BAB II
TINJAUAN PUSTAKA

2.1 Landasan Teori

2.1.1 Kriptografi

Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan, kriptografi juga merupakan ilmu yang mempelajari teknik-teknik matematika yang berhubungna dengan aspek keamanan informasi seperti kerahasiaan, integritas data serta otentikasi. (Benni dkk, 2014:34)

Ada empat tujuan mendasar dari ilmu kriptografi ini yang juga merupakan aspek keamanan informasi yaitu:

a) Kerahasiaan, adalah layanan yang digunakan untuk menjaga isi dari informasi dari siapapun kecuali yang memiliki otoritas atau kunci rahasia untuk membuka/mengupas informasi yang telah disandi.
b) Integritas data, adalah berhubungan dengan penjagaan dari perubahan data secara tidak sah. Untuk menjaga integritas data, sistem harus memiliki kemampuan untuk mendeteksi manipulasi data oleh pihak-pihak yang tidak berhak, antara lain penyisipan, penghapusan, dan pensubsitusian data lain kedalam data yang sebenarnya.
c) Autentikasi, adalah berhubungan dengan identifikasi/pengenalan, baik secara kesatuan sistem maupun informasi itu sendiri. Dua pihak yang saling berkomunikasi harus saling memperkenalkan diri. Informasi yang dikirimkan melalui kanal harus diautentikasi keaslian, isi datanya, waktu pengiriman, dan hal lainnya.
d) Non-repudiasi., atau nirpenyangkalan adalah usaha untuk mencegah terjadinya penyangkalan terhadap pengiriman atau terciptanya suatu informasi oleh yang mengirimkan/membuat.

Menurut Benni dkk(2014:34)berdasarkan kunci yang digunakan untuk enkripsi dan dekripsi, kriptografi dapat dibedakan menjadi 2 (dua) macam, yaitu kriptografi simetri dan kriptografi asimetri.

a) Kriptografi Simetri (Symetric Cryptography) kunci untuk proses enkripsi sama dengan kunci untuk proses dekripsi. Keamanan sistem kriptografi simetri

terletak pada kerahasiaan kunci. Istilah lain untuk kriptografi simetri adalah kriptografi kunci privat (private key cryptography) atau kriptografi konvensional. Sebelum melakukan pengiriman pesan, pengirim dan penerima harus memilih suatu suatu kunci tertentu yang sama untuk dipakai bersama, dan kunci ini haruslah rahasia bagi pihak yang tidak berkepentingan sehingga algoritma ini sering disebut juga sebagai algoritma kunci rahasia (secret-key algorithm).

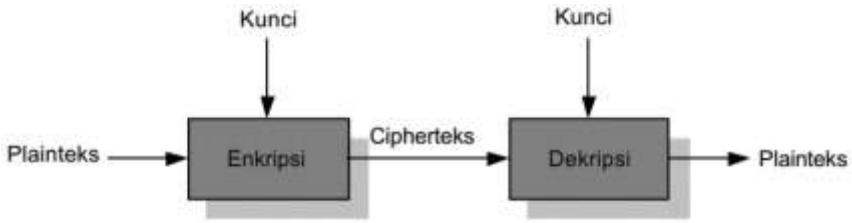
b) KriptografiAsimetri (Asymetric Cryptography), pada sistem kriptografi asimetri, kunci untuk proses enkripsi tidak sama dengan kunci untuk proses dekripsi. Istilah lain untuk kriptografi asimetri adalah kriptografi kunci publik (public key cryptography), sebab kunci untuk enkripsi tidak rahasia dan dapat diketahui oleh siapapun, sementara kunci untuk dekripsi hanya diketahui penerima. Kunci publik disebarkan secara umum sedangkan kunci privat disimpan secara rahasia oleh si pengguna. Walau kunci publik telah diketahui namun akan sangat sukar mengetahui kunci privat yang digunakan.

2.1.2 Enkripsi dan Dekripsi

Proses menyandikan plaintext menjadi ciphertext disebut enkripsi (encryption) atau enciphering (standar nama menurut ISO 7498-2). Proses mengembalikan ciphertext menjadi plaintext-nya disebut dekripsi (decryption) atau deciphering (standard nama menurut ISO 7498-2)

Enkripsi adalah sebuah proses yang melakukan perubahan sebuah kode yang bisa dimengerti menjadi sebuah kode yang tidak bisa dimengerti (tidak terbaca). Enkripsi dapat diartikan sebagai kode atau cipher

Proses yang dilakukan untuk mengamankan pesan (yang disebut plainteks) menjadi pesan yang tersembunyi (disebut chiperteks) adalah enkripsi. Ciphertext adalah pesan yang sudah tidak dapat dibaca dengan mudah. Proses sebaliknya, untuk mengubah ciphertext menjadi plaintext disebut deskripsi.(Yasin, 2017:4)



Gambar 2.1 Diagram Proses Enkripsi dan Dekripsi

2.1.3 Algoritma AES

Algoritma Advanced Encryption Standard (AES) adalah suatu algoritma block chiper dan mempunyai sifat simetri yang menggunakan kunci simetri pada waktu proses enkripsi dan dekripsi. Pada tahun 2001, AES digunakan sebagai standar algoritma kriptografi terbaru yang dipublikasikan oleh NIST (National Institute of Standard and Technology) sebagai pengganti algoritma DES (Data Encryption Standard) yang sudah berakhir masa penggunaannya. Algoritma AES adalah algoritma kriptografi yang dapat mengenkripsi dan mendekripsi data dengan panjang kunci yang bervariasi, yaitu 128 bit, 192 bit, dan 256 bit. Perbedaan dari ketiga urutan tersebut adalah panjang kunci yang mempengaruhi jumlah round (perputaran) yang dapat digambarkan dalam bentuk tabel:

	Panjang Kunci	Panjang Blok	Jumlah Putaran
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

Tabel 2.1 Perbedaan Macam – Macam AES

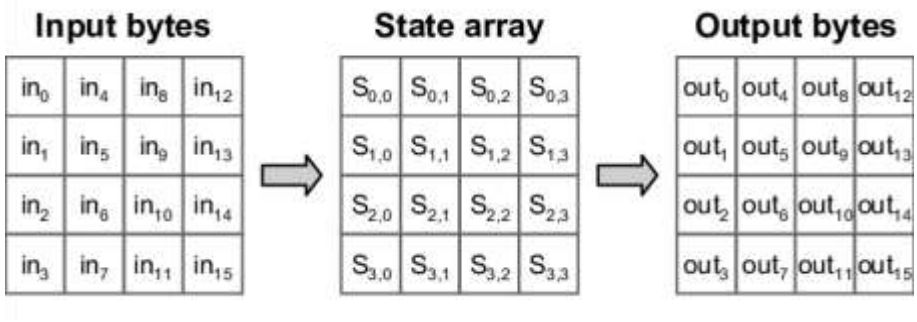
Pada tabel di atas dijelaskan mengenai tipe dari algoritma AES dengan panjang kunci, panjang blok dan jumlah putaran yang berbeda-beda. Terdapat 4 transformasi putaran pada proses enkripsi dan dekripsi:

1. SubBytes Berfungsi untuk menukar isi dari byte dengan menggunakan tabel substitusi.
2. ShiftRows Proses pergeseran blok per baris pada state array.
3. MixColumn Proses mengalikan blok data (pengacakan) di masing-masing state array dengan rumus sebagai berikut:

(x) = {03}2 + {01}2 + {01} + {02}

Mengombinasikan state array dan round key dengan hubungan XOR. Pada proses dekripsi algoritma AES:

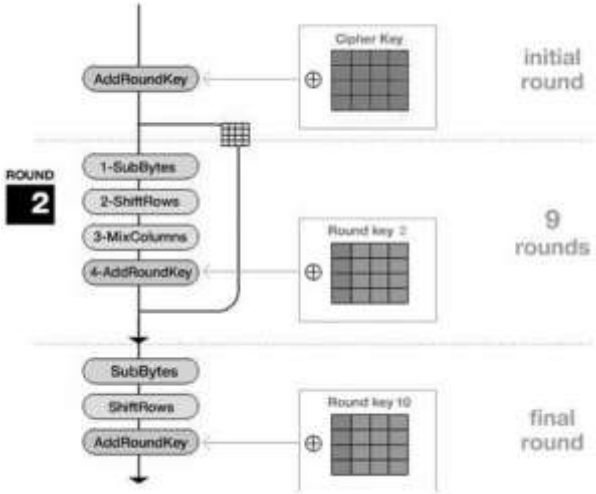
1. InvShiftRows Melakukan pergeseran bit ke kanan pada setiap blok baris.
2. InvSubBytes Setiap elemen pada state dipetakan dengan tabel Inverse S-Box.
3. InvMixColumn Setiap kolom dalam state dikalikan dengan matriks AES.
4. AddRoundKey Mengombinasikan state array dan round key dengan hubungan XOR. Penggambaran proses transformasi putaran dapat dilihat dari Gambar 2.2



Gambar 2.2 Proses Input Bytes, State Array, Output Bytes.

Dari Gambar 2.2 dapat dijelaskan bahwa algoritma AES ini ada dasarnya, algoritma AES ini merupakan array of bytes dengan dua dimensi yang disebut dengan state. Rumus ukuran dari state adalah $NROWS\ x\ NCOLS$, dari state ini akan diproses enkripsi dan dekripsi yang hasilnya akan dimasukkan ke dalam array of state. Pada awal proses enkripsi data dimasukkan ke dalam input bytes yang kemudian akan di salin kedalam array state, pada proses ini nantinya akan dilakukan enkripsi dan dekripsi, hasil keluarannya akan ditampung dalam output bytes. Pada awal proses enkripsi, input yang telah disalin ke dalam state akan mengalami transformasi AddRoundKey. Setelah itu state akan mengalami transformasi SubBytes, ShiftRows, MixColumns, dan AddRoundKey secara berulang-ulang sebanyak round/putaran (Nr). Proses ini dalam algoritma AES disebut sebagai round function. Round yang terakhir, state tidak diberikan transformasi MixColumns.

Ilustrasi proses awal enkripsi dengan menggunakan algoritma AES -128 dijelaskan pada Gambar 2.3. (Asri dan Nyoman, 2018:53)



Gambar 2.3 Proses Enkripsi Menggunakan Algoritma AES-128

2.1.4 PHP

PHP (Hypertext Preprocessor) adalah sebuah HTML-embedded scripting language, yaitu scripting language yang 'ditempelkan' dalam dokumen HTML, seperti halnya JavaScript atau VBScript. Tujuannya kurang lebih juga sama, yaitu untuk menciptakan halaman web yang interaktif dan dinamis. PHP atau PHP:Hypertext Preprocessor sebetulnya bermula dari Personal Home Page tools. PHP adlaah salah satu bahasa scripting yang ditaruh di dalam HTML. Sintaks PHP mirip dengan Perl, namun lebih sederhana. Saat ini PHP termasuk salah satu yang terpopuler. PHP dapat dijalankan lewat CGI atau sebagai modul Apache**.** (Benni dkk, 2014:34)

Gambar 2.4 Logo *PHP*

2.1.5 Macromedia Dreamwever 8

Gambar 2.5 Logo Aplikasi Macromedia Dreamweaver

Macromedia Dreamweaver adalah sebuah software design yang menawarkan cara mendesain website dengan dua langkah sekaligus dalam satu waktu, yaitu mendesain dan memprogram. Dreamweaver memiliki satu jendela mini yang disebut HTML source, tempat kode-kode HTML tertulis. Setiap kali mendesain web, seperti menulis kata-kata meletakkan gambar, membuat tabel dan proses lainnya, tag-tag HTML akan langsung tertulis. (Benni dkk, 2014:34)

2.1.6 Database

Database merupakan kumpulan dari data yang saling berhubungan satu dengan yang lainnya, tersimpan di simpanan luar komputer dan digunakan perangkat lunak tertentu untuk memanipulasinya. Database merupakan salah satu komponen yang penting di sistem informasi, karena berfungsi sebagai basis penyedia informasi bagi para pemakainya. Penerapan database dalam sistem informasi disebut dengan database system.

Model database adalah suatu konsep yang terintegrasi dalam menggambarkan hubungan (rela-tionships) antar data dan batasan-batasan (constraint) data dalam suatu sistem database.

Menurut Beni dkk (2014:35) Model database yang paling umum berdasarkan pada bagaimana hubungan antar record dalam database, terdapat tiga jenis, yaitu:

1) Model Database Hirarki (Hierarchical Database Model)
2) Model Database Jaringan (Network Database Model)
3) Model Database Relasi (Relational Database Model).

2.1.7 MySQL

MySQL mendukung hampir semua bahasa pemrograman populer saat ini, seperti C, C++, Java, Perl, PHP, dan Phyton. MySQL menerapkan metode yang sangat cepat dalam hal relasi antar tabel pada database-nya. Dengan metode one-sweep multijoin, MySQL sangat efisien dalam mengelola informasi yang diminta yang berasal dari banyak tabel sekaligus.

MySQL adalah server basis data yang kompak dan kecil yang ideal untuk banyak aplikasi basis data on-line. MySQL mendukung SQL standar (ANSI), meskipun tidak selengkap subset yang menjadi standar seperti PostgreSQL.MySQL dapat dijalankan di banyak platform dan memiliki kemampuan multithreading pada server UNIX. (Benni dkk, 2014:34)

2.1.8 Black-box Testing

Menurut Tri (2018:45) Black-Box Testing merupakan Teknik pengujian perangkat lunak yang berfokus pada spesifikasi fungsional dari perangkat lunak. Blackbox Testing bekerja dengan mengabaikan struktur kontrol sehingga perhatiannya difokuskan pada informasi domain. Blackbox Testing memungkinkan pengembang software untuk membuat himpunan kondisi input yang akan melatih seluruh syaratsyarat fungsional suatu program.

Keuntungan penggunaan metode Blackbox Tetsting adalah:

1. Penguji tidak perlu memiliki pengetahuan tentang bahasa pemrograman tertentu;
2. Pengujian dilakukan dari sudut pandang pengguna, ini membantu untuk mengungkapkan ambiguitas atau inkonsistensi dalam spesifikasi persyaratan;
3. Programmer dan tester keduanya saling bergantung satu sama lain.

Kekurangan dari metode Blackbox Testing adalah:

1. Uji kasus sulit disain tanpa spesifikasi yang jelas;
2. Kemungkinan memiliki pengulangan tes yang sudah dilakukan oleh programmer;
3. Beberapa bagian back end tidak diuji sama sekali.

2.2 Referensi Jurnal

Tabel 2.2 Daftar Referensi Jurnal

No	Judul Jurnal	Penulis	Tahun Terbit	Penerbit	Link
1.	Perancangan Pengamanan Data Menggunakan Algoritma AES (Advanced Encyption Standard)	Ami Aisiah Ibrahim	2017	STMIK Antar Bangsa	https://ejournal.antarbangsa.ac.id/index.php/jti/article/view/131
2.	Implementasi Algoritma Advanced Encryption Standard (AES) 128 Untuk Enkripsi dan Dekripsi File Dokumen	Asri Prameshwari dan Nyoman Putra Sastra	2018	STIKOM Bali	https://eksplora.stikom-bali.ac.id/index.php/eksplora/article/view/139
3.	Pengembangan Sistem Keamanan Untuk Toko Online Berbasis Kriptografi Aes Menggunakan Bahasa Pemrograman Php Dan Mysql	Benni Candra, Jusuf Wahyudi, Hermawansyah	2016	Universitas Dehasen Bengkulu	https://jurnal.unived.ac.id/index.php/jmi/article/view/250

4.	Implementasi Pengamanan Data Dan Informasi Dengan Metode Steganografi LSB Dan Algoritma Kriptografi AES	Syaiful Anwar	2017	STMIK AMIKOM Yogyakarta	https://ojs.amikom.ac.id/index.php/semnasteknomedia/article/view/1762
5.	Implementasi Algoritma AES Untuk Pengamanan Login Dan Data Customer Pada E-Commerce Berbasis Web	Laila Mustika	2020	STMIK Budi Darma	http://ejurnal.stmik-budidarma.ac.id/index.php/jurikom/article/view/1943