BAB I

PENDAHULUAN

1.1. Latar Belakang Masalah

Kriptografi adalah suatu ilmu yang mempelajari tentang bagaimana cara menjaga agar data atau pesan tetap aman saat dikirimkan, dari pengirim ke penerima tanpa mengalami gangguan apapun dari pihak ketiga. Dengan perkembangan teknologi yang begitu pesat memungkinkan manusia dapat berkomunikasi dan saling bertukar informasi/data secara jarak jauh. Antar kota antar wilayah antar negara bahkan antar benua bukan merupakan suatu kendala lagi dalam melakukan komunikasi dan pertukaran data. Seiring dengan itu tuntutan akan sekuritas (keamanan) terhadap kerahasiaan informasi yang saling dipertukarkan tersebut semakin meningkat.

Begitu banyak pengguna seperti departemen pertahanan, suatu perusahaan atau bahkan individu-individu tidak ingin informasi yang disampaikannya diketahui oleh orang lain. Kegiatan menyimpan data dan mengirim data menggunakan layanan internet menuntut penggguna membangun dan merancang arsitektur jaringan keamanan yang baik. Data merupakan kegiatan yang penting dalam pemanfaatan teknologi dalam organisasi apapun.

Keamanan data yang disimpan merupakan faktor penting bagi organisasi dalam menghadapi persaingan yang semakin lama semakin beresiko, dimana data proses kerja dan administrasi organisasi disimpan dan akan diolah menjadi informasi yang penting dan bersifat rahasia bagi perkembangan organisasi. Kebutuhan untuk bertahan dan terus berkembang sebuah organisasi yang memanfaatkan teknologi informasi harus menggunakan metode kriptografi penyandian data yaitu enkripsi terhadap informasi yang di kirimkan maupun data yang tersimpan.

Algoritma AES mengamankan data yang tersimpan dalam perangkat penyimpanan data, sehingga tidak mudah hilang maupun di manfaatkan oleh orang-orang yang tidak bertanggung jawab. Algoritma AES (Advanced Encryption Standard) atau Rijndael sebagai salah satu metode kriptografi. Algoritma ini diketahui sangat unggul dalam pengenkripsian dan pendekripsian data. AES digunakan dalam berbagai penyandian. Salah satunya adalah untuk penyandian sandi lewat yang digunakan pada aplikasi pengoperasian data.

Tabel unsur periodik kimia adalah tampilan unsur-unsur kimia dalam bentuk tabel. Unsur-unsur tersebut diatur berdasarkan struktur elektronnya, sehingga sifat unsur-unsur tersebut berubah-ubah secara teratur sepanjang tabel. Setiap unsur didaftarkan berdasarkan nomor atom dan lambang unsurnya.

Berdasarkan hal tersebut, penulis ingin membuat aplikasi sistem pengenkripsian data yang menggunakan beberapa langkah dalam pengenkripsiannya dengan menggunkan tabel unsur periodik kimia sebagai chiphertextnya. Sesuai dengan topik di atas, maka untuk skripsi penyusun mengambil judul : "Mengenkripsi Pesan Menggunakan Algoritma AES Tabel Sistem Unsur Periodik Kimia".

1.2. Rumusan Masalah

Berdasarkan dari latar belakang di atas maka dapat dirumuskan masalah sebagai berikut :

1. Bagaimana membuat aplikasi pengenkripsian pesan dengan menggunakan algoritma AES?
2. Analisis jenis apa yang digunakan dalam membuat aplikasi enkripsi pesan?
3. Bagaimana desain aplikasi enkripsi pesan yang akan dirancang?
4. Bagaimana hasil implementasi dari aplikasi enkripsi yang telah dirancang?
5. Bagaimana uji coba (*testing*) aplikasi enkripsi pesan setelah dilakukan perancangan sistem?

1.3. Batasan Masalah

Dalam pembuatan aplikasi ini, terdapat beberapa pembatasan masalah, antara lain :

1. Aplikasi yang dibuat penulis ini merupakan aplikasi pengenkripsian dan pendekripsian pesan.
2. Dalam penelitian ini tidak semua tabel periodik unsur kimia dijadikan kata kunci, melainkan penulis memilih dan memilah data dengan beberapa golongan dan periode dalam tahap pengenkripsian. Berikut kata kunci (*cipherkey*) dalam mengenkripsi pesan berdasarkan tabel periodik unsur kimia dibawah ini :

Nama Unsur	Lambang	Jenis unsur	Golongan	Periode
Litium	Li	Logam alkali	IA	2
Fransium	Fr	Logam alkali	IA	7
Strontium	Sr	Alkali tanah	IIA	5
Barium	Ba	Alkali tanah	IIA	6
Indium	In	Logam	IIIA	5
Talium	Tl	Logam	IIIA	6
Germanium	Ge	Metaloid	IVA	4
Stannum	Sn	Logam	IVA	5
Kripton	Kr	Gas mulia	VIIIA	4
Radon	Rn	Gas mulia	VIIIA	6
Skandium	Sc	Logam transisi	IIIB	4

Lawrensium	Lr	Logam transisi	IIIB	7
Titanium	Ti	Logam transisi	IVB	4
Rutherfordium	Rf	Logam transisi	IVB	7
Niobium	Nb	Logam transisi	VB	5
Tantalum	Ta	Logam transisi	VB	6

Tabel 1.1. Tabel Periodik Unsur Kimia Sebagai Kunci

3. Ada beberapa unsur-unsur kimia yang tidak dimasukkan kedalam penelitian sebagai *cipher key*. Tahap ini bertujuan untuk mengetahui atau membandingkan hasil ciphertext menggunakan tabel periodik unsur kimia yang dipilih secara acak menghasilkan hasil ciphertext yang sama atau tidak dengan plaintext yang sama. Berikut unsur-unsur kimia yang tidak dienkripsi :

Nama Unsur	Lambang	Jenis unsur	Golongan	Periode
Hidrogen	H	Non logam	IA	1
Natrium	Na	Logam alkali	IA	3
Kalium	K	Logam alkali	IA	4
Rubidium	Rb	Logam alkali	IA	5
Sesium	Cs	Logam alkali	IA	5
Berilium	Be	Alkali tanah	IIA	2
Magnesium	Mg	Alkali tanah	IIA	3

Kalsium	Ca	Alkali tanah	IIA	4
Radium	Ra	Alkali tanah	IIA	7
Yodium	Y	Logam transisi	IIIB	5
Lantnum	La	Logam transisi	IIIB	6
Aktinium	Ac	Logam transisi	IIIB	7
Zirkonium	Zr	Logam transisi	IVB	5
Hafnium	Hf	Logam transisi	IVB	6
Vanadium	V	Logam transisi	VB	4
Dubnium	Db	Logam transisi	VB	7
Krom	Cr	Logam	IIIA	3
Molibden	Mo	Logam	IIIA	4
Wolfram	W	Metaloid	IVA	3
Seaborgium	Sg	Metaloid	IVA	4
Mangan	Mn	Logam	IVA	6
Teknetium	Tc	Gas mulia	VIIIA	1
Renium	Re	Gas mulia	VIIIA	2
Bohrium	Bh	Gas mulia	VIIIA	3
Ferrum	Fe	Gas mulia	VIIIA	5
Rutenium	Ru	Gas mulia	VIIIA	6
Osmium	Os	Logam transisi	IIIB	6
Hassium	Hs	Logam transisi	IIIB	7
Kobalt	Co	Logam transisi	IVB	7

Rodium	Rh	Logam transisi	VB	5
Iridium	Ir	Logam transisi	VB	6
Meitnerium	Mt	Logam transisi	VIIIB	7
Nikel	Ni	Logam transisi	VIIIB	4
Paladium	Pd	Logam transisi	VIIIB	5
Platina	Pt	Logam transisi	VIIIB	6
Cuprum	Cu	Logam transisi	IB	4
Argentum	Ag	Logam transisi	IB	5
Aurum	Au	Logam transisi	IB	6
Zinc	Zn	Logam transisi	IIB	4
Kadmium	Cd	Logam transisi	IIB	5
Hydrargyum	Hg	Logam transisi	IIB	6
Boron	B	Metaloid	IIIA	2
Aluminium	Al	Logam	IIIA	3
Galium	Ga	Logam	IIIA	4
Karbon	C	Non logam	IVA	2
Silikon	Si	Metaloid	IVA	3
Plumbum	Pb	Logam	IVA	6
Nitrogen	N	Non logam	VA	2
Posfor	P	Non logam	VA	3
Arsenik	As	Metaloid	VA	4
Stibium	Sb	Metaloid	VA	5

Bismut	Bi	Metaloid	VA	6
Oksigen	O	Non logam	VIA	2
Sulfur	S	Non logam	VIA	3
Selenium	Se	Non logam	VIA	4
Telurium	Te	Metaloid	VIA	5
Polonium	Po	Metaloid	VIA	6
Fluor	F	Halogen	VIIA	2
Klorida	Cl	Halogen	VIIA	3
Bronium	Br	Halogen	VIIA	4
Iodium	I	Halogen	VIIA	5
Astatin	At	Halogen	VIIA	6
Helium	He	Gas mulia	VIIIA	1
Neon	Ne	Gas mulia	VIIIA	2
Argon	Ar	Gas mulia	VIIIA	3
Xenon	Xe	Gas mulia	VIIIA	5
Serium	Ce	Lantanida	IIIB	6
Platina	Pr	Lantanida	IVB	6
Neodimium	Nd	Lantanida	VB	6
Prometium	Pm	Lantanida	VIB	6
Samarium	Sm	Lantanida	VIIB	6
Europium	Eu	Lantanida	VIIIB	6
Gadolinium	Gd	Lantanida	VIIIB	6

Terbium	Tb	Lantanida	VIIIB	6
Disprosium	Dy	Lantanida	IB	6
Holmium	Ho	Lantanida	IIB	6
Erbium	Er	Lantanida	IIIA	6
Tulium	Tm	Lantanida	IVA	6
Iterbium	Yb	Lantanida	VA	6
Lutetium	Lu	Lantanida	VIA	6
Torium	Th	Aktinida	IIIB	7
Protaktinium	Pa	Aktinida	IVB	7
Uranium	U	Aktinida	VB	7
Neptunium	Np	Aktinida	VIB	7
Plutonium	Pu	Aktinida	VIIB	7
Amerisium	Am	Aktinida	VIIIB	7
Kurium	Cm	Aktinida	VIIIB	7
Berkelium	Bk	Aktinida	VIIIB	7
Kalifornium	Cf	Aktinida	IB	7
Einsteinium	Es	Aktinida	IIB	7
Fermium	Fm	Aktinida	IIIA	7
Mendelevium	Md	Aktinida	IVA	7
Nobelium	No	Aktinida	VA	7

Tabel 1.2. Tabel Periodik Unsur Kimia Tidak Dienkripsi

4. Aplikasi pengenkripsian pesan ini dirancang computer PC (stand alone) serta menggunakan bahasa pemrograman java.
5. Algoritma AES yang dibahas enkripsi dan dekripsi, yaitu menyandikan plaintext menggunakan chiper key untuk menghasilkan chipertext.
6. Aplikasi ini menggunakan software pendukung java.

1.4. Tujuan Penelitian

Berikut adalah beberapa butir yang dianggap sebagai tujuan dari penelitian ini adalah :

1. Mengembangkan secara nyata teori-teori yang sudah didapat selama mengikuti perkuliahan di Stmik Amikom Yogyakarta.
2. Memperoleh pengalaman untuk menambah keterampilan dalam merancang dan mengembangkan aplikasi pengenkripsian data.
3. Membuat aplikasi pengenkripsian data sebagai aplikasi yang dapat membantu stack holder dalam mengirimkan data atau pesan singkat penting atau rahasia.
4. Dapat diterapkan dalam fitur tambahan website berbasis desktop dan mobile.

1.5. Manfaat Penelitian

Hasil penelitian ini diharapkan dapat memberikan manfaat terhadap Penulis dan pembaca, manfaat tersebut antara lain :

1. Dapat berbagi ilmu pengetahuan yang telah didapat selama belajar di STMIK AMIKOM YOGYAKARTA.
2. Menambah pengetahuan dan kemampuan dalam pembuatan sistem aplikasi kriptografi.
3. Memudahkan instansi-intansi dalam mengirimkan data atau pesan singkat yang dirahasiakan .
4. Penerapannya dalam kehidupan nyata dapat digunakan di dalam berbagai macam plattform, seperti diterapkan di dalam sistem operasi android dan tambahan fitur enkripsi pesan di dalam website.
5. Dapat menjadi bahan referensi dalam pembuatan pengenkripsian dan pendekripsian pesan kriptografi dalam penyusunan skripsi selanjutnya.

1.6.Metode Penelitian

Dalam penelitian ini penulis menggunakan beberapa metode, adapun metode dan langkah-langkah dalam penelitian ini adalah :

1. Metode Literatur

   Metode literatur ini, dapat dilakukan dengan pencarian referensi-referensi terkait, buku-buku, yang akan digunakan untuk menentukan rancangan sistem, metode yang digunakan maupun teknis pengerjaan.

2. Perancangan Program

   Dilakukan sebagai gambaran dan acuan dalam desain program selanjutnya.

3. Desain Program

   Desain yang dilakukan meliputi desain sistem dan desain grafis.

4. Uji Coba program

   Pengujian program ini dilakukan untuk memastikan bahwa aplikasi yang dibuat dengan bantuan software sudah berjalan baik sesuai dengan yang diharapkan.

5. Penyusunan Laporan

   Penulisan laporan dalam penelitian ini, dikerjakan dalam akhir penelitian sebagai penjelasan dari proses pengerjaan sistem mulai dari tahap persiapan, perancangan, pelaksanaan hingga pengujian.

1.7.Sistematika Penelitian

Ruang lingkup dalam penulisan skripsi ini meliputi persiapan, perancangan, pembuatan, pengujian dan pengaplikasiannya. Sistematika penulisan tugas akhir ini adalah sebagai berikut :

BAB I. PENDAHULUAN

Bab ini membahas tentang latar belakang masalah, pokok permasalahan, batasan masalah, tujuan penelitian, pengumpulan data dan sistematika penulisan yang disajikan secara terstruktur.

BAB II. LANDASAN TEORI

Bab ini berisi dasar-dasar teori pendukung yang digunakan untuk penganalisaan dalam melakukan penelitian. Landasan teori merupakan rangkuman hasil studi literatur yang dilakukan penulis yang digunakan dalam penulisan skripsi ini.

BAB III. ANALISIS DAN PERANCANGAN SISTEM

Menjelaskan tentang gambaran umum objek penelitian, analisis, rancangan implementasi, dan proses pembuatan.

BAB IV. IMPLEMENTASI DAN PEMBAHASAN

Bab ini menjelaskan tentang gambaran umum implementasi hasil uji coba program sistem yang berjalan, spesifikasi aplikasi, prosedur operasional, serta memaparkan analisis desain, implementasi desain, hasil testing, spesifikasi sistem komputer mengenai perangkat lunak, perangkat keras dan konfigurasi komputer yang digunakan dalam pembuatan aplikasi.

BAB V. PENUTUP

Bab terakhir berisi mengenai kesimpulan dari semua yang telah diuraikan dan saran-saran yang dianggap perlu untuk mengatasi permasalahan yang terjadi.

DAFTAR PUSTAKA

LAMPIRAN