapun, baik dari *client* ataupun dari *server*. (Yunit dan Sunardi, 2017 : 60).

II.2.7. *Unified Modeling Language* (UML)

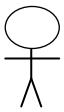
UML yaitu satu kumpulan konvensi permodelan yang digunakan untuk menentukan atau menggambarkan sebuah sistem perangkat lunak yang terkait dengan objek. UML merupakan suatu kumpulan teknik terbaik yang telah terbukti sukses dalam memodelkan system yang besar dan kompleks. UML tidak hanya digunakan dalam proses pemodelan perangkat lunak, namun hampir dalam semua bidang yang membutuhkan pemodelan. (Andikos, 2019 : 39).

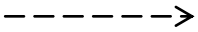
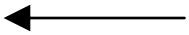
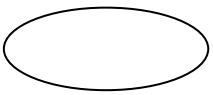
Alat bantu yang digunakan dalam perancangan berorientasi objek berbasiskan UML adalah sebagai berikut :

1. *Use Case* Diagram

Use case diagram menggambarkan fungsionalitas yang diharapkan dari sebuah sistem. Yang ditekankan adalah "apa" yang diperbuat sistem, dan bukan "bagaimana". Sebuah use case merepresentasikan sebuah interaksi antara aktor dengan sistem.use case diagram dapat digambarkan dengan sumber-sumber pada Tabel II.1.

Tabel II.1. Simbol *Use Case*

Gambar	Nama	Keterangan
	*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

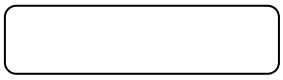
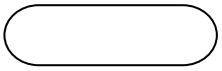
		besar dari jumlah dan elemen-elemennya (sinergi).
	*Note*	Elemen fisik yang eksis saat aplikasi dijalankan dan mencerminkan suatu sumber daya komputasi

(Sumber : Andikos, 2019 : 39)

2. Diagram Aktivitas (*Activity Diagram*)

Activity diagram menggambarkan berbagai alir aktivitas dalam sistem yang sedang dirancang, bagaimana masing-masing alir berawal, *decision* yang mungkin terjadi, dan bagaimana mereka berakhir. *Activity diagram* juga dapat menggambarkan proses paralel yang mungkin terjadi pada beberapa eksekusi. *Activity diagram* dapat digambarkan dengan simbol-simbol seperti pada tabel II.2.

Tabel II.2. Simbol *Activity Diagram*

Gambar	Nama	Keterangan
	*Activity*	Memperlihatkan bagaimana masing-masing kelas antarmuka saling berinteraksi satu sama lain.
	*Action*	State sistem yang mencerminkan eksekusi suatu aksi.

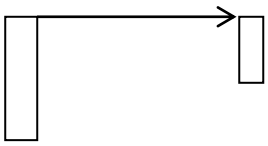
	*Initial Node*	Bagaimana objek dibentuk atau diawali.
	*Activity Final*	Bagaimana objek dibentuk dan dihancurkan
	*Fork Node*	Satu aliran yang pada tahap tertentu berubah menjadi beberapa aliran

(Sumber : Andikos, 2019 : 39)

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*

Gambar	Nama	Keterangan
	*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.

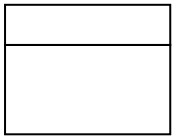
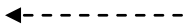
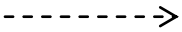
(Sumber : Andikos, 2019 : 39)

4. *Class Diagram* (Diagram Kelas)

Class adalah sebuah spesifikasi yang jika diinstansiasi akan menghasilkan sebuah objek dan merupakan inti dari pengembangan dan desain berorientasi objek. *Class diagram* menggambarkan struktur dan deskripsi class, package dan objek beserta hubungan satu sama lain seperti *containment*, pewarisan, asosiasi, dan lain-lain. Class diagram dapat digambarkan dengan simbol-simbol seperti pada Tabel II.4.

Tabel II.4. *Class Diagram*

Gambar	Nama	Keterangan
	Generalization	Hubungan dimana objek anak (*descendent*) berbagi perilaku dan struktur data dari objek yang ada di atasnya objek induk (ancestor).
	*Nary Association*	Upaya untuk menghindari asosiasi dengan lebih dari 2 objek.

	*Class*	Himpunan dari objek-objek yang berbagi atribut serta operasi yang sama.
	*Collaboration*	Deskripsi dari urutan aksi-aksi yang ditampilkan sistem yang menghasilkan suatu hasil yang terukur bagi suatu actor
	*Realization*	Operasi yang benar-benar dilakukan oleh suatu objek.
	*Depedency*	Hubungan dimana perubahan yang terjadi pada suatu elemen mandiri akan mempegaruhi elemen yang bergantung padanya elemen yang tidak mandiri
	Assocation	Apa yang menghubungkan antara objek satu dengan objek lainnya

(Sumber : Andikos, 2019 : 39)

2.5.1 *Web Server*

Salah satu protokol aplikasi paling populer yang digunakan di Internet adalah *HTTP*. *HTTP* adalah singkatan dari "Hypertext Transfer Protocol." *HTTP* adalah protokol aplikasi yang berjalan di atas protokol *TCP / IP*. Seluruh *World Wide Web* menggunakan protokol ini. Ketika *user* membuka halaman *web*, *browser* mungkin telah mengirim lebih dari 40 permintaan *HTTP* dan menerima respon *HTTP*. *Header HTTP* adalah bagian inti dari permintaan dan respon *HTTP* ini, dan membawa informasi tentang browser klien, halaman yang diminta, *server*, dan lainnya. Seperti yang diilustrasikan dalam gambar 2, klien *HTTP* mengirim pesan permintaan ke *server HTTP*. *Server*, pada gilirannya, mengembalikan pesan tanggapan. (Muhammad Ravis, Gian Muhammad, dkk 2019)

2.5.2 *PHP (Hypertext Preprocessor)*

Menurut Agus Saputra *PHP* merupakan suatu bahasa pemograman yang difungsikan untuk membangun suatu web dinamis. *PHP* menyatu dengan kode *HTML*, maksudnya adalah dengan beda kondisi. *HTML* digunakan sebagai pembangun atau pondasi dari kerangka layout web, sedangkan *PHP* difungsika sebagai prosesnya sehingga dengan adanya *PHP* tersebut, sebuah *web* akan sangat mudah di *maintenance.* (Agus Ramdhani Nugraha, Gati Pramukasari 2017)

2.5.3 *HTML*

Menurut Achmad Solichin, *HTML* (*Hypertext Markup Language)* merupakan bahasa pemograman *web* yang memberitahukan peramban *web (web browser)* bagaimana

menyusun dan menyajikan konten di halaman *web*. Dengan kata lain *HTML* adalah pondasi *web*. (Agus Ramdhani Nugraha, Gati Pramukasari 2017)

2.5.4 *MySQL*

MySQL adalah sebuah implementasi dari sistem manajemen basisdata relasional (*RDBMS*) yang didistribusikan secara gratis. Setiap pengguna dapat secara bebas menggunakan *MySQL*, namun dengan batasan perangkat lunak tersebut tidak boleh dijadikan produk turunan yang bersifat komersial. *MySQL* sebenarnya merupakan turunan salah satu konsep utama dalam basisdata yang telah ada sebelumnya; *SQL* (*Structured Query Language*). *SQL* adalah sebuah konsep pengoperasian basisdata, terutama untuk pemilihan atau seleksi dan pemasukan data, yang memungkinkan pengoperasian data dikerjakan dengan mudah secara otomatis. (Ramadhan Susilo Utomo, Arief Laila Nugraha, dkk. 2020)

Menurut Adi Nugroho *MySQL* (*My Structured Query Language*) adalah: " Suatu sistem basis data *relation* atau *Relational Database managemnt System (RDBMS)* yang mampu bekerja secara cepat dan mudah digunakan *MySQL* juga merupakan program pengakses database yang bersifat jaringan, sehingga sapat digunakan untuk aplikasi *multi user* (banyak pengguna). *MySQL* didistribusikan gratis dibawah lisensi *GPL* (*General Public License*). Dimana setiap program bebas menggunakan *MySQL* namun tidak bisa dijadikan produk turunan yang dijadikan *closed source* atau komersial". (Mara Destiningrum, Qadhli Jafar Adrian 2017)

2.5.5 *Notepad++*

Notepad++ adalah sebuah penyunting teks dan penyunting kode sumber yang berjalan di sistem operasi windows. *Notepad++* menggunakan komponen Scintilla untuk menampilkan dan mengedit teks maupun berkas kode sumber beragam bahasa pemrograman. (Muhammad Saed Novendri, Ade Saputra, dkk. 2019)

2.5.6 *Google Maps API*

Google Maps API merupakan aplikasi *interface* yang dapat diakses lewat *javascript* agar *Google Maps* dapat ditampilkan pada halaman *web* yang sedang kita bangun. Untuk dapat mengakses *Google Maps* kita harus melakukan pendaftaran *API Key* terlebih dahulu dengan data pendaftaran berupa nama *domain web* yang kita bangun dan untuk versi yang sekarang tidak perlu menggunakan *API Key*. Banyak sekali kegunaan *Google Maps* untuk *website* yang kita buat diantaranya dapat digunakan untuk menampilkan lokasi pemilik *website* (pada *about us*), lokasi *event/*kegiatan, atau dapat juga digunakan untuk aplikasi SIG berbasis *web*. (Sylvia Tri Yuliani, Bambang Sudarsono, dkk. 2016)

Menurut Fauzan masykur "Google Maps API adalah suatu library yang berbentuk java script". Menurut Enggar Kusuma. M dan Yanto Budisusanto "*Google Maps* API merupakan aplikasi antarmuka yang dapat diakses melalui javascript agar Google Maps dapat ditampilkan pada web yang sedang dibangun." (Chaidir Kurnia Thoullah, Agnia Bilqisti, dkk. 2019)

2.5.7 *XAMPP*

XAMPP merupakan singkatan dari X (empat sistem operasi apapun), *Apache, MySQL, PHP, Perl*. *XAMPP* adalah *tool* yang menyediakan paket perangkat lunak dalam satu buah paket. *XAMPP* adalah paket *PHP* yang berbasis *Open Source* yang dikembangkan oleh sebuah komunitas *Open Source*. Dengan menggunakan *XAMPP* tidak perlu lagi bingung untuk melakukan penginstalan program-program yang lain, karena semua kebutuhan telah disediakan oleh *XAMPP*. (Sylvia Tri Yuliani, Bambang Sudarsono, dkk. 2020)

XAMPP menurut Betha Sidik (Daniel Dido Jantce TJ Sitinjak, Maman, dkk 2020) *XAMPP* adalah singkatan yang setiap huruf adalah:

1. **X:** Program ini dapat dijalankan di banyak sistem operasi, seperti *Windows*, *Linux*, *Mac* OS, dan Solaris.
2. **A:** ***Apache,*** *server* aplikasi *Web*. *Apache* tugas utama adalah untuk menghasilkan halaman *web* yang benar kepada pengguna terhadap kode *PHP* yang sudah dituliskan oleh pembuat halaman *web*. Jika perlu kode *PHP* juga berdasarkan yang tertulis, dapat d*atabase* diakses dulu (misalnya MySQL) untuk mendukung halaman *web* yang dihasilkan.
3. **M:** ***MySQL***, server aplikasi *database*. Pertumbuhannya disebut *SQL* singkatan dari *Structured Query Language*. *SQL* merupakan bahasa terstruktur yang difungsikan untuk mengolah *database*. *MySQL* dapat digunakan untuk membuat dan mengelola *database* dan isinya. Bisa juga memanfaatkan *MySQL* guna untuk menambahkan, mengubah, dan menghapus data dalam *database*.

4. **P: *PHP***, bahasa pemrograman *web*. Bahasa pemrograman *PHP* adalah bahasa pemrograman untuk membuat *web* yang *server-side scripting*. *PHP* digunakan untuk membuat halaman *web* dinamis. Sistem manajemen *database* yang sering digunakan dengan *PHP* adalah *MySQL*. Namun PHP juga mendukung Pengelolaan sistem *database Oracle, Microsoft Access, Interbase, d-base, PostgreSQL,* dan sebagainya.
5. **P: *Perl,*** bahasa pemrograman untuk semua tujuan, pertama kali dikembangkan oleh *Larry Wall*, mesin *UNIX*. *Perl* dirilis pertama kali tanggal 18 Desember 1987 yang ditandai dengan keluarnya Perl 1. Pada versi-versi selanjutnya, Perl juga tersedia untuk berbagai sistem operasi *UNIX (SunOS, Linux, BSD, HP-UX),* juga tersedia untuk sistem operasi seperti *DOS, Windows, PowerPC, BeOS, VMS, EBCDIC,* dan *PocketPC.* Menurut Pratama, I Putu Agus Eka (2014: 440) "XAMPP adalah aplikasi *web server* bersifat instan (siap saji) yang dapat digunakan baik di sistem operasi Linux maupun di sistem operasi Windows. Menurut Hidayatullah (2015:127), "XAMPP merupakan *web server* yang mudah digunakan yang dapat melayani tampilan halaman *web* yang dinamis dan dapat diakses secara lokal menggunakan *web server local* (*localhost*)". Purbadian (2016:1), menjelaskan bahwa "XAMPP merupakan suatu *software* yang bersifat *open source* yang merupakan pengembangan dari LAMP (Linux, Apache, MySQL, PHP dan Perl)". Menarik kesimpulan dari beberapa pendapat para ahli bahwa XAMPP adalah perangkat pembantu yang menyediakan alat untuk sebagai jembatan pembuatan sebuah program.

BAB III

METODOLOGI PENELITIAN

III.1. Pengumpulan Data

Berikut ini adalah beberapa teknik pengumpulan data yang peneliti lakukan untuk melengkapi bahan penelitian :

1. Sampel

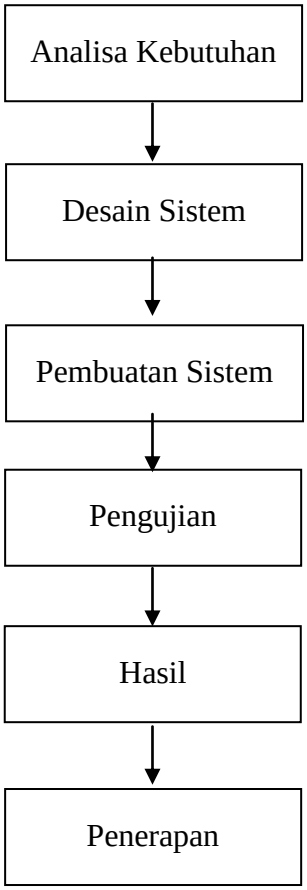
   Peneliti mengambil beberapa sampel penelitian yang berkaitan dengan penelitian ini yaitu aplikasi kriptografi dan contoh beberapa aplikasi didalam jurnal

2. Pustaka

   Peneliti menggunakan buku, jurnal dan karya ilmiah sebagai referensi dan landasan teori pada penelitian ini.

III.2. *Diagram* Tahapan Penelitian

Penelitian ini akan melalui beberapa tahapan. Tahapan dalam penelitian ini dapat di modelkan pada diagram tahapan penelitian. Adapun beberapa tahapan yang digunakan dalam penelitian ini adalah sebagai berikut :



Gambar III.1. Diagram *Fish Bone* Metodologi Penelitian

Keterangan :

1. Analisa Kebutuhan

Pada tahapan ini merupakan analisa terhadap kebutuhan yang diperlukan untuk mencapai tujuan penelitian yang akan dilakukan. Pada tahap ini dilakukan pengumpulan data-data teori mengenai data basis data dan data kriptografi.

2. Desain Sistem

Desain sistemyang digunakan dalam teori adalah pemodelan UML yaitu *use case diagram*, *class diagram*, *activity diagram* dan *sequence diagram*.

3. Pembuatan Sistem

Pada tahapan ini peneliti menggunakan *visual basic* 2010, MySQL, laptop dan sistem operasi *windows* dalam pembuatan sistem.

4. Pengujian

Pada tahapan ini peneliti menguji sistem yang telah dibuat menggunakan pengujian teori dan praktek. Pengujian teori peneliti menggunakan *blackbox testing* dan pengujian praktek peneliti menggunakan *visual basic* 2010.

5. Hasil

Pada tahapan ini penelitian sudah selesai dibuat, hasil dari penelitian ini yaitu Aplikasi Modifikasi Metode One Time Pad +3 Menggunakan Keystream Generator Yang Diterapkan Untuk Kerahasiaan Data MySQL.

6. Penerapan

Pada tahapan ini hasil yang telah dicapai diterapkan pada kasus yang sebenarnya sehingga dapat membuktikan manfaatnya secara langsung.