# PENERAPAN ALGORITMA KRIPTOGRAFI UNTUK PENGAMANAN DOKUMEN TRANSAKSI DENGAN METODE RIVEST SHAMIR ADLEMAN

**Bagus Tri Mahardika.,MMSI[1], Muhammad Rizky Alfian[2]**
[1]Dosen Program Studi Teknologi Informasi Universitas Darma Persada
[2]Program Studi Teknologi Informasi Universitas Darma Persada

Email: bagusunsada@gmail.com

**ABSTRAK**

*Beberapa tahun belakang ini teknologi informasi telah mengalami percepat, oleh karena itu harus diikuti dengan keamanan data dan informasi, Dengan menggunakan teknologi internet dan informasi, mewajibkan berbagai bidang usaha untuk melindungi dan mengamankan data digital mereka dari pihak yang tidak bertanggung jawab. Teknologi kritografi merupakan salah satu teknologi yang bisa digunakan untuk mengamankan data digital tersebut. Salah satunya pada keamanan data nasabah dibank. Salah satu algoritma untuk pengamanan adalah Rivest Shamir Adleman (RSA), dengan mengimplentasikan metode RSA pada sistem repository dokumen pada bank BTN yang di fokuskan untuk data nasabah KPR. Data nasabah KPR dalam bentuk file dokumen akan di enkripsi saat data di inputkan dalam sistem repository menggunakan algoritma RSA, selanjutnya data hanya bisa di akses melalui sistem repository karena file data hanya bisa di dekripsi melaui aplikasi repository.*

**Kata kunci**: Rivest Shamir Adleman (RSA), keamanan data digital, algoritma kriptografi, sistem repository

## 1. PENDAHULUAN

### 1.1 Latar Belakang

Data digital merupakan asset yang sangat penting, dalam teknologi informasi, dengan adanya teknologi internet yang semakin berkembang membuat para pengguna teknologi digital untuk semakin meningkatkan kemanan dan kerahasiaan data digital mereka dari pihak-pihak yang tidak memeliki kepentingan. Salah satu metode untuk mengamanakan data digital yaitu dengan menggunakan algoritma kriptografi Rivest Shamir Adleman (RSA). ALgoritma RSA dibangun oleh para peneliti dari MIT (Massachussets Institute of Technology) pada tahuan 1976, RSA merupakan teknik dimana kunci untuk enkripsi dibuat berbeda dengan kunci untuk deskripsi.

Sama halnya dengan keamanan data nasabah KPR pada Bank Tabungan Negara BTN demi menjaga seluruh data nasabah yang merupakan tanggung jawab pihak BTN, Peran manusia sebagai penjaga juga menjadi peran penting. Apalagi jika data digital tersebut terdapat pada jaringan internet. Tentu menjadi hal yang sangat rawan, dan masih belum bisa di katakan aman karena tidak ada keamanan tambahan didalamnya. Pasalnya dalam

implementasi saat ini pikah BTN masih menggunakan sistem aplikasi yang belum menggunakan ekripsi ataupun dekripsi dalam hal penyimpanan data nasabah KPR.

Pada pembuatan tugas akhir ini, penulis akan mengimplentasikan metode RSA pada sistem repository dokumen pada bank BTN yang di fokuskan untuk data nasabah KPR. Data nasabah KPR dalam bentuk file dokumen akan di enkripsi saat data di inputkan dalam sistem repository menggunakan algoritma RSA, selanjutnya data hanya bisa di akses melalui sistem repository karena file data hanya bisa di dekripsi melaui aplikasi repository. Ini diharapkan dapat meningkatkan keamanan sehingga tidak mudah untuk di akses orang yang tak berkepentingan kecuali *user* yang telah terdaftar pada sistem repository

### 1.2. Rumusan Masalah

Dari uraian pada latar belakang, dapat dirumuskan sebagai berikut :

a. Bagaimana membangun aplikasi repository dokumen BTN ?
b. Bagaimana cara mengimplementasikan metode RSA pada sistem repository dokumen BTN ?

### 1.2 Batasan Masalah

Terdapat beberapa pembatasan masalah antara lain:

a. Aplikasi repository dokumen ini hanya diperuntukan menyimpan data nasabah KPR.
b. Aplikasi repository dokumen ini dibuat hanya berbasis web.
c. Metode RSA di gunakan untuk enkripsi dan dekripsi file data.
d. File data yang di enkripsi berupa text.

### 1.3 Tujuan Dan Manfaat Penelitian

#### 1.3.1. Tujuan

Berdasarkan rumusan masalah, tujuan pada laporan ini antara lain :

1. Mengetahui cara untuk membangun sistem aplikasi repository dokumen pada BTN.
2. Mengetahui cara untuk membangun sistem aplikasi yang dapat melakukan enkripsi dan dekripsi dengan menggunakan metode RSA.

#### 1.3.2. Manfaat Penelitian

1. Dapat Menambah keamanan file data nasabah KPR pada BTN
2. Diharapkan hasil penulisan ini dapat menjadi ilmu pengetahuan baru atau sumber referensi untuk penelitian yang akan datang.

### 1.4 Metode Penelitian

Dalam penyusunan laporan ini digunakan beberapa metode penulisan, yaitu::

#### 1.4.1. Metode Pengumpulan Data

Studi Pustaka : Observasi dan Wawancara.

### 1.5 Metode perancangan waterfall

Pada pengembangan aplikasi ini menggunakan metode waterfall dengan beberapa fase antara lain fase – fase Analisa, desain, pembangunan, implementasi dan pengujian.

Berikut adalah tahapan dalam Metode Waterfall:

1. *Requirement* (analisis kebutuhan)

Pengumpulan data bisa dengan sebuah penelitian, wawancara, dan studi literatur. Hasil dari pengumpulan data dapat digunakan sebagai informasi yang akan diterapkan kedalam sistem

2. *Design System* (sistem desain)

   Desain sistem merupakan suatu permodelan awal perangkat lunak yang akan digunakan sebagai referensi developer untuk membangun sistem.

3. *Coding & Testing* (penulisan sinkode program / implementation)

   Bertujuan membangun dan mengevaluasi jika masih terdapat kesalahan didalamnya.

4. Penerapan / Pengujian Program (*Intergration & Testing*)

   Pada fase ini dapat dikatakan sistem sudah siap untuk digunakan dan dilakukan uji coba.

5. Pemeliharaan (*Evaluasi & Maintenance*)

   *Maintenance* sebuah sistem untuk pengembangan sistem yang baru, dan perubahan permintaan karena pelanggan membutuhkan pekembangan fungsional.

## 2. LANDASAN TEORI

### 2.1. RSA

RSA merupakan salah satu teknik pengamanan yang digunakan untuk melakukan enkripsi dan dekripsi secara berbeda. Algoritma RSA dikembangkan pada tahun 1976 di MIT (Massachussets Institute of Technology), yaitu: Ron (R)ivest, Adi (S)hamir, dan Leonard (A)dleman. Keamanan algoritma RSA tedapat pada rumitnya membuat faktor bilangan besar menjadi faktor-faktor prima. Hasil dari pemfaktoran adalah untuk mendapatkan kunci privat. Selama pembuatan factor pada bilangngan besar menjadi fakto untuk bilangan prima belum didapatkan, maka kemanan algoritma RSA masih terus terjaga.

Tujuan penggunaan algoritma kriptografi RSA antara lain.

*1. Confidentiality*

Menjaga data digital secara rahasia, menyimpan data dalam bentuk sandi informasi dengan Teknik enkripsi.

*2. Data Integrity*

Jaminan pada tiap bagian data digital tidak akan berubah pada saat data disimpan sampai dengan saat data tersebut dibuka

## 3. ANALISIS DAN PERANCANGAN SISTEM

### 3.1 Analisa Kebutuhan

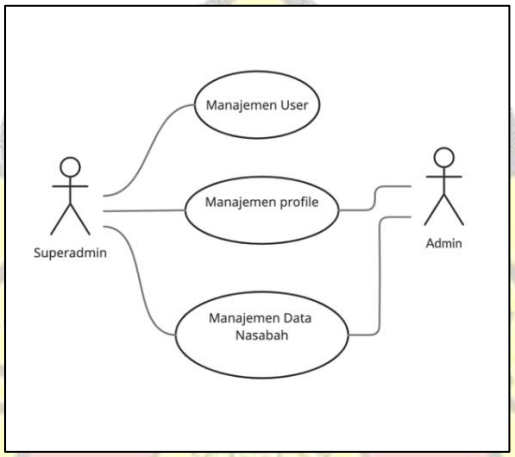
Berdasarkan hasil wawancara terhadap pihak karyawan BTN,dapat dibuat kesimpulan kebutuhan akan sebuah sistem yang dapat membatu dalam menyimpan dan memanajemen data nasabah KPR dan memiliki keamanan dari pihak luar ataupun dalam yang tidak bertanggung jawab serta bisa di gunakan kapan dan dimana pun. Sebab itu akan di buat aplikasi repository data nasabah KPR berbasis web yang bertujuan untuk menyelesaikan permasalahan tersebut.

### 3.2 Metode Perancangan Sistem

Perancangan sistem dibuat dengan menggunakan *Unified Modelling Language* (UML) dengan beberapa diagram yang akan digunakan, antara lain: *Use case model diagram, Activity model diagram,* dan *Squence model diagram*.

#### 3.2.1 Use case Diagram Superadmin dan Admin

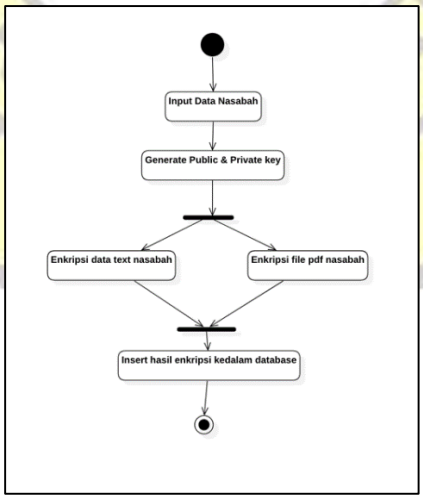
*Use Case model diagram* menjelaskan jenis interaksi yang dapat dilakukan oleh superadmin dan Admin ketika menjalankan aplikasi.




Gambar 1. Usecase Diagram Superadmin Dan Admin

#### 3.2.2 Activity model diagram

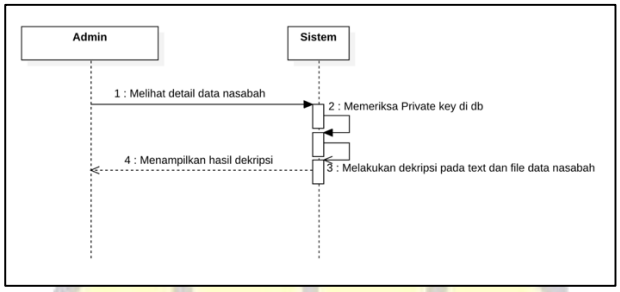
Berikut ini merupakan model activity diagram sistem saat superadmin atau admin melakukan tambah data nasabah KPR.




Gambar 2. Activity Diagram Input Data Nasabah.

### 3.2.3 Sequence model diagram

Berikut merupakan sequence model diagram saat superadmin ataupun admin ingin melihat detail data nasabah yang sudah di inputkan sebelumnya.




Gambar 3. Sequence Diagram Detail Data Nasabah.

### 3.3 Rancangan Database

Database digunakan untuk menyimpan data-data dari aplikasi. Berikut merupakan rancangan database dari aplikasi tersebut.

### 3.3.1 Tabel User

Tabel data user digunakan untuk menyimpan data berupa informasi dalam memanajemen user. Untuk lebih jelasnya terdapat pada tabel 3.1 berikut.

**Tabel 1.1** Struktur Tabel User

| NO | Nama Field | Tipe Data | Keterangan |
|---|---|---|---|
| 1 | Id | Int | Primary key |
| 2 | Username | Varchar | |
| 3 | Password | Varchar | |
| 4 | level | Tinyint | |

### 3.3.2 Tabel Nasabah

Tabel nasabah digunakan untuk menyimpan data nasabah KPR dan url source lokasi file data nasabah di simpan. Untuk lebih jelasnya terdapat pada tabel 3.2 berikut.

Tabel 2. Struktur Tabel Nasabah

| No | Nama Field | Type Data | Keterangan |
|---|---|---|---|
| 1 | Id | Int | Primary key |
| 2 | User_log | Int | |
| 3 | User_code | Varchar | |
| 4 | User_nik | Text | |
| 5 | User_name | Text | |
| 6 | User_email | Text | |
| 7 | File_path | Text | |
| 8 | Private_key | Text | |
| 9 | Status_en | Int | |

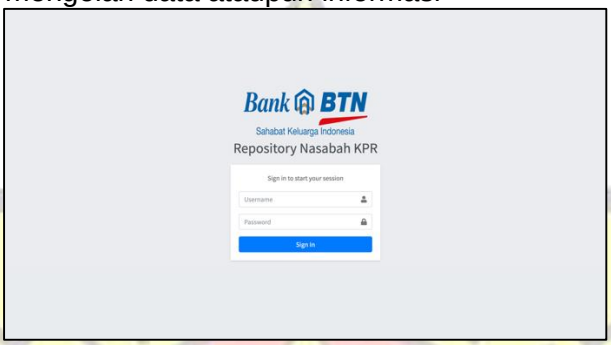
## 4. IMPLEMENTASI SISTEM DAN ANALISA HASIL

### 4.1. Implementasi Sistem

Setelah melakukan perancangan aplikasi, telah dilakukan uji coba pada sistem yang sudah dibangun. Hasil dari tampilan sistem tersebut sebagai berikut:

### 4.2.1 Tampilan Halaman Login

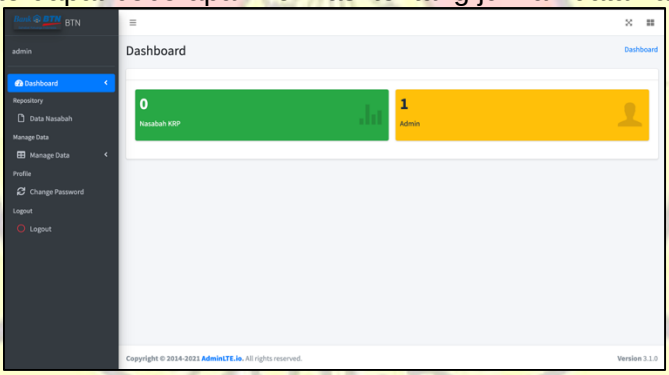
Berikut ini merupakan fitur login untuk superadmin ataupun admin sebelum masuk kedalam aplikasi untuk mengolah data ataupun informasi




Gambar 4.Fitur Halaman Login

### 4.2.2 Tampilan Fitur Dashboard

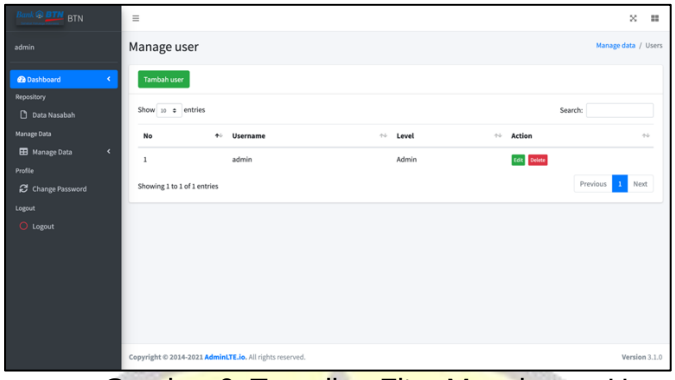
Pada fitur ini terdapat beberapa informasi tentang jumlah data nasabah dll.




Gambar 5. Tampilan Fitur Dashboard

### 4.2.3 Tampilan Fitur Manajemen User

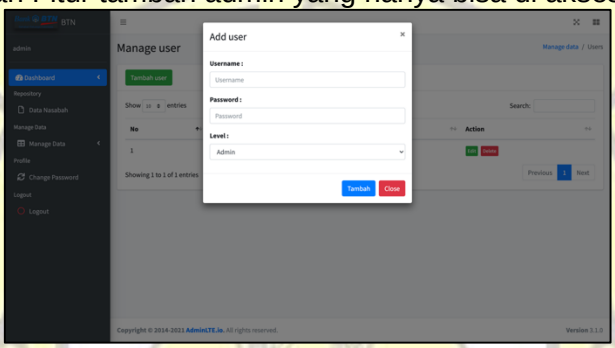
Pada halaman ini superadmin dapat mengelola admin yang dapat mengaskses data nasabah KPR.




Gambar 6. Tampilan Fitur Manajemen User

### 4.2.4 Tampilan Fitur Tambah User

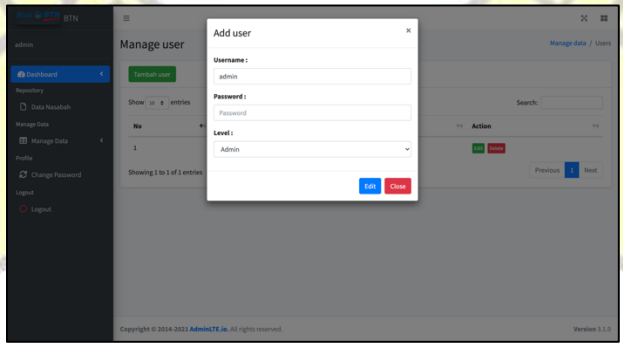
Berikut ini adalah Fitur tambah admin yang hanya bisa di akses oleh superadmin.




Gambar 7. Tampilan Fitur Tambah User

### 4.2.5 Tampilan Fitur Edit User

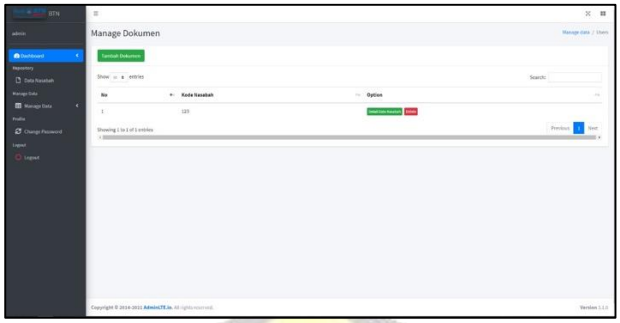
Berikut ini adalah fitur edit data admin yang hanya bisa dilakukan oleh superadmin.




Gambar 8. Tampilan fitur Edit User

### 4.2.6 Tampilan Fitur Manajemen Data Nasabah

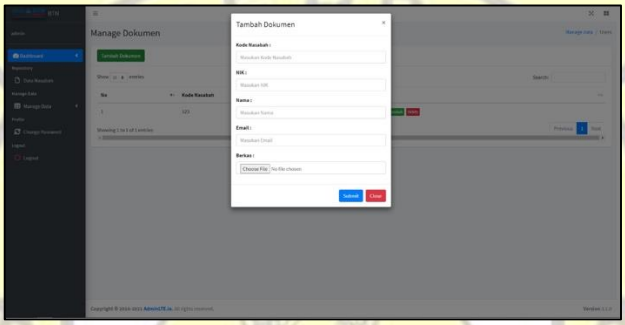
Berikut ini adalah fitur manajemen data nasabah KPR




Gambar 9. Tampilan Fitur Manajemen Data Nasabah

### 4.2.7 Tampilan Fitur Tambah Data Nasabah

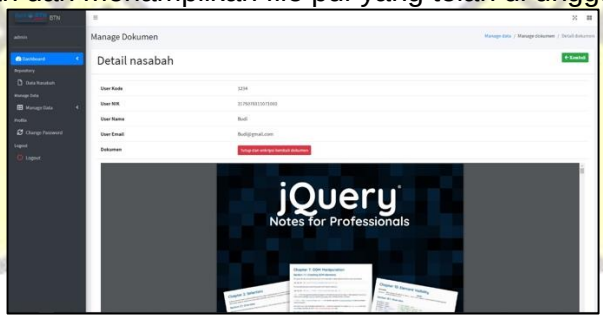
Berikut ini merupakan fitur untuk menambahkan data nasabah yang berisikan beberapa form serta form input file untuk melampirkan data nasabah berupa file pdf.




Gambar 10. Tampilan Fitur Tambah Data Nasabah

### 4.2.8 Tampilan Fitur Detail Data Nasabah

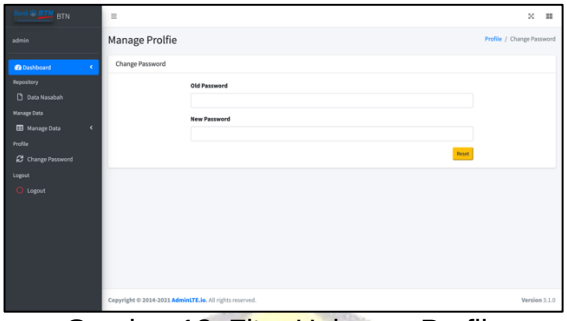
Berikut ini merupakan fitur detail data nasabah yang berisikan informasi dari nasabah yang telah di tambahkan dan menampilkan file pdf yang telah di unggah.




Gambar 11. Tampilan Fitur Detail Data Nasabah

### 4.2.9 Tampilan Halaman Profile

Berikut ini merupakan tampilan halaman profile yang bertujuan user dapat mengubah password.




Gambar 12. Fitur Halaman Profile

## 5. PENUTUP

### 5.1. Kesimpulan

Dari uraian bab sebelumnya dapat disimpulkan antara lain :

1. Aplikasi ini adalah sistem dengan teknologi web yang dibangun menggunakan bahasa pemrograman PHP, Javascript dan menggunakan Database MySQL. Untuk melakukan generate, enkripsi dan dekripsi metode RSA penulis memanfaatkan beberapa function yang sudah di sediakan oleh PHP.
2. Dengandilakukannya pemakaian aplikasi tersebut akan memudahkan pihak karyawan BTN khususnya bagian pengurus data nasabah KPR untuk mengelola dan mengawasi data nasabah KPR pada BTN

### 5.2. Saran

Beberapa saran untuk pengembangan sistem ini kedepannya antara lain:

1. Untuk kedepannya, desain tampilan dapat lebih dibuat interaktif dan menarik.
2. Sistem dapat dikembangkan lagi dengan menambah beberapa fitur, agar sistem menjadi lebih baik dan lebih lengkap dan mudah digunakan.

## DAFTAR PUSTAKA

1. Amin, M.M, 2016, ***Implementasi Kriptografi Klasik pada Komunikasi Berbasis Text***. Jurnal Pseudocode
2. Ariona, R., 2013, ***Belajar HTML dan CSS "Tutorial Fundamental dalam Mempelajari HTML dan CSS***, Ariona.net.
3. Hakim. Lukmanul, 2013, ***Proyek Website Super Wow dengan PHP & Jquery***, Yogyakarta: Lokomedia.
4. Shalahuddin, A.M, & Rosa, 2016, ***Sistem Informasi***, Jakarta, Salemba Empat.
5. Lubis, Adyanata, 2016, ***Basis Data Dasar***, Yogyakarta, Deepublish.
6. Sibero, Alexander F.K, 2014, ***Web Programming Power Pack***, Yogyakarta, Mediakom.
7. Yuliandru, A. R, 2016, ***Teknik Kriptografi Hill Cipher Menggunakan Matriks***, Makalah IF2123