BAB II

LANDASAN TEORI

A. Data

Menurut Hutahaean (2014:8), "Data adalah bahan mentah bagi informasi, dirumuskan sebagai kelompok lambang-lambang tidak acak. Menunjukan jumlah, tindakan-tindakan, hal-hal dan sebagainya."

Selain itu menurut Rainer dan Prince (2016:10), "Data merupakan deskripsi dasar tentang berbagai hal, peristiwa, aktivitas, dan transaksi yang direkam, diklasifikasi, dan disimpan tetapi belum disusun atau diolah untuk menyampaikan suatu makna tertentu."

Beberapa contoh dari data :

- Data yang terformat adalah data dengan suatu format tertentu. Misalnya data yang menyatakan tanggal atau jam, atau menyatakan nilai mata uang.
- Teks adalah sederetan huruf, angka, dan simbol-simbol khusus yang kombinasinya tidak tergantung pada masing-masing item secara individual
- Citra (Image) adalah data dalam bentuk gambar. Citra dapat berupa foto, grafik, hasil rontgen, dan tanda tangan, dan lainnya.
- Audio adalah data dalam bentuk suara. Audio dapat berupa suara manusia atau binatang, musik dan lagu, detak jantung, dll.
- Video menyatakan data dalam bentuk sejumlah gambar yang bergerak dan bias saja dilengkapi dengan suara. Video dapat digunakan untuk mengabadikan suatu kejadian atau aktivitas.

B. Informasi

Pengertian sistem menurut Romney dan Steinbart (2015:4), "Informasi (information) adalah data yang telah dikelola dan diproses untuk memberikan arti dan memperbaiki proses pengambilan keputusan. Sebagaimana perannya, pengguna

membuat keputusan yang lebih baik sebagai kuantitas dan kualitas dari peningkatan informasi."

Menurut Rainer dan Prince (2016:10), "Informasi mengacu pada data yang telah disusun sehingga memiliki makna dan nilai bagi penerima."

Informasi dapat juga dikatakan sebagai sebuah pengetahuan yang diperoleh dari pembelajaran, pengalaman, dan instruksi. Sehingga dapat disimpulkan bahwa informasi merupakan data hasil pengolahan sistem maupun teknologi informasi yang memiliki nilai dan berguna bagi pengguna/ penerimanya.

C. Sistem

Menurut Romney dan Steinbart (2015:3), Sistem adalah suatu rangkaian yang terdiri dari dua atau lebih komponen yang saling berhubungan dan saling berinteraksi satu sama lain untuk mencapai tujuan dimana sistem biasa nya terbagi dalam sub system yang lebih kecil yang mendukung system yang lebih besar.

Definisi sistem menurut Mulyadi (2016:5), "Sistem adalah suatu jaringan prosedur yang dibuat menurut pola yang terpadu untuk melaksanakan kegiatan pokok perusahaan."

Dari kedua informasi yang telah dijabarkan di atas, secara sederhana sistem dapat diartikan sebagai suatu kumpulan atau himpunan dari unsur, komponen, atau variabel yang terorganisir, saling berinteraksi, saling tergantung satu sama lain, dan terpadu.

1. Pendekatan sistem pada prosedurnya

   Suatu sistem adalah suatu jaringan dan prosedur yang saling berkaitan, dan bekerjasama untuk melakukan suatu pekerjaan atau menyelesaikan suatu masalah tertentu.

2. Pendekatan sistem pada komponennya

   Suatu sistem adalah sekumpulan dari beberapa elemen yang saling berinteraksi dengan teratur sehingga membentuk suatu totalitas untuk menyelesaikan suatu masalah tertentu.

Berdasarkan beberapa pendapat yang dikemukakan diatas dapat ditarik kesimpulan bahwa sistem adalah kumpulan bagian-bagian atau sub sistem - sub sistem yang disatukan dan dirancang untuk mencapai suatu tujuan.

D. Sistem Informasi

Menurut Kenneth C Laudon dan Jane P Laudon (2014:45), "Suatu sistem informasi dapat didefinisikan secara teknis sebagai seperangkat komponen yang saling terkait yang mengumpulkan (atau mengambil), memproses, menyimpan, dan mendistribusikan informasi untuk mendukung pengambilan keputusan dan kontrol dalam suatu organisasi."

Menurut Yakub dan Hisbanarto (2014:32) "Sistem informasi merupakan hal yang sangat penting bagi manajemen dalam pengambilan keputusan dalam sebuah organisasi yang berhubungan dengan proses penciptaan dan aliran informasi."

Sementara menurut R. Kelly Rainer dan Casey G. Cegielski (2015:5), "Sistem Informasi merupakan sistem yang mengumpulkan, mengolah, menyimpan, menganalisa, dan menguraikan informasi untuk tujuan spesifik."

E. Keamanan Informasi

Menurut Whitman dan Mattord (2011:41), Keamanan informasi merupakan upaya untuk melindungi informasi dan elemen-elemen penting yang ada didalamnya, baik berupa sistem atau perangkat keras yang digunakan untuk menyimpan dan mengirimkan informasi.

Keamanan informasi menggambarkan usaha untuk melindungi komputer dan non peralatan komputer, fasilitas, data, dan informasi dari penyalahgunaan oleh orang yang tidak bertanggung jawab. Keamanan informasi dimaksudkan untuk mencapai kerahasiaan, ketersediaan, dan integritas di dalam sumber daya informasi baik bagi kebutuhan personal maupun kebutuhan bisnis perusahaan.

Masalah keamanan merupakan salah satu aspek penting dari sebuah sistem informasi, sayang sekali masalah keamanan ini seringkali kurang mendapat perhatian dari pemilik dan pengelola sistem infromasi. Jatuhnya informasi ke pihak lain (misal pihak lawan bisnis) dapat menimbulkan kerugian bagi pemilik informasi. Untuk itu keamanan dari sistem informasi yang digunakan harus terjamin dalam batas yang

diterima. Web server dan database Server bagaikan jantung dan otak dari organisme internet. Dua komponen ini menjadi komponen pokok dari sebuah aplikasi internet yang tangguh dan tepatlah keduanya menjadi target hacker. Dalam beberapa kasus kita harus dapat menentukan titik-titik lemah dalam aplikasi tersebut yang bisa menjadi sasaran penyerang. Jatuhnya informasi ke tangan pihak lain dapat menimbulkan kerugian bagi pemilik informasi.

Keamanan informasi dimaksudkan untuk mencapai tiga sasaran utama yaitu:

- Melindungi data dan informasi personal dan bisnis dari penyingkapan orang-orang yang tidak berhak. Inti utama dari aspek kerahasiaan adalah usaha untuk menjaga informasi dari orang-orang yang tidak berhak mengakses. *Privacy* lebih kearah data-data yang sifatnya privat. Serangan terhadap aspek *privacy* misalnya usaha untuk melakukan penyadapan. Usaha-usaha yang dapat dilakukan untuk meningkatkan privacy adalah dengan menggunakan teknologi kriptografi. Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti keabsahan, integritas data, serta autentikasi data.
- Ketersediaan. Aspek ini berhubungan dengan metode untuk menyatakan bahwa informasi benar-benar asli, atau orang yang mengakses atau memberikan informasi adalah betul-betul orang yang dimaksud. Masalah pertama untuk membuktikan keaslian dokumen dapat dilakukan dengan teknologi watermarking dan digital signature.Watermarking juga dapat digunakan untuk menjaga intelektual property, yaitu dengan menandatangani dokumen atau hasil karya pembuat. Masalah kedua biasanya berhubungan dengan akses control, yaitu berkaitan dengan pembatasan orang-orang yang dapat mengakses informasi. Dalam hal ini pengguna harus menunjukkan

bahwa memang dia adalah pengguna yang sah atau yang berhak menggunakannya.

- Aspek ini menekankan bahwa informasi tidak boleh diubah tanpa seijin pemilik informasi. Adanya virus, trojan horse, atau pemakai lain yang mengubah informasi tanpa izin. Sistem informasi perlu menyediakan representasi yang akurat dari sistem fisik yang direpresentasikan.

F. Unified Modelling Language (UML)

UML (Unified Modelling Language) adalah sekumpulan alat yang digunakan untuk melakukan abstraksi terhadap sebuah sistem atau perangkat lunak berbasis objek. UML juga menjadi salah satu cara untuk mempermudah pengembangan aplikasi yang berkelanjutan. Aplikasi atau sistem yang tidak terdokumentasi biasanya dapat menghambat pengembangan karena developer harus melakukan penelusuran dan mempelajari kode program. UML juga dapat menjadi alat bantu untuk transfer ilmu tentang sistem atau aplikasi yang akan dikembangkan dari satu developer ke developer lainya. Tidak hanya antar developer terhadap orang bisnis dan siapapun dapat memahami sebuah sistem dengan adanya UML.

1. Use Case Diagram

Use Case Diagram adalah gambaran grafis dari beberapa atau semua actor, use case, dan interaksi diantaranya yang memperkenalkan suatu sistem.

Simbol-simbol yang digunakan dalam use case diagram, yaitu :

- Use case menggambarkan fungsionalitas yang disediakan sistem.
- Aktor adalah orang, proses, atau sistem lain yang berinteraksi dengan sistem informasi yang akan dibuat.

- Asosiasi adalah komunikasi antara aktor dan use case yang berpartisipasi pada use case diagram atau use case yang memiliki interaksi dengan aktor.
- Include adalah relasi use case tambahan ke sebuah use case dimana use case yang ditambahkan membutuhkan use case ini untuk menjalankan fungsinya atau sebagai syarat dijalankan use case ini.
- Extend adalah relasi use case tambahan ke sebuah use case dimana use case yang ditambahkan dapat berdiri sendiri meski tanpa use case tambahan itu.
- Hubungan generalisasi dan spesialisasi (umum - khusus) antara dua buah use case dimana fungsi yang satu merupakan fungsi yang lebih umum dari lainnya.

2. Activity Diagram

Diagram ini menggambarkan tentang aktifitas yang terjadi pada sistem. Dari pertama sampai akhir, diagram ini menunjukkan langkah – langkah dalam proses kerja sistem yang dibuat.

Komponen yang ada pada Activity Diagram antara lain :

- Start Point/Initial State (Titik Mulai)

  Start Point merupakan lingkaran hitam kecil, yang menandakan tindakan awal atau titik awal aktivitasuntuk setiap diagram aktivitas.
- Activitiy (Aktivitas)

  Activity menunjukan aktivitas yang dilakukan atau yang sedang terjadi dalam activity diagram.
- Action Flow (Arah)

Action Flow digunakan untuk transisi dari suatu tindakan ke tindakan yang lain atau menunjukan aktivitas selanjutnya setelah aktivitas sebelumnya.

- Decision (Keputusan)

  Decision adalah suatu titik atau point pada activity diagram yang mengindikasikan suatu kondisi dimana ada kemungkinan perbedaan transisi.

- Synchronization

  Synchornization dibagi menjadi 2 yaitu fork dan join.

  - Fork (percabangan) digunakan untuk memecah behaviour menjadi activity atau action yang paralel.
  - Join (penggabungan) untuk menggabungkan kembali activity atau action yang paralel.

- Merge Event (Menggabungkan)

  Merge Event berfungsi untuk menggabungkan flow yang dipecah oleh decission.

- Swimlanes

  Swimlanes berfungsi untuk memecah activity diagram menjadi baris dan kolom untuk membagi tangung jawab obyek-obyek yang melakukan aktivitas.

- Final State/ End Point (Titik Akhir)

  Final State menunjukan bagian akhir dari aktivitas.

3. Class Diagram

Class Diagram menggambarkan serta deskripsi atau penggambaran dari class, atribut, dan objek disamping itu juga hubungan satu sama lain seperti pewarisan, containmet, asosiasi dan lainnya.

G. Sistem Basis Data

Menurut Rosa dan Shalahuddin (2015:43) “Basis data merupakan salah satu bagian dalam rekayasa perangkat lunak yang terkomputerisasi dan bertujuan utama memelihara data yang sudah diolah atau media penyimpanan informasi agar dapat diakses dengan mudah dan cepat.”

Sedangkan menurut Yakub dan Hisbanarto (2015:25) menjelaskan, “Basis data merupakan kumpulan data yang saling berhubungan atau punya relasi”.

Dari teori ahli di atas, dapat disimpulkan bahwa sistem basis data merupakan kumpulan dari data yang saling berhubungan (relasi) antara satu dengan yang lainnya yang diorganisasikan berdasarkan skema atau struktur tertentu sehingga menghasilkan suatu informasi.

Pada penelitian ini, sistem basis data yang penulis gunakan adalah MySQL. MySQL merupakan sistem basis data yang menggunakan perintah dasar SQL (Structured Query Language). SQL sendiri merupakan suatu bahasa yang dipakai di dalam pengambilan data pada *relational database* atau sistem basis data yang terstruktur. Jadi MySQL adalah *database management system* yang menggunakan bahasa SQL sebagai bahasa penghubung antara perangkat lunak aplikasi dengan database server.

1) Elemen SQL

Elemen dari SQL yang paling dasar antara lain pernyataan, nama, tipe data, ekspresi, konstanta dan fungsi bawaan.

a. Pernyataan

Perintah dari SQL yang digunakan untuk meminta sebuah tindakan kepada DBMS. Pernyataan SQL dapat dikelompokan menjadi 3 kelompok, yaitu : DDL, DML dan DCL.

- DDL (*Data Defination Language*)

  DDL berfungsi untuk mendefinisikan atribut basis data, table, atribut(kolom), batasan-batasan terhadap suatu atribut, serta hubungan antar tabel. Perintah yang digunakan biasanya : CREATE untuk membuat database dan tabel, ALTER untuk merubah database dan tabel, dan DROP untuk menghapus database dan tabel

- DML (*Data Manipulation Language*)

  DML berfungsi untuk memanipuladi data yang ada di dalam basis data, contohnya untuk pengambilan data, penyisipan data, pengubahan data dan penghapusan data. Perintah yang digunakan biasanya adalah : INSERT untuk menambah data pada tabel, DELETE untuk menghapus data pada tabel, UPDATE untuk mengubah data pada tabel, dan SELECT untuk menampilkan data pada tabel.

- DCL (*Data Control Language)*

  DCL adalah sub bahasa SQL yang berfungsi untuk melakukan pengontrolan data dan server databasenya, seperti manipulasi user dan hak akses (priviledges). Yang termasuk perintah dalam DCL ada dua, yaitu GRANT yang digunakan untuk memberikan hak akses oleh admin ke salah satu user

atau pengguna dan REVOKE yang digunakan untuk mencabut hak akses yang telah diberikan kepada user.

b. Nama

Nama digunakan sebagai identitas, yaitu identitas bagi objek pada DBMS. Misal : tabel, kolom dan pengguna.

c. Tipe Data

Tipe data numerik yang ada dalam MYSQL :

- TINYINT : Nilai integer yang sangat kecil
- SMALLINT : Nilai integer yang kecil
- MEDIUMINT: Nilai integer yang sedang
- INT : Nilai integer dengan nilai standar
- BEGINT : Nilai integer dengan nilai besar
- FLOAT : Bilangan decimal dengan single-precission
- DOUBLE : Bilangan decimal dengan double-precission
- DECIMAL : Bilangan float yang dinyatakan sebagai string.

Tipe data string yang ada dalam MYSQL :

- CHAR : Karakter yang memiliki panjang tetap yaitu sebanyak n
- VARCHAR : Karakter yang memiliki panjang tidak tetap yaitu maksimum n
- TINYBLOB : BLOB dengan ukuran sangat kecil
- BLOB : BLOB yang memiliki ukuran kecil
- MEDIUMBLOB : BLOB yang memiliki ukuran sedang
- LONGBLOB : BLOB yang memiliki ukuran besar

- TINYTEXT : teks dengan ukuran sangat kecil
- TEXT : teks yang memiliki ukuran kecil
- MEDIUMTEXT : teks yang memiliki ukuran sedang
- LONGTEXT : teks yang memiliki ukuran besar
- ENUM : kolom diisi dengan satu member enumerasi
- SET : Kolom dapat diisi dengan beberapa nilai anggota himpunan

Tipe data *date and time* yang ada dalam MYSQL :

- DATE : date memiliki format tahun-bulan-tanggal
- TIME : time memiliki format jam-menit-detik
- DATETIME : gabungan dari format date dan time

d. Ekspresi

Ekspresi digunakan untuk menghasilkan/menghitung nilai. Ekspresi aritmatika antara lain :

- + : tambah
- - : kurang
- / : bagi
- * : kali.

e. Konstanta

Nilai yang tetap.

f. Fungsi bawaan

Fungsi adalah subprogram yang dapat menghasilkan suatu nilai apabila fungsi tersebut dipanggil. Fungsi Agregat adalah

fungsi yang digunakan untuk melakukan summary, statistik yang dilakukan pada suatu tabel/ query.

- AVG : digunakan untuk mencari nilai rata-rata dalam kolom dari tabel.
- COUNT : digunakan untuk menghitung jumlah baris dari sebuah kolom dari tabel
- MAX : digunakan untuk mencari nilai yang paling besar dari suatu kolom dari tabel
- MIN : digunakan untuk mencari nilai yang paling kecil dari suatu kolom dari tabel
- SUM : digunakan untuk mengitung jumlah keseluruhan dari suatu kolom dari tabel

Berikut adalah kelebihan dari mysql yang membuat penulis menggunakan sistem basis data mysql dalam penelitian ini :

- Program yang multi-threaded, sehingga dapat dipasang pada server yang memiliki mulit-CPU
- Didukung bahasa pemrograman umum seperti C, C++, Java, Perl, PHP, Python, TCL, APls dls.
- Bekerja pada berbagai platform
- Memiliki jenis kolom yang cukup banyak sehingga memudahkan konfigurasi system database
- Memiliki jenis kolom yang cukup banyak sehingga memudahkan konfigurasi sistem database
- Memiliki system sekuriti yang cukup baik dengan verifikasi host

- Mendukung ODBC untuk OS Microsoft Windows
- Mendukung record yang memiliki kolom dengan panjang tetap
- Software yang free

H. Kriptografi

Menurut Dan Boneh dan Victor Shoup (2015:2), “Kriptografi adalah alat yang sangat diperlukan untuk melindungi informasi dalam sistem komputasi.”

Perkembangan komunikasi telah mendorong manusia untuk menyembunyikan informasi yang dimilikinya dari orang lain demi alasan keamanan dan privasi, untuk itu ditemukanlah konsep kriptograf. Kriptografi telah dikenal sejak 4000 tahun yang lalu. Konsep kriptografi sendiri telah lama digunakan oleh manusia misalnya pada peradaban Mesir dan Romawi walau masih sangat sederhana.

Kriptografi merupakan seni dan keahlian mengamankan pesan atau data menghasilkan suatu pesan atau data yang asli berubah menjadi tidak dikenali lagi. Secara umum kriptografi dapat diartikan sebagai ilmu dan seni penyandian yang bertujuan untuk menjaga keamanan dan kerahasiaan suatu pesan.

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

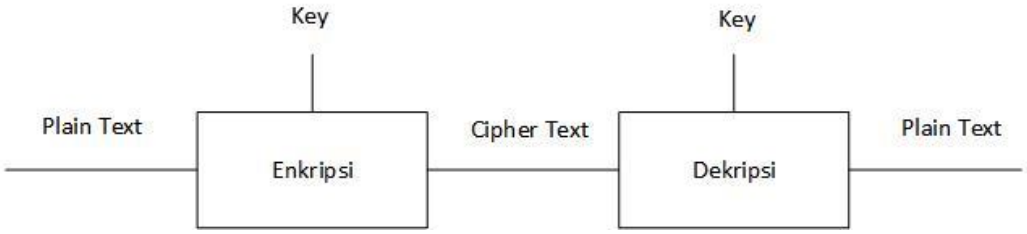
1. Kerahasiaan, adalah layanan yang digunakan untuk menjaga isi dari informasi dari siapapun kecuali yang memiliki otoritas atau kunci rahasia untuk membuka/mengupas informasi yang telah disandi.
2. Integritas data, adalah berhubungan dengan penjagaan dari perubahan data secara tidak sah. Untuk menjaga 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.

3. 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 lain-lain.
4. Non-repudiasi., adalah usaha untuk mencegah terjadinya penyangkalan terhadap pengiriman/terciptanya suatu informasi oleh yang mengirimkan/membuat. Istilah-istilah yang digunakan dalam bidang kriptografi :
   A. Plaintext (M) adalah pesan yang hendak dikirimkan (berisi data asli).
   B. Ciphertext (C) adalah pesan ter-enkrip (tersandi) yang merupakan hasil enkripsi.
   C. Enkripsi (fungsi E) adalah proses pengubahan plaintext menjadi ciphertext.
   D. Dekripsi (fungsi D) adalah kebalikan dari enkripsi yakni mengubah ciphertext menjadi plaintext, sehingga berupa data awal/asli.

Kriptografi pada dasarnya terdiri dari dua proses, yaitu proses enkripsi dan proses dekripsi. Proses enkripsi adalah proses penyandian pesan terbuka menjadi pesan rahasia (ciphertext). Pada saat ciphertext diterima oleh penerima pesan, maka pesan rahasia tersebut diubah lagi menjadi pesan terbuka melalui proses deskripsi sehingga pesan tadi dapat dibaca kembali oleh penerima pesan. Secara umum, proses enkripsi dan dekripsi dapat digambarkan sebagai berikut:

Gambar 2.1

Proses Enkripsi dan Deskripsi



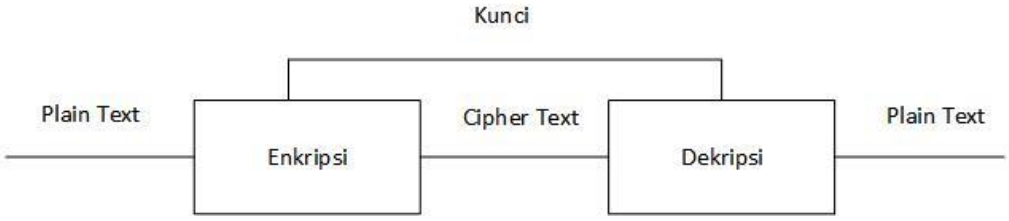
Sumber : AES, Algoritma Rijndael

Algoritma Kriptografi Ada 2 jenis kriptografi berdasar jenis kuncinya yaitu algoritma simetri (konvensional/secret key) dan algoritma asimetri (kunci publik/public key).

a. Kriptografi Simetri (Secret Key) Kriptografi secret key adalah kriptografi yang hanya melibatkan satu kunci dalam proses enkripsi dan dekripsi. Kriptografi secret key seringkali disebut sebagai kriptografi konvensional atau kriptografi simetris (Symmetric Cryptography) dimana proses dekripsi adalah kebalikan dari proses enkripsi dan menggunakan kunci yang sama.

Gambar 2.2

Kriptografi simetris



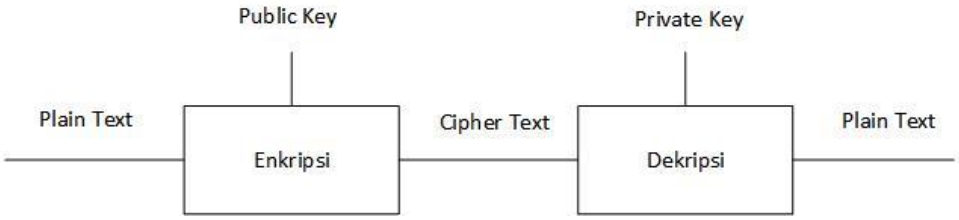
Sumber : AES, Algoritma Rijndael

Yang termasuk dalam kriptografi algoritma kunci simetri adalah OTP, DES, RC2, RC4, RC5, RC6, IDEA, AES, Twofish, Blowfish, Magenta, FEAL, SAFER, CAST, GOST, A5, LOKI, dan lain-lain

b. Kriptografi Asimetri (Public Key) Kriptografi public key sering disebut dengan kriptografi asimetris. Berbeda dengan kriptografi secret key, kunci yang digunakan pada proses enkripsi dan proses dekripsi pada kriptografi public key ini berbeda satu sama lain. Jadi dalam kriptografi public key, suatu key generator akan menghasilkan dua kunci berbeda dimana satu kunci digunakan untuk melakukan proses enkripsi dan kunci yang lain digunakan untuk melakukan proses dekripsi. Yang termasuk dalam algoritma asimetri adalah ECC, LUC, RSA, El Gamal, dan DH.

Gambar 2.3

Kriptografi asimetris



Sumber : AES, Algoritma Rijndael

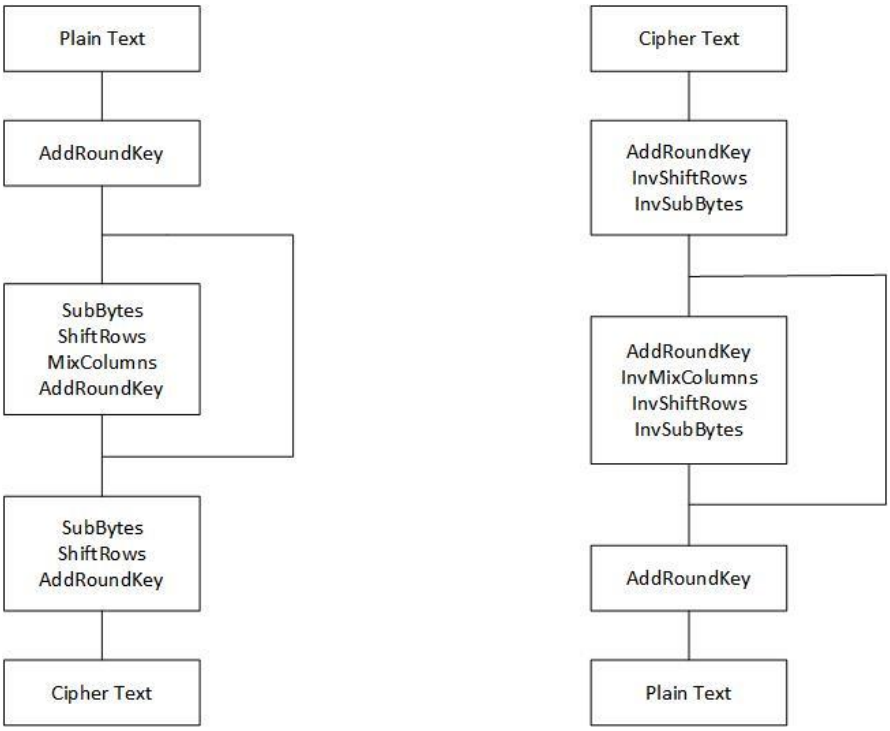
I. Enkripsi

Menurut Dan Boneh dan Victor Shoup (2015:18), “Enkripsi adalah kasus bagaimana dua pihak dapat berkomunikasi secara rahasia di Internet dengan adanya kehadiran penyadap.”

Proses enkripsi pada algoritma AES terdiri dari 4 jenis transformasi bytes, yaitu SubBytes, ShiftRows, Mixcolumns, dan AddRoundKey. Pada awal proses enkripsi, input yang telah dikopikan ke dalam akan mengalami transformasi byte AddRoundKey. Setelah itu, State akan mengalami transformasi SubBytes, ShiftRows, MixColumns, dan AddRoundKey secara berulang-ulang sebanyak Nr. Proses ini dalam algoritma AES disebut sebagai round function.

Gambar 2.4

Diagram Alir Proses Enkripsi dan Dekripsi



Sumber : AES, Algoritma Rijndael

J. Dekripsi

Dekripsi Transformasi cipher dapat dibalikkan dan diimplementasikan dalam arah yang berlawanan untuk menghasilkan inverse cipher yang mudah dipahami untuk algoritma AES. Transformasi byte yang digunakan pada invers cipher adalah InvShiftRows, InvSubBytes, InvMixColumns, dan AddRoundKey.

K. Algoritma AES Rijndael

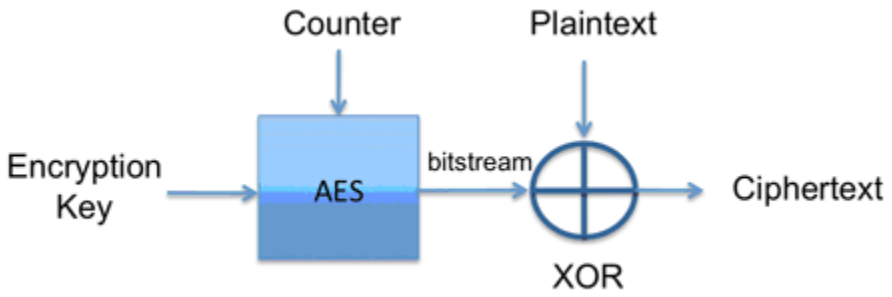
AES adalah lanjutan dari algoritma enkripsi standar DES yang pada 2 Maret tahun 2001 ditetapkanlah algoritma baru Rijndael sebagai AES. Kriteria pemilihan AES didasarkan pada 3 kriteria utama yaitu: keamanan, harga, dan karakteristik algoritma beserta implementasinya.

Rijndael termasuk dalam jenis algoritma kriptografi yang sifatnya simetri dan cipher block. Dengan demikian algoritma ini mempergunakan kunci yang sama saat

enkripsi dan dekripsi serta masukan dan keluarannya berupa blok dengan jumlah bit tertentu.

Gambar 2.5

Algoritma AES



Sumber : AES, Algoritma Rijndael

Rijndael mendukung berbagai variasi ukuran blok dan kunci yang akan digunakan. Namun Rijndael mempunyai ukuran blok dan kunci yang tetap sebesar 128, 192, 256 bit. Pemilihan ukuran blok data dan kunci akan menentukan jumlah proses yang harus dilalui untuk proses enkripsi dan dekripsi. Proses enskripsi adalah kebalikkan dari deskripsi. Berikut penjelasannya :

1. Key Schedule

   Proses key schedule diperlukan untuk mendapatkan subkey-subkey dari kunci utama agar cukup untuk melakukan enkripsi dan dekripsi. Proses ini terdiri dari beberapa operasi, yaitu :

   a. Operasi Rotate, yaitu operasi perputaran 8 bit pada 32 bit dari kunci.
   b. Operasi SubBytes, pada operasi ini 8 bit dari subkey disubstitusikan dengan nilai dari S-Box.
   c. Operasi Rcon, operasi ini dapat diterjemahkan sebagai operasi pangkat 2 nilai tertentu dari user. Operasi ini menggunakan nilai-nilai dalam Galois

field. Nilai-nilai dari Rcon kemudian akan di-XOR dengan hasil operasi SubBytes.

d. Operasi XOR dengan w[i-Nk] yaitu word yang berada pada Nk sebelumnya.

2. AddRoundKey

Pada proses ini subkey digabungkan dengan state. Proses penggabungan ini menggunakan operasi XOR untuk setiap byte dari subkey dengan byte yang bersangkutan dari state. Untuk setiap tahap, subkey dibangkitkan dari kunci utama dengan menggunakan proses key schedule. Setiap subkey berukuran sama dengan state yang bersangkutan.

3. SubBytes

Rijndael hanya memiliki satu S-box. Kriteria desain untuk kotak S yang dibuat sedemikian rupa sehingga tahan terhadap diferensial linear yang dikenal sebagai pembacaan sandi dan menyerang menggunakan manipulasi aljabar. Koordinat x merupakan digit pertama sedangkan y yang kedua dari bilangan hexadecimal

4. ShiftRows

Proses ShiftRows akan beroperasi pada tiap baris dari tabel state. Proses ini akan bekerja dengan cara memutar byte-byte pada 3 baris terakhir (baris 1, 2, dan 3) dengan jumlah perputaran yang berbeda-beda. Baris 1 akan diputar sebanyak 1 kali, baris 2 akan diputar sebanyak 2 kali, dan baris akan diputar sebanyak 3 kali. Sedangkan baris 0 tidak akan diputar.

5. MixColums

Proses MixColumns akan beroperasi pada tiap kolom dari tabel state. Operasi ini menggabungkan 4 bytes dari setiap kolom tabel state dan

menggunakan transformasi linier Operasi Mix Columns memperlakukan setiap kolom sebagai polinomial 4 suku dalam Galois field dan kemudian dikalikan dengan c(x) modulo (x4+1), dimana c(x)=3x3+x2+x+2. Kebalikkan dari polinomial ini adalah c(x)=11x3+13x2+9x+14. Operasi MixColumns juga dapat dipandang sebagai perkalian matrix.

Sebagai varian dari Square Cipher, Rijndael memiliki kemampuan untuk bekerja sangat baik pada platform apapun. Ditambah dengan operasi yang menggunakan table lookup dan operasi XOR membuat prosesnya menjadi tidak terlalu rumit.

L. Tolak Ukur Kata Sandi yang Kuat dan Lemah

Kata sandi yang kuat adalah kata sandi yang dirancang untuk sulit ditemukan oleh seseorang atau program. Karena tujuan kata sandi adalah untuk memastikan bahwa hanya pengguna yang berwenang yang dapat mengakses informasi, kata sandi yang mudah ditebak menjadi suatu risiko keamanan. Komponen penting dari kata sandi yang kuat mencakup panjang yang cukup dan campuran jenis karakter. Kata sandi yang lemah biasanya pendek dan hanya terdiri dari huruf kecil atau besar.

Ketika orang membuat kata sandi, seringkali menggunakan hal-hal yang mudah ditebak seperti bagian dari nama mereka, nama hewan peliharaan mereka, atau bahkan kata "kata sandi," itu sendiri, yang merupakan kata sandi yang paling umum digunakan selama bertahun-tahun. Kata sandi dapat dibuat lebih sulit untuk dipecahkan dengan menggunakan lebih banyak karakter, menggabungkan huruf besar dan kecil, dan termasuk angka dan karakter khusus. Menurut panduan keamanan dari Texas A&M University's Research Foundation, kata sandi enam karakter, satu kasus memiliki 308 juta kemungkinan kombinasi, yang semuanya

dapat diakses oleh *cracker* kata sandi hanya dalam beberapa menit. Menggabungkan huruf besar dan kecil dan menggunakan delapan karakter meningkatkan kemungkinan kombinasi menjadi 53 triliun; mengganti angka dengan salah satu huruf menghasilkan 218 triliun kemungkinan; dan mengganti karakter khusus atau tanda baca dengan yang lain menghasilkan 6.095 triliun kemungkinan kombinasi.

M. Perbandingan Algoritma AES dan DES

Tabel 2.1

Perbandingan Algoritma AES dan DES

Factors	DES	AES
Key Length	56 bits	128, 192 or 256 bits
Block Size	64 bits	128, 192, or 256 bits
Cipher Text	Symmetric block cipher	Symmetric block cipher
Developed	1977	2000
Security	Proven inadequate	Considered secure
Cryptanalysis Resisteance	Vulnerable to differential and linear cryptanalysis; weak substitution tables	Strong against differential, truncated differential, linear, interpolation and square attacks
Possible keys	2^{56}	2^{128},2^{192} and 2^{256}
Possible ASCII printable character key	95^{7}	95^{16}, 95^{24} or 95^{32}

Sumber : Analysis and Comparison between AES and DES Cryptographic Algorithm, International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 6, December 2012

Kesimpulannya algoritma AES dibandingkan dengan DES, algoritma AES memiliki banyak variasi panjang kunci dan block yang lebih banyak sehingga dapat dicocokkan sesuai kebutuhan, selain itu sudah dibuktikan bahwa DES memiliki kinerja yang lebih buruk dalam hal keamanan dibandingkan AES, DES lebih rentan terhadap serangan dibandingkan AES.

N. Penelitian Terdahulu

Dari pencarian dan studi pustaka yang dilakukan penulis, penulis menemukan bahwa adanya penelitian terdahulu yang berkaitan dengan penerapan algoritma Rijndael. Penelitian-penelitian tersebutlah yang menjadi sumber inspirasi dan bahan pertimbangan penulis dalam memilih topik penelitian.

Pada tahun 2013, Eka Adhitya Dharmawan, Erni Yudaningtyas, dan M. Sarosa melakukan penelitian yang berjudul “Perlindungan Web pada Login Sistem Menggunakan Algoritma Rijndael”. Para peneliti tersebut membahas lebih mendalam mengenai algoritma rijndael dan implementasinya dalam sistem berbasis web yang dapat mengatasi beberapa ancaman dan serangan salah satunya yaitu SQL Injection. Selain itu algoritmna rijndael dikenal sebagai algoritma kriptografi yang dapat melindungi informasi dengan baik serta efisien dalam implementasinya.