BAB I PENDAHULUAN

A. Latar Belakang Masalah

Teknologi sudah masuk ke abad 21 ini dan dimana teknologi menjadi hal yang sudah lumrah bahkan hampir semua manusia di dalam nya dapat menggunakan serta sudah mengetahui segala tentang hal yang ada sangkut-pautnya dengan Teknologi. Dengan begitu banyak pula hal yang telah berubah dan berkembang. Dari mulai dari cara berkomunikasi, berinteraksi, bertranportasi, berbisnis, pendidikan dan masih banyak lainnya. Teknologi sekarang bukan hanya di gunakan oleh pihak Industri saja. Melainkan dari lembaga pemerintah, perusahaan, serta individual. Dengan kemajuan teknologi yang berkembang pesat serta kurangnya adaptasi dalam memberikan arahan serta sosialisasi dari beberapa pihak kepada masyarakat umum membuat terjadinya beberapa kasus yang telah dilakukan oleh beberapa oknum yang tidak bertanggung jawab. Kasus-kasus yang sering terjadi dalam menggunakan teknologi yaitu Cyber Crime atau dunia kejahatan dalam internet. Banyak kasus-kasus sering terjadi dalam Cyber Crime, dimulai dari marak nya kasus perampokan dan pembajakan dalam data maupun informasi serta bahkan perampokan keuangan dalam dunia maya. Para pelaku sering disebut dengan Hacker, Cracker dan sebagai nya. Data yang sering terkena adalah data-data penting dan hanya beberapa orang tertentu yang dapat mengakses nya. Dan data penting yang telah di curi disebar luaskan di dunia maya. Sungguh sesuatu yang sangat merugikan.

Saat bidang pendidikan tengah menerapkan teknologi untuk ujian sekolah. Dikarenakan ujia dengan sistem kertas serta manual serta pembagian soal ujian hanya lewat kertas serta dibagikan dari pusat ke sekolah dianggap tidak efektif serta kurang optimal. Belum lagi terhitung banyak kasus tentang bocornya kunci jawaban yang tersebar kepada para murid-murid yang hendak akan mengerjakan ujian sekolah. Belum lagi dalam biaya untuk sistem ujian manual di anggap banyak meraup biaya anggaran negara. Dalam proses menerapkan sistem teknologi dalam ujian sekolah tengah dalam pengembangan.

Meskipun ujian sekolah saat ini telah menggunakan ilmu teknologi dengan sistem berbasis komputer. Langkah ini diambil agar memangkas nya dana anggaran negara serta untuk mengoptimalkan kinerja sekolah dalam bidang pemerintah. Akan tetapi masalah yang baru adalah sistem pengamanannya, sistem keamanan dalam mengamankan data penting ini sangat perlu ditingkatkan kembali. karena terjadi juga beberapa kasus juga yang pernah terjadi yaitu masih bocornya kunci jawaban ujian sekolah.

Maka peningkatan keamanan pada sebuah data dan informasi penting sangat lah diperlukan oleh pemiliki data itu agar tidak bocor bahkan jatuh ke dalam tangan seseorang yang tidak bertanggung jawab lalu terjadinya pencurian data bahkan bocornya ke pihak luar hingga membuat kerugian besar bagi pemilik data itu. Namun. Setelah kasus-kasus kejahatan yang sering merajarela sekarang ini tidak membuat banyak para pemilik data penting menghiraukannya. Sehingga ini dapat menjadi kesempatan bagi para pelaku kejahatan untuk melakukan kejahatan nya kembali. Lalu pengamanan atau sekuritas seperti apa yang harus dan dapat digunakan untuk mengamankan data yang penting. Seperti yang diketahui bahwa pengamanan data atau sekuritas data dapat dilakukan dengan Enkripsi data. Enkripsi data adalah salah satu bidang dalam ilmu Kriptografi.

Seperti yang telah diketahui bahwa Enkripsi merupakan proses mengamankan informasi dengan membuatnya tak dapat di baca tanpa adanya pengetahuan khusus tentang enkripsi tersebut. Dengan sistem yang seperti itu enkripsi telah di gunakan untuk mengamankan komunikasi di berbagai negara, dan juga organisasi organisasi maupun individu yang memiliki kepentingan mendesak yang memakainya.

dari bahasa Yunani, Kriptografi (cryptography), terdiri dari dua suku kata yaitu kripto dan graphia. Kripto artinya menyembunyikan, sedangkan graphia artinya tulisan. Menjadikan Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data .Tetapi tidak semua aspek keamanan informasi dapat diselesaikan dengan kriptografi. Kriptografi dapat pula diartikan sebagai ilmu atau seni untuk menjaga keamanan pesan.

Kriptografi sendiri memiliki 4 komponen utama yaitu: Plaintext, yaitu pesan yang dapat dibaca Ciphertext, yaitu pesan acak yang tidka dapat dibaca Key, yaitu kunci untuk melakukan teknik kriptografi Algorithm, yaitu metode untuk melakukan enkrispi dan dekripsi Kemudian, proses yang akan dibahas dalam artikel ini meliputi 2 proses dasar pada Kriptografi yaitu: Enkripsi (Encryption) Dekripsi (Decryption) dengan key yang digunakan sama untuk kedua proses diatas. Penggunakan key yang sama untuk kedua proses enkripsi dan dekripsi ini disebut juga dengan Secret Key, Shared Key atau Symetric Key Cryptosystems.

Dalam menggunakan metode ini dapat membuat orang lain tidak dapat mengetahui dan memahami lagi data yang dimiliki. Jadi dapat mencegah serta mengatasi bocor nya informasi data penting dari tangan para orang yang tidak bertanggung jawab. Metode ini juga sudah sangat banyak yang menggunakan nya dalam mengaman kan data. Jadi rasa keraguan dalam menggunakan metode dan cara ini dapat teratasi. Akan tetapi bukan

berarti metode dan cara ini tanpa ada kelemahan. Kelemahan terbesar dalam metode ini adalah dari namanya dan cara kerja nya. Karena jika seseorang menggunakan cara metode ini yaitu menggunakan metode kriptografi dalam mengamankan data nya. Maka orang lain akan curiga dan akan segera mencari tahu nya serta mencoba meretas data penting yang di enkripsi kan karena diduga mereka data ini data yang penting dan sangat rahasia yang akan membuat mereka merasa terpuaskan bahkan akan membuat mereka merasa akan menguntungkan jika dapat meretas hingga mencuri data yang di enkripsi kan menggunakan kriptografi.

Teknik dalam kriptografi sangat lah dibutuhkan dalam pengamanan data.mengapa sangat penting?.

Karena algoritma kriptografi merupakan seni dalam merahasiakan informasi data dimulai dari perhitungan matematika yang akurat, perkembangannya yang pesat. Dan dengan menggunakan pola-pola tertentu. Dengan begitu sesuatu yang berkaitan dengan “seni” pengamanan data sangat kental dengan teknik algoritma kriptografi. karena banyak dalam mengamankan data. Algoritma yang sering digunakan dalam mengamankan data adalah Advance Encryption Server (AES), Hill Cipher, Md5 serta masih banyak lainnya. Akan tetapi dalam penelitian kali ini metode yang akan digunakan adalah algoritma kriptografi caesar cipher.

diketahui Caesar Cipher merupakan salah satu algoritma cipher tertua dalam perkembangan ilmu kriptografi. Caesar cipher juga merupakan salah satu jenis cipher substitusi yang membentuk cipher dengan cara melakukan penukaran karakter pada plainteks menjadi tepat satu karakter pada chiperteks. Teknik seperti ini disebut juga sebagai chiper abjad tunggal.

Algoritma kriptografi Caesar Cipher sangat mudah untuk digunakan. Inti dari algoritma kriptografi ini adalah melakukan pergeseran terhadap semua karakter pada plaintext dengan nilai pergeseran yang sama.

Dengan adanya aplikasi keamanan data ini diharapkan terciptanya prosedur instansi lebih dalam menyimpan dan mengirimkan suatu data atau pesan, salah satu instansi yang akan menerapkan aplikasi keamanan data yaitu SMK INDIKA KOTA BOGOR merupakan salah satu sekolah swasta menengah kejuruan yang ada di Kota Bogor, oleh karena nya itu sangat perlu diterapkan aplikasi kriptografi keamanan data untuk meminimalisir pencurian atau kehilangan data agar tidak dapat dilihat atau diketahui oleh orang lain kecuali si pemilik data tersebut, dalam mengimplementasikan aplikasi kriptografi keamanan data dengan

caesar chiper adalah dengan microsoft visual studio (VB.Net) karena memiliki keunggulan opensource yaitu gratis tanpa perlu membayar lisensi software

Berdasarkan permasalahan dan penelitian sebelumnya didalam peneletian ini dilakukan aplikasi

B. Permasalahan

Dalam Proses data Ujian di SMK INDIKA KOTA BOGOR belum adanya pengamanan data sehingga ada bocornya data soal yang diujikan. Dari permasalahan diatas perlunya kebutuhan teknologi dalam pengamanan soal data

kelemahan dari sekolah belum adanya prose pengamanan data secara komputer (enkripsi-deksripsi) sehingga adanya kerawanan pencurian atau kehilangan data

. Berikut ini adalah tabel bukti kehilangan data ujian disekolah sekolah yaitu :

Tabel 1.1 Mata pelajaran yang bocor

NO	MATA PELAJARAN	TAHUN AJARAN	JUMLAH
1	Matematika, Bhs Inggris	2017-2018	2
2	Akuntansi Perbankan Syariah	2018-2019	1
3	Ekonomi Islam	2016-2017	1

Sistem Ujian Sekolah menggunakan teknologi berbasis komputer saat ini sedang dalam pengembangan dan hanya beberapa sekolah saja yang baru menerapkan nya. Karena terkait dalam biaya dan ketersediaan sarana yang mendukung. Ketika sarana pendukung telah tersedia dan sekolah-sekolah telah memenuhi syarat untuk mengikuti serta menerapkan ujian sekolah menggunakan berbasis komputer. Akan tetapi masih ada masalah yang perlu diperhatikan. Yaitu pengamanan data ujian itu sendiri. Maka Enkripsi data ujian sekolah mulai di perhatikan serta diterapkan agar tidak bocor nya kunci jawaban serta soal yang akan di uji kan.

1. Identifikasi Masalah

Permasalahan yang daat diidentifikasi adalah :

a. Belum aman dalam penyimpanan data ujian sekolah
b. Belum amannya proses dalam pengamanan data ujian sekolah

2. Rumusan Masalah

a. Problem statement

Belum tersedianya aplikasi pengamanan file basis data untuk mengamankan data ujian sekolah

b. Research Question

1) Bagaimana penerapan metode Caesar Chiper dapat digunakan untuk Enkripsi data Ujian Sekolah.?
2) Seberapa aman dan efektif penerapan metode Caesar Chiper dalam Enkripsi data Ujian Sekolah.?

C. Maksud Dan Tujuan Penelitian

1. Maksud

Menerapkan metode Caesar Chiper untuk mengamankan data ujian sekolah yang dibuat oleh guru-guru

2. Tujuan

Tujuan dari penelitian yang akan didapat adalah:

a. Memberikan pengamanan pada penyimpanan data
b. Mendapatkan proses pengamanan data ujian sekolah yang lebih baik
c. Mengembangkan prototipe aplikasi enkripsi soal dengan menerapkan metode caesar ciper
d. Mengukur tingkat keamanan penerapan caesar ciper untuk enkripsi data

D. Spesifikasi Produk Yang Diharapkan

Produk yang diharapkan dalam pengembangan ini adalah aplikasi enkripsi soal ujian diharapkan dapat mengamankan soal ujian dan kerahasiaan soal. dalam mengenkripsi soal menerapkan metode Kriptografi Caesar Chiper Aplikasi berbasis dekstop. Data yang sama sebelum maupun sesudah di enkripsi atau di deskripsi

E. Signifikasi Penelitian

Dalam rangka penelitian ini adalah untuk menciptakan sebuah teknik dalam mengamankan data dan mengengkripsikan dengan penerapan metode Caesar Chiper pada data ujian sekolah dengan adanya aplikasi ini ada beberapa manfaat diantaranya:

1. Manfaat Teoritis yaitu: Hasil dari penelitian ini dapat menjadi landasan dalam pengembangan aplikasi kriptografi dan penelitian ini masih dapat di kembangkan
2. Manfaat Praktis
   a. Bagi sekolah (Instansi/Lembaga), hasil penelitian ini dapat menghasilkan sebuah pengamanan data soal ujian di sekolah Sehingga dapat secara aman tersimpan
   b. Bagi Akademik, hasil dari penelitian ini dapat menjadi contoh nyata pembelajaran, pemahaman dan penguasaan secara teori maupun praktik
   c. Bagi Penulis, hasil penelitian ini diharapkan mampu menerapkan ilmu tentang kriptografi yang telah dipelajari di perkuliahan
3. Manfaat Kebijakan Aplikasi kriptografi keamanan data ini dapat dijadikan sebagai acuan dalam pengelolaan keamanan data yang ada di sekolah.

F. Asumsi Dan Keterbatasan Pengembangan

1. Asumsi

Asumsi pengembangan dalam penelitian ini yaitu:

a. Tersedianya pengamanan data yang di peroleh dari Enkripsi data
b. Penggunaan Metode Kriptografi Caesar Chiper untuk Enkripsi dalam pengaman data lebih optimal.

2. Keterbatasan

Keterbatasan pengembangan dalam penelitian ini yaitu:

a. Proses enkripsi akan lambat.
b. Penelitian ini ditujukan untuk sistem keamanan saja yang ditujukan pada guru di sekolah bukan untuk tidak digunakan umum.

G. Definisi istilah

1. Enkripsi

   Enkripsi adalah proses mengamankan informasi

2. Caesar Cipher

   algoritma cipher tertua dan paling diketahui dalam perkembangan ilmu kriptografi adalah Caesar Chiper.

3. Data

   Data merupakan kumpulan fakta.

4. Kriptografi

   diartikan sebagai ilmu atau seni untuk menjaga keamanan

5. Plaintext

   Plaintext adalah pesan yang tidak dapat dibaca sembarangan

6. Key

   Key adalah kunci untuk melakukan sebuah eknripsi