

BAB 2

LANDASAN TEORI

2.1 Repository

Repository atau yang biasa disingkat repo merupakan sebuah alokasi ruang atau tempat untuk penyimpanan aplikasi yang memiliki jumlah ratusan atau bahkan mencapai ribuan yang bisa diakses melalui internet.

2.2 RSA

RSA adalah salah satu teknik kriptografi dimana kunci untuk melakukan enkripsi berbeda dengan kunci untuk melakukan dekripsi. Algoritma RSA dibuat oleh 3 orang peneliti dari MIT (Massachusetts Institute of Technology) pada tahun 1976, yaitu: Ron (R)ivest, Adi (S)hamir, dan Leonard (A)dleman. Keamanan algoritma RSA terletak pada sulitnya memfaktorkan bilangan yang besar menjadi faktor-faktor prima. Pemfaktoran dilakukan untuk memperoleh kunci privat. Selama pemfaktoran bilangan besar menjadi faktor faktor prima belum ditemukan algoritma yang mangkus, maka selama itu pula keamanan algoritma RSA tetap terjamin. Tujuan-tujuan dari penggunaan algoritma kriptografi RSA antara lain adalah sebagai berikut.

1. Confidentiality

yaitu menjaga kerahasiaan data dan menyimpan data dengan menyandikan informasi menggunakan teknik-teknik enkripsi.

2. Data Integrity

yaitu memberikan jaminan bahwa untuk tiap bagian data tidak akan mengalami perubahan dari saat data disimpan sampai dengan saat data tersebut dibuka

Untuk pembangkitan pasangan kunci RSA, digunakan algoritma sebagai berikut.

1. Dipilih dua buah bilangan prima sembarang yang besar, p dan q . Nilai p dan q harus dirahasiakan.
2. Dihitung $n = p \times q$. Besaran n tidak perlu dirahasiakan.
3. Dihitung $m = (p-1)(q-1)$
4. Dipilih sebuah bilangan bulat sebagai
5. kunci publik, disebut namanya e , yang relatif prima terhadap m .
6. e relatif prima terhadap m artinya faktor pembagi terbesar keduanya adalah 1, secara matematis disebut $\text{gcd}(e, m) = 1$. Untuk mencarinya dapat digunakan algoritma Euclid
7. Dihitung kunci privat, disebut namanya d sedemikian agar $(d \times e) \bmod m = 1$. Untuk mencari nilai d yang sesuai dapat juga digunakan algoritma Extended Euclid.

Maka hasil dari algoritma tersebut diperoleh :

1. kunci publik adalah pasangan (e,n)
2. kunci privat adalah pasangan (e,m)

n tidak bersifat rahasia, namun ia diperlukan pada perhitungan enkripsi/dekripsi.

Keamanan algoritma RSA terletak pada tingkat kesulitan dalam memfaktorkan bilangan non prima menjadi faktor primanya, yang dalam hal ini $n = p \times q$. Jika n berhasil difaktorkan menjadi p dan q , maka $m = (p - 1)(q - 1)$ dapat dihitung. Dan karena kunci enkripsi e telah diumumkan (tidak dirahasiakan), maka kunci dekripsi d dapat dihitung melalui persamaan $(d \times e) \bmod n = 1$. Selama belum ditemukan cara untuk memfaktorkan bilangan besar menjadi faktor-faktor primanya, maka selama itu pula keamanan algoritma RSA terjamin.

Berikut contoh perhitungan metode RSA

1. Pertama, menentukan 2 buah bilangan prima untuk p dan q :

$$p = 11$$

$$q = 13$$

2. Selanjutnya mendapatkan nilai n dimana rumus-nya :

$$n = p * q$$

dan akan menjadi seperti ini :

$$n = 11 * 13$$

$$n = 143$$

3. Mendapatkan nilai m dimana rumus-nya :

$$m = (p - 1) * (q - 1)$$

dan akan menjadi seperti ini :

$$m = (11 - 1) * (13 - 1)$$

$$m = (10) * (12)$$

$$m = 120$$

4. Menentukan nilai e dengan syarat :

$$e = e > 1 \text{ and } \text{GCD}(m,e) = 1$$

Dimana "17" adalah nilai yang memenuhi syarat untuk nilai e

$$e = \text{GCD}(120,17) = 1$$

5. Menentukan nilai d dengan syarat :

$$d = (d * e) \text{ mod } m = 1$$

Dimana "473" adalah nilai yang memenuhi syarat untuk nilai d

$$d = (473 * 17) \text{ mod } 120 = 1$$

6. Dari proses diatas, maka akan mendapatkan kunci public dan kunci

privat dimana :

$$\text{public key} = (e,n)$$

$$\text{private key} = (d,n)$$

Dan kunci akan menjadi seperti ini :

public key = (17,143)

private key = (473,143)

2.3 Pemodelan Objek

Pemodelan objek merupakan suatu metode untuk menggambarkan struktur sistem yang memperlihatkan semua objek yang ada pada sistem. (Nugroho, 2005, hal:37)

2.2.1 Definisi UML

“Unified Modeling Language (UML) adalah standar bahasa yang banyak digunakan di dunia industri untuk mendefinisikan requirement, membuat analisis dan desain, serta menggambarkan arsitektur dalam pemrograman berorientasi objek (Rosa A.S,2013).

2.2.2 Diagram-diagram dalam UML

Asosiasi bisa digunakan untuk memodelkan relasi diantara obyek-obyek. Nama dari asosiasi memberi informasi secara tepat tentang relasi apa yang sedang dimodelkan. “Di UML, ada relasi dengan perlakuan khusus yang disebut dengan “bagian dari (part of)” yang menangani antar obyek-obyek dimana salah satunya adalah bagian dari yang lain” (Rosa, dkk: 2011).

Berikut ini adalah beberapa jenis diagram yang digunakan dalam pembuatan diagram UML (Unified Modeling Language):

a. Use Case Diagram

“Use Case adalah deskripsi sebuah interaksi antara satu atau lebih aktor dengan sistem informasi yang akan dibuat” (Rosa, dkk: 2011). Use Case bekerja dengan cara mendeskripsikan tipikal interaksi antara user (pengguna) sebuah sistem dengan sistemnya sendiri melalui sebuah cerita bagaimana sebuah sistem dipakai. Urutan langkah-langkah yang menerangkan antara pengguna dan sistem disebut Scenario. Setiap Scenario mendeskripsikan urutan kejadian. Setiap urutan diinisialisasi oleh orang, sistem yang lain, perangkat keras atau urutan waktu. Dengan demikian secara singkat bisa dikatakan use case adalah serangkaian scenario yang digabungkan bersama-sama oleh tujuan umum pengguna.






Syarat penamaan pada use case adalah nama didefinisikan sesimpel mungkin dan dapat dipahami (Rosa, dkk: 2011). Ada dua hal utama pada use case yaitu pendefinisian apa yang disebut aktor dan use case.

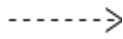
- a) Aktor merupakan orang, proses, atau sistem lain yang berinteraksi dengan sistem informasi yang akan dibuat di luar sistem informasi yang akan di buat itu sendiri.
- b) Use case merupakan fungsionalitas yang disediakan sistem sebagai unit-unit yang saling bertukar pesan antar unit atau aktor.

Berikut ini simbol-simbol yang sering digunakan pada saat pembuatan use case diagram, dapat kita lihat pada tabel 2.1 berikut ini

:

Tabel 2.1 Simbol-simbol Use Case Diagram

NO	GAMBAR	NAMA	KETERANGAN
1		Use Case	Deskripsi dari urutan aksi-aksi yang ditampilkan sistem yang menghasilkan suatu hasil yang terukur bagi suatu actor.
2		Actor	Menspesifikasikan himpunan peran yang pengguna mainkan ketika berinteraksi dengan use case.
3		Association	Apa yang menghubungkan antara objek satu dengan objek lainnya.
4		<<extend>>	Menspesifikasikan bahwa use case target memperluas perilaku dari use case sumber pada suatu titik yang diberikan.
5		Generalization	Hubungan dimana objek anak (descendent) berbagi perilaku dan struktur data dari objek yang ada di atasnya objek induk (ancestor).

6		<<include>>	Menspesifikasikan bahwa use case sumber secara eksplisit.
---	---	-------------	---




Sumber: Rosa,dkk (2011)




b. Activity Diagram

Activity diagram menggambarkan workflow (aliran kerja) atau aktifitas dari sebuah sistem atau proses bisnis (Rosa, dkk: 2011). Yang perlu diperhatikan disini adalah bahwa diagram activity menggambarkan aktivitas sistem bukan apa yang dilakukan aktor, jadi aktivitas yang dapat dilakukan oleh sistem.

Berikut ini simbol-simbol yang sering digunakan pada saat pembuatan activity diagram, dapat kita lihat pada tabel 2.2 berikut ini :

Tabel 2.2 Simbol-simbol Activity Diagram

NO	GAMBAR	NAMA	KETERANGAN
1		Status Awal	Bagaimana objek dibentuk atau diawali.
2		Aktivitas	Aktifitas yang dilakukan sistem, aktifitas biasanya diawali dengan kata kerja.
3		Decision	Asosiasi percabangan dimana jika ada pilihan aktifitas lebih dari satu.

4		Join	Asosiasi penggabungan dimana lebih dari satu aktivitas digabung menjadi satu.
5		Status Akhir	Status akhir yang dilakukan sistem, sebuah diagram aktivitas memiliki akhir.
6		Swimlane	Memisahkan organisasi bisnis yang bertanggung jawab terhadap aktivitas yang ada

Sumber: Rosa,dkk (2011)

c. Sequence Diagram

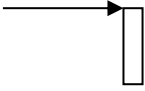
Sequence diagram menggambarkan interaksi antar objek di dalam dan di sekitar sistem (termasuk pengguna, display, dan sebagainya) berupa message yang digambarkan terhadap waktu. Sequence diagram digunakan untuk menggambarkan perilaku pada sebuah scenario yang diterapkan pada sistem untuk model penerapan pada bahasa pemrograman.

Berikut ini simbol-simbol yang sering digunakan pada saat pembuatan sequence diagram, dapat kita lihat pada tabel 2.5 berikut ini :

Tabel 2.3 Simbol-simbol Sequence Diagram

NO	GAMBAR	NAMA	KETERANGAN
----	--------	------	------------

1		Aktor	Orang, proses, atau sistem lain yang berinteraksi dengan sistem informasi yang akan dibuat di luar sistem.
2		Lifeline	Menyatakan kehidupan suatu objek
3		Objek	Merupakan objek yang berinteraksi pesan.
4		Waktu aktif	Menyatakan objek dalam keadaan aktif dan beriteraksi pesan.
5		Pesan tipe create	Menyatakan suatu objek memuat objek yang lain, arah panah mengarah pada objek yang dibuat.
6		Pesan tipe call	Menyatakan suatu objek memanggil oprasi/metode yang ada pada objek lain atau sendirinya sendiri.
7		Pesan tipe send	Menyatakan bahwa suatu objek mengirimkan data /masukan/informasi ke objek lainnya.
8		Pesan tipe return	Menyatakan bahwa suatu objek yang telah menjalankan suatu operasi atau metode menghasilkan suatu kembali ke

			objek tertentu.
9		Pesan tipe destroy	Menyatakan suatu objek mengakhiri hidup objek yang lain.

Sumber: Rosa,dkk (2011)

2.4 Pengertian Aplikasi

Menurut Nazrudin Safaat H (2012 : 9) Perangkat lunak aplikasi adalah suatu subkelas perangkat lunak komputer yang memanfaatkan kemampuan komputer langsung untuk melakukan suatu tugas yang diinginkan pengguna.

Biasanya dibandingkan dengan perangkat lunak sistem yang mengintegrasikan berbagai kemampuan komputer, tapi tidak secara langsung menerapkan kemampuan tersebut untuk mengerjakan suatu tugas yang menguntungkan pengguna. Contoh utama perangkat lunak aplikasi adalah pengolah kata, lembar kerja, dan pemutar media. Beberapa aplikasi yang digabung bersama menjadi suatu paket kadang disebut sebagai suatu paket atau suite aplikasi (application suite).

2.5 Pengertian Sistem Informasi

Menurut Laudon dan Laudon (2010, p46) sistem informasi merupakan komponen yang saling bekerja sama untuk mengumpulkan,

mengolah, menyimpan dan menyebarkan informasi untuk mendukung pengambilan keputusan, koordinasi, pengendalian, analisis masalah dan visualisasi dalam sebuah organisasi.

Aktifitas dasar dari Sistem Informasi menurut Laudon dan Laudon (2010, p46-47) adalah sebagai berikut :

1. Input

Melibatkan pengumpulan data mentah dari dalam organisasi atau dari lingkungan eksternal untuk pengolahan dalam suatu sistem informasi.

2. Process

Melibatkan proses mengkonversi input mentah ke bentuk yang lebih bermakna.

3. Output

Mentransfer proses informasi kepada orang yang akan menggunakannya atau kepada aktivitas yang akan digunakan.

4. Feedback

Output yang di kembalikan ke anggota organisasi yang sesuai untuk kemudian membantu mengevaluasi atau mengkoreksi tahap Input.

2.6 Perangkat lunak yang digunakan dalam membuat aplikasi

2.6.1 Website

Menurut (Yeni Kustiyahningsih, 2011) website (situs web) adalah kumpulan dari beberapa halaman web. Home page sering juga disebut

dengan website. Untuk bisa mengakses informasi yang terdapat didalam home page diperlukan suatu software tool yang disebut web browser untuk membaca HTML yang terdapat dalam suatu komputer.

Web terdiri atas beberapa jenis yaitu sebagai berikut :

1. Komersial, merupakan jenis web yang berekstensi .com dan .co.id
2. Pendidikan, merupakan jenis web yang berekstensi .edu.id dan .ac.id
3. Pemerintahan, merupakan jenis web yang berekstensi .go
4. Organisasi, merupakan jenis web yang berekstensi .go.id, .or. Id dan .ac.id

Website merupakan salah satu layanan yang didapat oleh komputer yang terhubung ke internet dengan fasilitas hypertext untuk menampilkan data berupa teks, gambar, suara, animasi dan multimedia lainnya.

2.6.2 HTML

Menurut (Yeni Kustiyahningsih, 2011) HTML adalah HyperText Markup Language, yaitu suatu format data yang digunakan untuk membuat dokumen hypertext yang dapat dibaca dari satu platform computer keplatform computer lainnya, tanpa perlu melakukan suatu perubahan apapun. HTML tidak hanya mampu menampilkan teks tapi juga dapat menampilkan format – format lain dari teks tersebut,

misalnya table, list, form, frame serta dapat digabungkan dengan objek suara, gambar, maupun video.

Dokumen yang berisi script HTML merupakan dokumen yang disajikan dalam bentuk website. Dokumen HTML disebut markup language karena mengandung tanda-tanda tertentu yang digunakan untuk menentukan tampilan suatu teks dan tingkat kepentingan dari teks tersebut dalam suatu dokumen. Kita dapat menentukan baris-baris mana yang merupakan judul menentukan gambar yang harus tampil, pengaturan format teks dan lain sebagainya.

2.6.3 CSS

Menurut (Yeni Kustiyahningsih, 2011) menyatakan bahwa CCS (Cascading Style Sheet) adalah kumpulan kode-kode yang berurutan dan saling berhubungan untuk mengatur format atau tampilan suatu halaman HTML.

Cascading Style Sheet (CSS) merupakan salah satu bahasa pemrograman web untuk mengendalikan beberapa komponen dalam sebuah web sehingga akan lebih terstruktur dan seragam. Sama halnya styles dalam aplikasi pengolahan kata seperti Microsoft Word yang dapat mengatur beberapa style, misalnya heading, subbab, bodytext, footer, images, dan style lainnya untuk dapat digunakan bersama-sama dalam beberapa berkas (file). Pada umumnya CSS dipakai untuk

memformat tampilan web yang dibuat dengan bahasa HTML dan XHTML.

CSS dapat mengendalikan ukuran gambar, warna bagian tubuh pada teks, warna tabel, ukuran border, warna border, warna hyperlink, warna mouse over, spasi antar paragraf, spasi antar teks, margin kiri, kanan, atas, bawah, dan parameter lainnya. CSS adalah bahasa style sheet yang digunakan untuk mengatur tampilan dokumen. Dengan adanya CSS memungkinkan kita untuk menampilkan halaman yang sama dengan format yang berbeda.

Ada dua sifat CSS yaitu internal dan eksternal. Jika internal yang dipilih, maka skrip itu dimasukkan secara langsung ke halaman website yang akan didesain. Kalau halaman web yang lain akan didesain dengan model yang sama, maka skrip CSS itu harus dimasukkan lagi ke dalam halaman web yang lain itu. Sifat yang kedua adalah eksternal dimana skrip CSS dipisahkan dan diletakkan dalam berkas khusus. Nanti cukup gunakan semacam tautan menuju berkas CSS itu jika halaman web yang didesain akan dibuat seperti model yang ada di skrip tersebut.

2.6.4 PHP

Menurut (Budi Raharjo, 2012) dalam Buku “Modul Pemrograman Web (HTML, PHP, & MYSQL)”. PHP adalah salah satu pemrograman skrip yang dirancang untuk membangun aplikasi web.

Ketika dipanggil dari web browser, program yang ditulis dengan PHP akan di-parsing didalamweb server oleh interpreter PHP dan diterjemahkan dalam dokumen HTML, yang selanjutnya akan ditampilkan kembali ke web browser. Karena pemrosesan program PHP dilakukan dilingkungan web server, PHP dikatakan sebagai bahasa sisi server (server-side) oleh sebab itu, seperti yang telah dikemukakan sebelumnya, kode PHP tidak akan terlihat pada saat user memilih perintah “view source” pada web browser yang mereka gunakan. Selain menggunakan PHP, aplikasi web juga dapat dibangun dengan Java (JSP- JavaServer Pages dan Servlet), Perl, maupun ASP (Active Server Pages).

Syntax Program PHP adalah bahasa yang dirancang untuk mudah diletakkan dalam kode HTML. Banyak dijumpai kode PHP yang menyatu dengan kode HTML. Kode PHP diawali dengan tag<?php dan diakhiri dengan tag ?>. apabila kita melakukan konfigurasi terhadap file PHP ini untuk mengizinkan pengguna tag pendek (short tag) dengan mengubah nilai short_open_tag menjadi on, maka tag tersebut dapat digantikan dengan <? dan ?>. dalam PHP, nilai default dari short_open_tag adalah off. Selain itu, PHP kita juga dapat menggunakan tag gaya ASP <% dan %>, dengan mengubah nilai asp_tags dalam file PHP ini menjadi on. Berikut ini contoh kode PHP :

```
<? Php
```



```
echo "Hello World";
```

```
?>
```

Perintah echo di dalam PHP berguna untuk mencetak nilai, baik teks maupun numerik ke layar web browser.

2.6.5 Javascript

Menurut (R.H. Sianipar, 2015) javascript adalah bahasa scripting yang populer di internet dan dapat bekerja di sebagian besar browser populer seperti Internet Explorer, Mozilla Firefox, Netscape dan Opera. Kode javascript dapat disisipkan dalam halaman web menggunakan tag script.

Berikut ini beberapa sifat dari javascript:

1. Menambahkan interaktivitas ke halaman HTML.
2. Merupakan bahasa pemrograman scripting.
3. Bahasa Scripting merupakan bahasa yang ringan.
4. Javascript merupakan bahasa terinterpretasi.

2.6.6 Bootstrap

Menurut (Husein Alatas, 2013) bootstrap merupakan Framework ataupun Tools untuk membuat aplikasi web ataupun situs web responsive secara cepat, mudah dan gratis.

Bootstrap terdiri dari CSS dan HTML untuk menghasilkan Grid, Layout, Typography, Table, Form, Navigation, dan lain-lain. Di dalam Bootstrap juga sudah terdapat jQuery plugins untuk menghasilkan

komponen UI yang cantik seperti Transitions, Modal, Dropdown, Scrollspy, Tooltip, Tab, Popover, Alert, Button, Carousel dan lain-lain.

Dengan bantuan Bootstrap, kita bisa membuat responsive website dengan cepat dan mudah dan dapat berjalan sempurna pada browser-browser populer seperti Chrome, Firefox, Safari, Opera dan Internet Explorer

2.6.7 jQuery

Menurut (Lukmanul Hakim, 2010) dalam buku Bikin Website Super Keren dengan PHP & jQuery, jQuery adalah Javascript Library berupa kumpulan kode/fungsi javascript siap pakai, sehingga mempermudah dan mempercepat kita dalam membuat kode javascript. Secara standar, apabila kita membuat kode javascript, maka diperlukan kode yang cukup panjang, bahkan terkadang sangat sulit dipahami, jQuery digunakan untuk menyederhanakan kode javascript. Hal ini sesuai dengan slogannya “Write lees, do more”, cukup tulis sedikit tapi bisa melakukan banyak hal.

2.6.8 MySQL

Menurut (R.H. Sianipar, 2015) dalam Buku “ Membangun Web dengan PHP & MYSQL untuk Pemula & Programmer ”. MySQL bukan termasuk bahasa pemrograman. MySQL merupakan salah satu database populer dan mendunia. MySQL bekerja menggunakan SQL Language (Structure Query Language). Pada umumnya, perintah yang

paling sering digunakan dalam MySQL adalah SELECT (mengambil), INSERT (menambah), UPDATE (mengubah), dan DELETE (menghapus). Selain itu, SQL juga menyediakan perintah untuk membuat database, field, ataupun index untuk menambah atau menghapus data.

