Jurnal Elektronik Ilmu Komputer Udayana
Volume 12, No 1. August 2023

p-ISSN: 2301-5373
e-ISSN: 2654-5101

Penerapan Kriptografi RSA pada Rancang Bangun Aplikasi Koperasi Simpan Pinjam Berbasis Android

Ariffurrahman[a1], I Ketut Gede Suhartana[a2], I Gusti Ngurah Anom Cahyadi Putra[b3]

[a]Program Studi Informatika, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Udayana
Jalan Raya Kampus Unud, Badung, 80361, Bali, Indonesia
[1]Ariffurahman3@gmail.com
[2]ikg.suhartana@unud.ac.id

Abstract

Koperasi merupakan sebuah badan usaha yang beranggotakan sekumpulan orang yang kegiatannya berlandaskan prinsip kerjasama. Ataupun dapat disebut sebagai kegiatan ekonomi kerakyatan yang berasas kekeluargaan. Mensejahterakan nasabah atau anggota juga merupakan tujuan dari koperasi tersebut. Hampir keseluruhan sistem pelayanan ekonomi saat ini menggunakan sistem terkomputerisasi dan bahkan telah diterapkan juga pada perangkat komputer genggam atau seluler, yakni perangkat android. Begitupun dimaksudkan dalam penelitian ini untuk membangun sebuah aplikasi koperasi berbasis android sebagai pelayanan transaksi. Didalam proses transaksi pada aplikasi koperasi mobile ini menggunakan algoritma kriptografi RSA sebagai pengamanan untuk penyamaran data yang dilakukan. Data yang disamarkan dapat dipulihkan menjadi data awal hanya dengan pasangan kuncinya saja. Sedangkan untuk pengujiannya dilakukan dengan menggunakan RMSE (Root Mean Square Error) yang mendapat rata-rata hasil deskripsi 208,766377. Karna yang diuji adalah algoritma kriptografi maka semakin besar perbedaan antara data awal dan akhir, maka akan semakin baik pula karena proses dekripsinya pun akan menjadi semakin rumit.

Keywords: *Koperasi, Mobile Android, Algoritma RSA, RMSE*

1. Introduction

Pengaruh dari perkembangan teknologi membawa pengaruh juga pada sistem perekonomian dalam masyarakat. Rata-rata saat ini sistem ekonomi telah menerapkan komputerisasi pada setiap pelayanannya. Bahkan, telah banyak juga yang menggunakan layanan *mobile* atau perangkat seluler. Koperasi sebagai salah satu badan ekonomi masyarakat yang cukup populer pun ingin menerapkan hal yang sama yaitu dengan penggunaan sistem layanan seluler untuk memudahkan pelanggan dalam bertransaksi dalam koperasi. Koperasi memiliki pengertian badan usaha bersama yang berisi orang-orang yang menjalankan usaha dengan melandaskan kegiatan berdasarkan prinsip kerjasama sekaligus sebagai gerakan ekonomi rakyat yang berdasar atas asas kekeluargaan [2].

Android adalah sistem operasi dan patform pemrograman yang dikembangkan untuk pembangunan ekosistem aplikasi seluler bagi ponsel pintar dan perangkat seluler lain seperti tablet PC. Sedangkan aplikasi seluler *(mobile)* adalah program yang siap dipakai dan digunakan untuk menjalankan perintah pengguna dengan tujuan untuk mendapatkan hasil yang tepat sesuai dengan tujuan dari pembuatan aplikasi tersebut [1].

Algoritma kriptografi RSA adalah algoritma kriptografi modern yang dapat mengamankan informasi yang terdapat dalam suatu pesan [3]. Algoritma ini melakukan penfaktoran bilangan yang besar, sehingga membuatnya sulit untuk pecahkan. oleh karena alasan tersebut algoritma RSA dianggap aman. Untuk membangkitkan dua buah kunci, dipilih dua bilangan prima secara acak yang berukuran besar. Dan dalam pengoprasiannya teks asli (plainteks) yang dienkripsi akan di letakan ke dalam blok blok binner. Adapun tingkat kerahasian dipengaruhi oleh memfaktorkan bilangan besar ke bilangan prima yang digunakan.

2. Reseach Methods

Adapun jenis penelitian yang digunakan pada penelitian ini adalah penelitan lapangan kualitatif eksperimental. Penelitian kualitatif bersifat deskriptif dan cenderung menggunakan analisis. Proses dan makna (perspektif subyek) lebih ditonjolkan dan landasan teori dimanfaatkan.

2.1. Sumber Data

Sumber data pada penelitian ini diperoleh dari kumpulan buku mengenai pemrograman android, keamanan data, kriptografi dan dari e-book, jurnal tentang penelitian terdahulu, serta dari telusuran internet.

2.2. Metode Pengumpulan Data

Metode pengumpulan data yang digunakan adalah studi literatur, studi dokumentasi dan observasi.

a. Studi Literatur

Studi literatur adalah metode pengumpulan data dengan cara mempelajari hal-hal yang berkaitan seperti membaca buku atau jurnal.

b. Studi Dokumentasi

Mempelajari dokumentasi program serupa yang berupa source code untuk digunakan sebagai contoh dalam proses pembuatan perangkat lunak.

c. Observasi

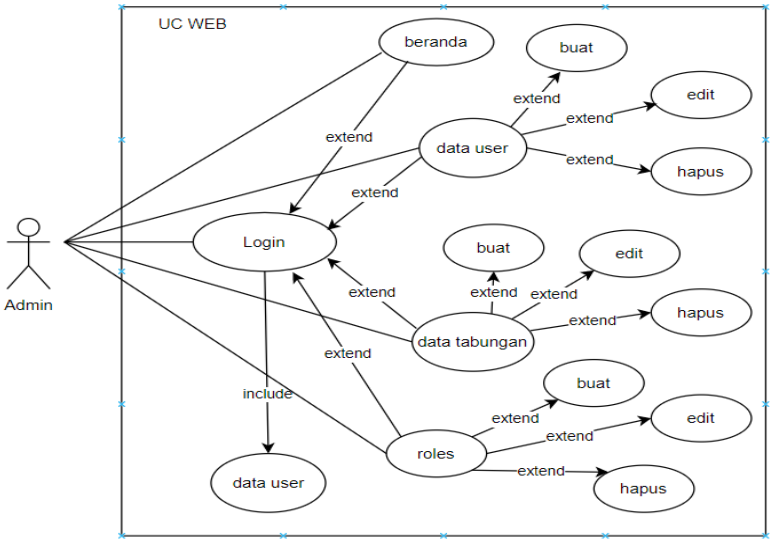
Mengamati proses secara langsung terhadap beberapa perangkat lunak yang mirip.

2.3. Perancangan Sistem

Perancangan sistem dibuat dengan menggunakan UML (Unifield Modelling Languange).

a. Use Case Diagram

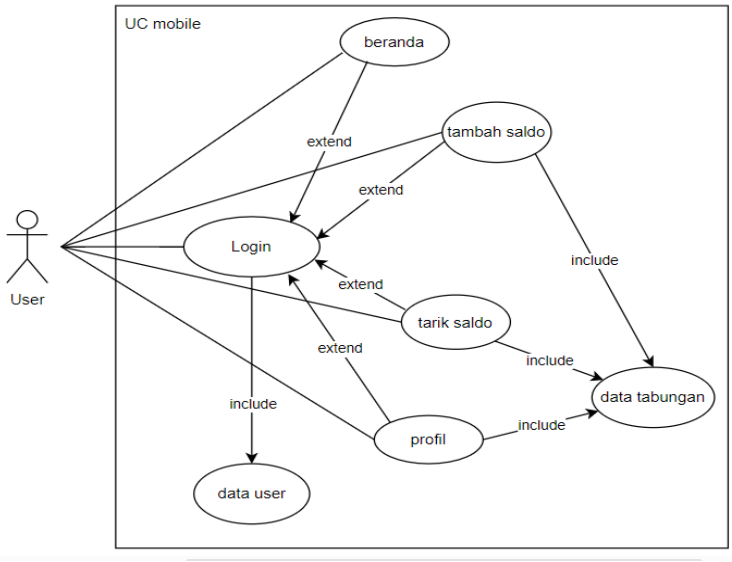
Selanjutnya adalah menggunakan Use Case Diagram, diagram ini digunakan untuk melihat hubungan yang terjadi antara pengguna dengan aplikasi serta aktivitas yang dapat dilakukan.



Gambar 1. *Use Case* Diagram Admin

Pada Gambar 1. Di ditunjukan admin sebagai aktor dapat melakukan interaksi terhadap sistem melalui *login*. Setelah *login* admin dapat memilih berbagai menu yang berguna untuk mengatur data pada sistem koperasi. Dimana terdapat menu “data user” untuk mengelola pengguna yang terdaftar dalam sistem, lalu menu “data tabungan” yang berguna untuk mengelola data-data tabungan dari setiap pengguna, dan juga menu “*roles*” yang fungsi sebagai tempat pemgaturan peran dari *user* yang terdaftar apakah sebagai pengguna biasa (nasabah) atau sebagai pengelola (admin).

p-ISSN: 2301-5373
e-ISSN: 2654-5101

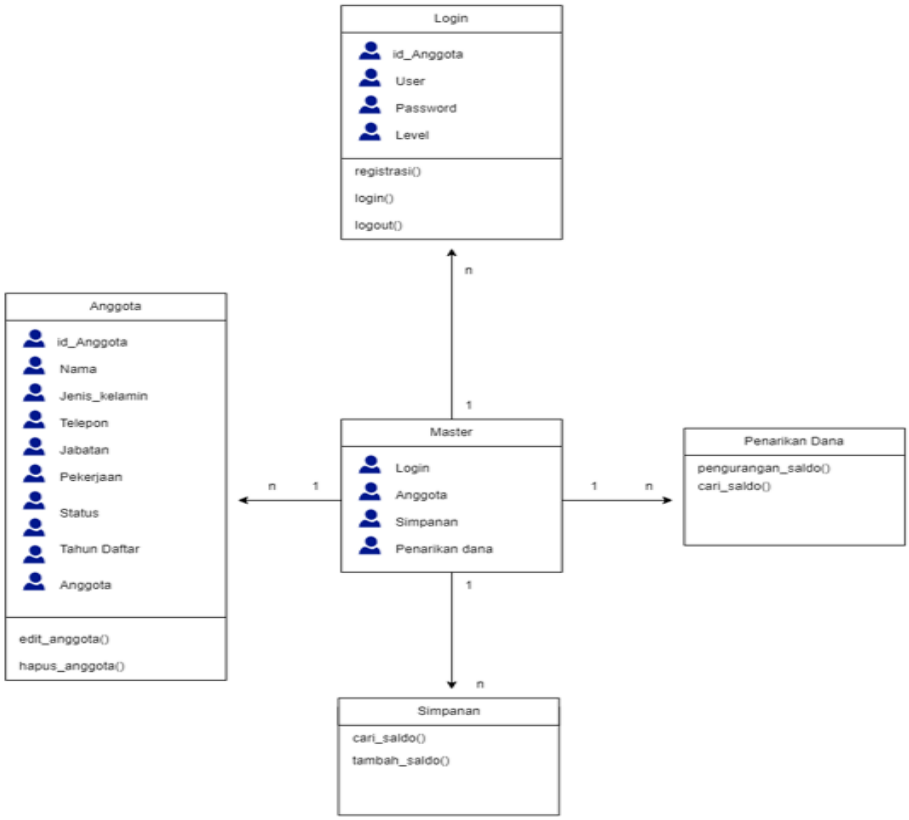


Gambar 2. *Use Case* Diagram *User*

Pada gambar 2. Ditunjukan user sebagai aktor dapat melakukan interaksi terhadap sistem melalui login. Setelah login, akan berlanjut dengan pilihan menu halaman utama, tarik saldo, tambah saldo, dan profil. Dengan 4 menu tersebut user dapat melakukan transaksi sesuai dengan nama menu tersebut. Sedangkan untuk menu profil sendiri memiliki beberapa fungsi didalamnya seperti menampilkan data profil pengguna, jumlah saldo, sejarah transaksi dan juga tombol logout bagi user terdapat didalam menu ini.

b. Class Diagram

Berikut ini adalah gambar Class Diagram yang berisi komponen-komponen himpunan entitas dan himpunan relasi masing-masing dilengkapi dengan atribut-atribut elemen untuk membentuk sebuah sistem. Dapat dilihat seperti pada gambar 3. Dibawah ini.



Gambar 3. *Class Diagram* sistem

2.4. Perancangan Basis Data

Desain database yang digunakan untuk menentukan struktur dari tabel-tabel yang dibuat. berisikan nama-nama field, type field dan ukurannya, yaitu sebagai berikut :

Tabel 1. Anggota

Field Name	*Type*	*Width*	Keterangan
Id_anggota	Int	50	Id_anggota
nama	Varchar	100	nama
username	Varchar	50	username
password	Varchar	50	password
jenis_kelamin	Varchar	50	jenis_kelamin
telepon	Int	50	telepon
pekerjaan	Varchar	50	pekerjaan
status	Varchar	50	status
tahun_daftar	Varchar	50	tahun_daftar
alamat	Varchar	200	alamat

Tabel anggota menyimpan data-data anggota yang terdaftar dengan beberapa atribut seperti biodata diri untuk membedakan tiap-tiap user.

Tabel 2. Grup

Field Name	*Type*	*Width*	Keterangan
Id_grup	Int	50	Id_grup
Jabatan	Varchar	100	Jabatan

Tabel grup berguna untuk menyimpan tingkatan user. Misalnya user yang hanya sebagai nasabah akan dibedakan hak aksesnya dengan user yang berlaku sebagai admin
.

Tabel 3. Tabungan

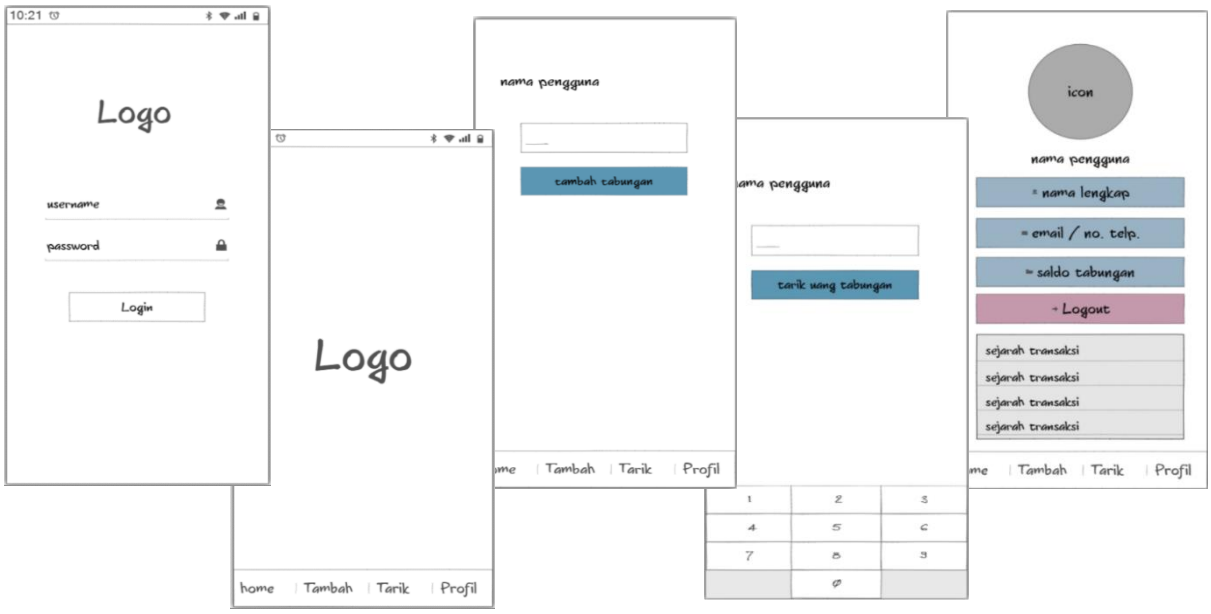
Field Name	*Type*	*Width*	Keterangan
Id_tabungan	Int	50	Id_tabungan
Id_anggota	Int	50	Id_anggota
setoran	Int	50	setoran
penarikan	Int	50	penarikan
saldo	Int	50	saldo

Tabel tabungan menyimpan data-data tabungan dari user seperti nilai setoran, penarikan dan saldo tersimpan.

2.5. Perancangan Tampilan Antarmuka

Berikut merupakan rancangan sederjana tampilan antar muka dari aplikasi koperasi mobile.
Pada contoh gambar 4. dibawah ini menunjukan beberapa tampilan antarmuka, dimulai dengan tampilan awal aplikasi, login, menu tambah saldo tabungan, tarik tabungan, dan profil.

p-ISSN: 2301-5373
e-ISSN: 2654-5101



Gambar 4. Rancangan tampilan aplikasi

3. Hasil dan Pembahasan

Pada tahap ini menunjukan pembahasan dari implementasi desain dan perhitungan yang terjadi dalam sistem.

3.1. Implementasi Sistem

3.1.1 Proses perhitungan kriptografi

a. Proses Pembuatan Kunci

Algoritma pembangkit kunci yakni dengan mengambil 2 bilangan prima besar yaitu n = p x q yang sangat sulit untuk difaktorisasikan. Direkomendasikan besar p dan q adalah 512 bit sehingga n berukuran 1024 bit. Karena p dan q adalah prima, maka n = (p – 1) (q – 1). Kemudian pilih sebuah integer e dipilih secara acak dari $Z_{\phi}(n)$ yang memenuhi gcd(e,ϕ(n)) sehingga e merupakan generator pada $Z_{\phi}(n)$. Selanjutnya algoritma pembangkit kunci RSA menghitung d invers perkalian e pada $Z_{\phi}(n)$. Pada akhirnya algoritma pembangkit kunci RSA menetapkan (e,n) sebagai kunci publik dan d sebagai kunci privat atau tetap dirahasiakan [5]. Langkah-langkah dalam pembangkit kunci RSA adalah:

- Pilih dua buah bilangan prima sembarang p dan q. nilai p dan q harus dirahasiakan.
- Hitung nilai n dari rumus, n – p x q. Besaran n tidak perlu dirahasiakan.
- Hitung m = (p – 1) (q – 1). Bersaran m perlu dirahasiakan.
- Dipilih sebuah bilangan bulat sebagai kunci publik, disebut namanya e, yaitu relativ prima terhadap m. e relative prima terhadap m artinya factor pembagi terbesar keduanya adalah 1- secara matematis disebut gcd (e,m)=1. Untuk mencarinya dapat digunakan algoritma Euclid. Nilai e bersifat tidak rahasia.
- Hitung kunci privat, disebut namanya d sedemikian agar (d x e) mod m=1. Untuk mencari d yang sesuai dapat juga digunakan algoritma Extended Euclid.

Maka hasil dari algoritma tersebut diperoleh

a. Kunci public adalah pasangan (e,n) bersifat tidak rahasia.
b. Kunci privat adalah pasangan (d,n) bersifat rahasia.

b. Proses Pembangkit Kunci

Pembangkit kunci merupakan bilangan yang menentukan kunci enkripsi (public key) dan kunci dekripsi (private key) dengan syarat :

- Pilihlah bilangan prima sembarang. Bilangan prima adalah bilangan asli yang lebih besar dari 1, yang tidak dapat dibagi oleh bilangan lain kecuali bilangan itu sendiri dan 1 yang tidak dapat dibagi oleh bilangan lain kecuali bilangan itu sendiri dan 1. Karena bilangan prima lebih besar dari 1, maka bilangan prima dimulai dari 2, yaitu 2,3,5,7,11,13 dan seterusnya. Seluruh bilangan prima adalah ganjil, kecuali 2 yang merupakan bilangan genap. Secara sistematis tidak ada “bilangan prima yang terbesar” karena jumlah bilangan prima tak terhingga dan kedua bilangan prima tidak boleh sama antara p dan q dalam pemilihan ini, dipilihlah nilai prima (p)=47 dan quotient (q)= 71. [5].
- Untuk mencari nilai dari kedua bilangan prima. Maka, perlu dilakukan perkalian yaitu n = p * q = 47 * 71 = 3337.
- Hitung m = (p – 1) (q – 1) = 46 * 71 = 3220.
- Pilih nilai e dengan syarat e > 1 dan pembagi persekutuan terbesar (e,3220) = 1 nilai e yang diambil adalah 101.

  Bukti : (101,3220)

  3220 mod 101=89

  101 mod 89 = 12

  89 mod 12 = 5

  12 mod 5 = 2

  5 mod 2 = 1

  2 mod 1=0

- Sehingga d e = 1 (mod 3220) dan d < 3220

Mencari nilai = d x 101 = 1 mod 3220 d x 101 mod 3220 = 1 d = 1881 Bukti : 1881 x 101 mod 3220 = 1 Sehingga pasangan kunci yang didapat adalah kunci enkripsi (public key) =(101,3337) dan kunci dekripsi (private key) = (1881,3337).0

c. Proses Enkripsi & Dekripsi

Setelah didapat perhitungan diatas, maka akan dilakukan enkripsi plaintext P = 200000 pertama-tama plaintext tersebut diubah menjadi format ASCII [4]. Sebagai berikut :

Karakter	2	0	0	.	0	0	0
ASCII	50	48	48	46	48	48	48

Setelah dibagi perblock, maka akan dihitung menggunakan rumus sebagai berikut yaitu

Ci=Pi ^e mod n.

C1 = 50 ^ 101 mod 3337 = 1071

C2 = 48 ^ 101 mod 3337 = 471

C3 = 48 ^ 101mod 3337 = 471

C4 = 46 ^ 101 mod 3337 = 46

C5 = 48 ^ 101 mod 3337 = 471

C6 = 48 ^ 101 mod 3337 = 471

C7 = 48 ^ 101 mod 3337 = 471

Maka chipertext yang didapatkan C = 1071 471 471 46 471 471 471

Setelah chipertext dari 200.000 didapat, untuk mengubah kembali jadi plaintext menggunakan dekripsi dengan rumus Pi = Ci ^ d mod n.

P1 = 1071 ^ 1881 mod 3337 = 50

P2 = 471 ^ 1881 mod 3337 = 48

P3 = 471 ^ 1881 mod 3337 = 48

p-ISSN: 2301-5373
e-ISSN: 2654-5101

P4 = 46 ^ 1881 mod 3337 = 46

P5 = 471 ^ 1881 mod 3337 = 48

P6 = 471 ^ 1881 mod 3337 = 48

P7 = 471 ^ 1881 mod 3337 = 48

Maka, setelah dideskripsi hasil akan sama yaitu 50 48 48 46 48 48 48. Dalam karakter ASCII yaitu: ASCII 50 48 48 46 48 48 48 Karakter 2 0 0 . 0 0 0

d. Pengujian

Pengujiannya dilakukan dengan tahapan uji kemiripan data saat sudah dienkripsi dan sebelum data dienkripsi pada program. Pengujian ini menggunakan RMSE (Root Mean Square Error) agar dapat mengetahui perbedaan dan kualitas hasil dari pengujian dari program yang sudah dibuat. Karakter chipertext dan karakter plaintext akan diubah terlebih dahulu ke dalam bilangan ASCII kemudian dilakukan proses perhitungan sesuai dengan rumus. maka proses dapat langsung dihitung dengan rumus.

$$\frac{1}{n}\sqrt{\sum_{i=1}^{n}(zi' - zi)^2}$$

Keterangan :

n = jumlah total inputan pesan

zi'= nilai pesan hasil (chipertext)

zi = nilai pesan asli (Plaintext)

id	plain	plain_ascii	chiper	sigma	created_at
5	14500	49 52 53 48 48	103 532 59 108 108	240552	2023-01-03 00:06
6	0	48	108	3600	2023-01-03 00:06
7	24500	50 52 53 48 48	50 532 59 108 108	237636	2023-01-03 00:06
8	0	48	108	3600	2023-01-03 00:06
9	35800	51 53 56 48 48	51 59 515 108 108	217917	2023-01-03 00:07

Gambar 5. Perbandingan RMSE

Diambilkan salah satu baris data transaksi yang pernah dilakukan pada gambar 5. dan dimasukan kedalam rumus berikut.-

$$\frac{1}{n}\sqrt{\sum_{i=1}^{n}(zi' - zi)^2} = \frac{1}{n}\sqrt{217917}$$

$$= \frac{1}{5}\sqrt{217917}$$

$$= \sqrt{\frac{217917}{5}}$$

$$= \sqrt{43.583{,}4}$$

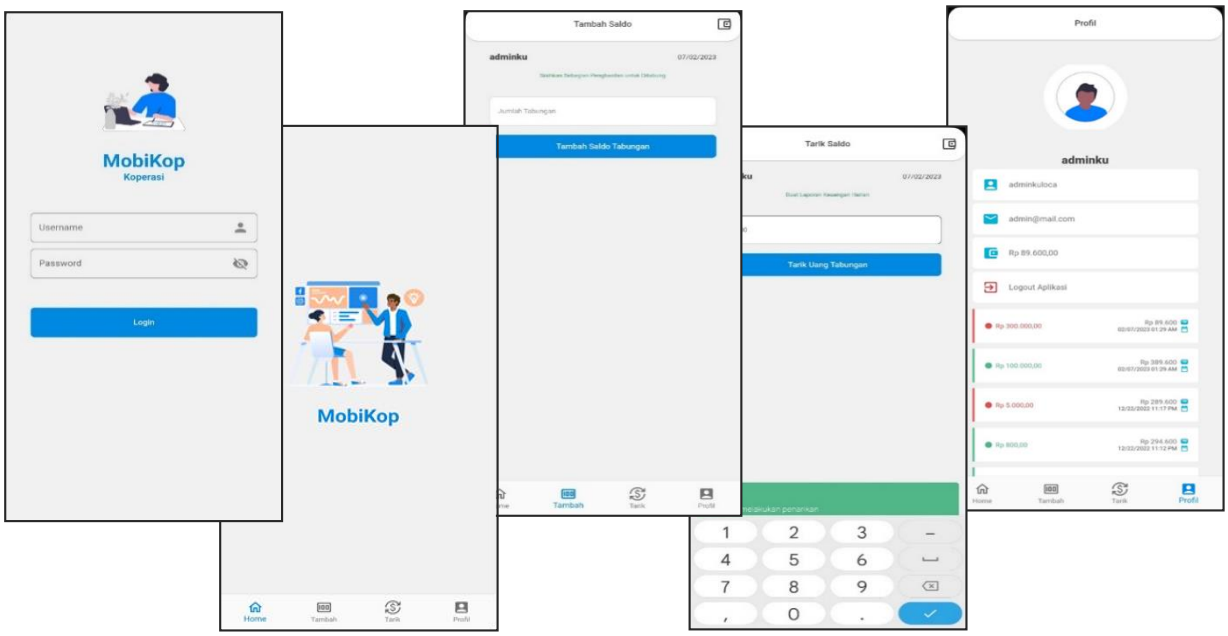
$$= 208{,}766377$$

Pada hasil perhitungan baris ke-5 data pada gambar 5. yang dilakukan dalam percobaan ini mendapatkan nilai rata-rata sebesar 208,766377.

Nilai hasil dari RSME memiliki kisaran terendah dari 0 sampai dengan ∞ (tidak terbatas). Penentuan nilai RMSE dikatakan semakin baik apabila nilai kemiripan antara nilai awal dan nilai akhir semakin kecil atau mendekati 0. Namun, karna pada pengujian ini nilai yang dihitung adalah nilai enkripsi, Maka, makin besar nilai perbedaan antara nilai awal (plaintext) dan nilai akhir (chipertext) akan semakin baik.

3.1.2 Tampilan Antarmuka

Berikut merupakan adalah tampilan antarmuka dari aplikasi koperasi mobile. Gambar 6. dibawah ini menunjukan beberapa tampilan antarmuka aplikasi, dimulai dengan tampilan awal login aplikasi, menu home atau beranda, menu tambah saldo tabungan, menu tarik tabungan, dan menu profil



Gambar 6. Tampilan aplikasi koperasi *mobile*

4. Kesimpulan

Berdasarkan dari hasil pembahasan sebelumnya dan pengamatan yang telah dilakukan maka dapat diambil kesimpulan diantaranya sebagai berikut:

1. Algoritma RSA ternyata bisa bekerja dengan baik pada pengaplikasiannya di aplikasi koperasi mobile meskipun terkadang memiliki masalah pada besarnya komputasi yang ditimbulkan apabila penggunaan nilai maksimal tidak dibatasi.
2. Hasil dari pengujian yang dilakukan dengan RMSE didapatkan hasil dengan nilai 208,766377. Hasil dari pengujian yang dilakukan dengan RMSE dianggap makin baik apabila nilai hasil pengujian mendekati 0. Namun pada pengujian ini nilai yang dihitung adalah nilai enkripsi, yangmana makin besar nilai perbedaan antara nilai awal (plaintext) dan nilai akhir (chipertext) akan semakin baik karena berarti sistem telah berhasil menyamarkan nilai asli dari pesan yang disandikan tersebut.

There are no sources in the current document.

Daftar Pustaka

[1]. Hendriyani Y. dan Suryani K., Pemrograman Android Teori dan Aplikasi. Pasuruan, Qiara Media, 2020. pp. 2-30.

[2]. Sattar, Buku Ajar Ekonomi Koperasi, Yokyakarta, Deepublish, 2017, pp. 31-33.

[3]. Harun Mukhtar, Kriptografi Untuk Keamanan Data, Yokyakarta, Deepublish, 2018, pp.12-22.

[4]. Sulaiman R. dan Vebu M., “Peningkat Keamanan Pesan Berbasis Android Menggunakan Algoritma RSA” pada *Jurnal SISFOKOM*, Vol. 7, No. 2, p.116-167. 2018.

[5]. Giri Adi N. dan Hari M., “Implementasi Kriptografi pada Aplikasi Memo Berbasis Android Menggunakan Algoritma RSA” pada *Prosiding SENDI_U 2019,* Semarang, 2019, pp. 293-300.

This page is intentionally left blank