SISTEM DISTRIBUSI *E-BOOK* BERBASIS KRIPTOGRAFI ASIMETRIS MENGGUNAKAN ALGORITMA RSA UNTUK PERLINDUNGAN HAK CIPTA

Disusun Oleh:

N a m a : Vyo Uvan Arywa

NIM : 20523137

PROGRAM STUDI INFORMATIKA – PROGRAM SARJANA

FAKULTAS TEKNOLOGI INDUSTRI

UNIVERSITAS ISLAM INDONESIA

2025

HALAMAN PENGESAHAN DOSEN PEMBIMBING

SISTEM DISTRIBUSI *E-BOOK* BERBASIS KRIPTOGRAFI ASIMETRIS MENGGUNAKAN ALGORITMA RSA UNTUK PERLINDUNGAN HAK CIPTA

TUGAS AKHIR

Disusun Oleh:

N a m a	: Vyo Uvan Arywa
NIM	: 20523137

Yogyakarta, 30 Desember 2024

Pembimbing,

(Dr. Raden Teduh Dirgahayu, S.T., M.Sc.)

HALAMAN PENGESAHAN DOSEN PENGUJI

SISTEM DISTRIBUSI *E-BOOK* BERBASIS KRIPTOGRAFI ASIMETRIS MENGGUNAKAN ALGORITMA RSA UNTUK PERLINDUNGAN HAK CIPTA

TUGAS AKHIR

Telah dipertahankan di depan sidang penguji sebagai salah satu syarat untuk memperoleh gelar Sarjana Komputer dari Program Studi Informatika – Program Sarjana di Fakultas Teknologi Industri Universitas Islam Indonesia

Yogyakarta, 13 Januari 2025

Tim Penguji

Dr. Raden Teduh Dirgahayu, S.T, M.Sc. _____

Anggota 1

Erika Ramadhani, S.T., M.Eng. _____

Anggota 2

Dr. Nur Wijayaning Rahayu, S.Kom, M.Cs. _____

Mengetahui,

Ketua Program Studi Informatika – Program Sarjana

Fakultas Teknologi Industri

Universitas Islam Indonesia

(Dhomas Hatta Fudholi, S.T., M.Eng., Ph.D.)

HALAMAN PERNYATAAN KEASLIAN TUGAS AKHIR

iv

Yang bertanda tangan di bawah ini:

Nama : Vyo Uvan Arywa

NIM : 20523137

Tugas akhir dengan judul:

SISTEM DISTRIBUSI E-BOOK BERBASIS KRIPTOGRAFI ASIMETRIS MENGGUNAKAN ALGORITMA RSA UNTUK PERLINDUNGAN HAK CIPTA

Menyatakan bahwa seluruh komponen dan isi dalam tugas akhir ini adalah hasil karya saya sendiri. Apabila di kemudian hari terbukti ada beberapa bagian dari karya ini adalah bukan hasil karya sendiri, tugas akhir yang diajukan sebagai hasil karya sendiri ini siap ditarik kembali dan siap menanggung risiko dan konsekuensi apapun.

Demikian surat pernyataan ini dibuat, semoga dapat dipergunakan sebagaimana mestinya.

Yogyakarta, 30 Desember 2024

(Vyo Uvan Arywa)

HALAMAN PERSEMBAHAN

Alhamdulillahirabbil'alamin, dengan mengucap syukur kepada Allah SWT atas segala berkat rahmat dan hidayah-Nya, skripsi ini penulis persembahkan kepada kedua orang tua saya, Bapak Arga Sukwantoro dan Ibu Damayanti, serta kedua adik saya, Enzo Uvan Arywa dan Neo Uvan Arywa, yang selama ini telah memberikan doa, kasih, dukungan dan motivasi sehingga penulis dapat menyelesaikan skripsi ini. Skripsi ini juga penulis persembahkan kepada dosen pembimbing, Bapak Dr. Raden Teduh Dirgahayu, S.T., M.Sc., yang telah memberikan bimbingan, ilmu, dan arahan kepada penulis selama masa pengerjaan skripsi. Terakhir, skripsi ini penulis persembahkan kepada seluruh teman penulis yang tak dapat penulis sebutkan satu per satu, yang telah membersamai penulis dari awal hingga selesai pengerjaan skripsi. Semoga skripsi ini bisa memberikan manfaat bagi pihak-pihak yang terkait. *Aamin ya rabbal'alamin*.

HALAMAN MOTO

"Dan bersabarlah. Sesungguhnya Allah bersama orang-orang yang sabar."
(Q.S. Al-Anfal : 46)

"*Long love all the magic we made.*"
(Taylor Swift)

"*We know what we are, but know not what we may be.*"
(William Shakespeare)

"*Do, or do not. There is no try.*"
(Yoda)

KATA PENGANTAR

Alhamdulillahirabbil'alamin, segala puji dan syukur penulis panjatkan atas kehadiran Allah SWT atas berkat rahmat dan hidayah-Nya, penulis dapat menyelesaikan penyusunan tugas akhir skripsi yang berjudul "Pengembangan Sistem Distribusi *E-book* Berbasis Kriptografi Asimetris Menggunakan Algoritma RSA untuk Perlindungan Hak Cipta" untuk memenuhi salah satu persyaratan untuk menyelesaikan pendidikan pada Program Sarjana Informatika Universitas Islam Indonesia.

Penulis ingin mengucapkan terima kasih kepada seluruh pihak berkat dukungan dan doa telah diberikan, sehingga penulis dapat menyelesaikan tugas akhir ini. Dengan rendah hati, penulis ingin mengucapkan terima kasih sebesar-besarnya kepada:

1. Kedua orang tua tercinta, Bapak Arga Sukwantoro dan Ibu Damayanti, serta kedua adik saya, Enzo Uvan Arywa dan Neo Uvan Arywa, yang senantiasa memberikan doa dan dukungan kepada penulis selama menyelesaikan tugas akhir.
2. Bapak Dr. Raden Teduh Dirgahayu, S.T., M.Sc., selaku Ketua Program Studi Informatika Universitas Islam Indonesia sekaligus dosen pembimbing yang telah memberikan bimbingan dan masukan kepada penulis selama pengerjaan tugas akhir.
3. Ibu Sheila Nurul Huda, S.Kom., M.Cs., selaku dosen pembimbing akademik.
4. Bapak Dhomas Hatta Fudholi, S.T., M.Eng., Ph.D., selaku Ketua Program Studi Informatika Program Sarjana Universitas Islam Indonesia.
5. Bapak dan Ibu dosen Program Studi Informatika, atas ilmu yang diberikan selama masa perkuliahan.
6. Teman-teman seperjuangan dari Program Studi Informatika Angkatan 2020, semoga kalian sehat dan sukses selalu dimana pun kalian berada.
7. Teman-teman dari komunitas Sobomaos dan Yogyakarta Book Party, yang telah memberikan motivasi baru dan tempat singgah yang nyaman bagi penulis selama penyelesaian tugas akhir.
8. Teman-teman daring dari komunitas *booktwt* yang telah membersamai penulis selama tiga tahun terakhir.

Penulis menyadari bahwa tugas akhir ini masih terdapat banyak kekurangan. Oleh karena itu, penulis meminta maaf apabila terdapat kesalahan dalam perkataan yang kurang berkenan dan terbuka untuk berbagai kritik dan saran. Akhir kata, semoga tugas akhir ini dapat menjadi

manfaat bagi perkembangan ilmu pengetahuan dalam bidang terkait. *Aamin ya rabbal'alamin*.

Yogyakarta, 30 Desember 2024

(Vyo Uvan Arywa)

SARI

Pengembangan sistem distribusi dan aplikasi pembaca *e-book* merupakan pengembangan sistem yang berfokus pada penerapan algoritma kriptografi asimetris, yaitu algoritma yang menggunakan sepasang kunci, kunci privat dan kunci publik. Sistem ini dikembangkan berdasarkan fakta bahwa maraknya fenomena pembajakan buku digital yang terjadi saat ini, yang merupakan pelanggaran hak cipta. Akibatnya, seluruh pihak yang terlibat dalam pendistribusian *e-book* akan mengalami kerugian yang besar.

Sistem ini merupakan sistem berbasis web yang dikembangkan menggunakan bahasa pemrograman PHP, basis data SQL, serta algoritma RSA dengan bantuan *library* OpenSSL untuk menerapkan algoritma asimetris. Sistem ini memiliki beberapa fitur utama yang didefinisikan menggunakan diagram *use case* dan diagram aktivitas, yaitu membeli buku, membaca buku, menambahkan pengguna lain sebagai teman, dan memberi buku kepada pengguna lain. Adapun pengguna yang memiliki akses sebagai admin dapat menambahkan buku ke dalam basis data.

Hasil dari pengujian sistem menggunakan metode *black box* menunjukkan bahwa seluruh fitur sistem dapat berjalan dengan baik sesuai harapan. Pengujian proses enkripsi dan dekripsi *e-book* menggunakan algoritma asimetris RSA juga dilakukan, dengan hasil waktu yang cukup lama untuk pemrosesan *e-book* berukuran besar.

Dengan adanya sistem ini, diharapkan dapat menjadi wadah yang aman dalam ekosistem pendistribusian buku digital, sehingga upaya untuk melindungi hak cipta dapat terlaksana dengan baik.

Kata kunci: *e-book*, kriptografi, asimetris, RSA, kunci publik, kunci privat, hak cipta

GLOSARIUM

ASCII	Kode yang digunakan untuk mewakili teks dalam komputer.
Backend	Bagian belakang infrastruktur sistem yang tak terlihat oleh pengguna
Command-line	Perintah untuk berinteraksi pada komputer.
Framework	Kumpulan fungsi yang dipergunakan untuk mempermudah proses pengembangan perangkat lunak.
Frontend	Bagian depan sistem yang dapat dilihat oleh pengguna, seperti antarmuka.
Library	Kumpulan kode program untuk mengembangkan perangkat lunak.
Modal	Komponen situs web yang berupa kotak dialog atau jendela *popup*.
Navbar	Komponen situs web yang berisi menu navigasi.
Open Source	Perangkat lunak yang kode sumbernya dapat digunakan oleh siapa saja.

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB I
PENDAHULUAN

1.1 Latar Belakang

Di era modern ini, kemajuan teknologi sudah berkembang dengan pesat. Hampir segala aktivitas sehari-hari sudah dapat dilakukan melalui bantuan teknologi, mulai dari berkomunikasi dengan orang lain hingga melakukan aktivitas jual beli secara daring. Selain mempermudah berinteraksi sosial dan kegiatan ekonomi, teknologi juga mampu memberikan akses terhadap berbagai media hiburan. Berbagai macam karya tulis, lagu, gim, dan film kini dapat diakses dengan mudah dengan bantuan teknologi.

Salah satu aktivitas yang dapat dilakukan dengan teknologi adalah membaca buku digital atau yang biasa disebut dengan *e-book*. *E-book* merupakan suatu buku dalam media digital yang dapat dengan mudah diakses melalui internet. *E-book* dapat lebih mudah disebarluaskan dibandingkan dengan buku cetak. Sama seperti media lainnya, *e-book* memiliki hak cipta. Penulis memiliki hak eksklusif dalam menyebarluaskan karyanya. Namun, nyatanya saat ini banyak *e-boo*k yang disebarluaskan oleh pihak yang tidak bertanggungjawab tanpa seizin penulis. Tentu saja tindakan seperti ini merupakan tindakan pelanggaran hak cipta (Tiawati, Pura, 2021). Pembajakan *e-book* merupakan masalah serius dalam industri penerbitan buku. 17% dari *e-book* yang dibaca di Inggris merupakan *e-book* bajakan. Rata-rata, pembaca *e-boo*k di Belanda memiliki 117 *e-boo*k, tetapi hanya 11 *e-boo*k yang dibeli melalui situs legal. 92% dari pembaca *e-boo*k di Rusia mendapatkan akses *e-boo*k melalui situs ilegal (Kozlowski, 2018). Untuk menghindari pembajakan, dibutuhkan suatu sistem keamanan agar kegiatan distribusi *e-boo*k dapat berjalan dengan aman. Salah satu teknologi yang dapat digunakan untuk mendukung sistem tersebut adalah kriptografi.

Dalam penelitian yang berjudul "Sistem Distribusi *E-book* Berbasis Kriptografi Asimetris Menggunakan Algoritma RSA Untuk Perlindungan Hak Cipta" ini, penulis akan mengembangkan sebuah sistem berbasis web yang mendukung distribusi *e-book* dengan menerapkan kriptografi asimetris menggunakan algoritma RSA (*Rivest–Shamir–Adleman*). Penggunaan kriptografi asimetris dapat dikatakan lebih aman, dikarenakan menggunakan dua kunci yang berbeda dan ukuran kunci yang digunakan relatif lebih panjang (Zulfikar et al., 2019). Sistem ini akan dikembangkan dengan aplikasi *text editor* Microsoft Visual Studio

Code menggunakan bahasa pemrograman HTML, CSS dengan *framework* Bootstrap, PHP, basis data SQL, dan memanfaatkan *library* OpenSSL untuk implementasi algoritma RSA.

Dengan dikembangkannya sistem ini, diharapkan ekosistem pendistribusian buku digital dapat berjalan dengan aman sehingga hak-hak yang dimiliki oleh penulis dan penerbit dapat terjaga dengan baik.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah di atas, rumusan masalah yang diajukan adalah:

a. Bagaimana mengembangkan sistem distribusi *e-book* dengan menerapkan kriptografi asimetris guna meningkatkan keamanan terhadap tindakan pembajakan?
b. Bagaimana cara untuk memastikan sistem bahwa proses penyimpanan dan pendistribusian *e-book* hanya dapat dilakukan oleh pengguna yang memiliki akses?
c. Bagaimana cara untuk memastikan bahwa penerapan algoritma asimetris merupakan pilihan yang efektif dan efisien dalam proses perlindungan *e-book* terhadap pembajakan?

1.3 Batasan Masalah

Untuk menentukan ruang lingkup penelitian, batasan yang diterapkan adalah:

a. Fokus penelitian terbatas hanya pada implementasi kriptografi sebagai upaya pengamanan sistem.
b. Jenis kriptografi yang digunakan terbatas hanya menggunakan kriptografi asimetris.
c. Sistem yang dikembangkan berbasis *website*.

1.4 Tujuan Penelitian

Tujuan yang ingin dicapai dalam penelitian ini adalah mengembangkan sebuah sistem berbasis web yang mendukung distribusi *e-book* dengan menerapkan kriptografi asimetris melalui algoritma RSA (Rivest–Shamir–Adleman) untuk pengamanan terhadap pembajakan, sehingga hak cipta tetap terlindungi.

1.5 Manfaat Penelitian

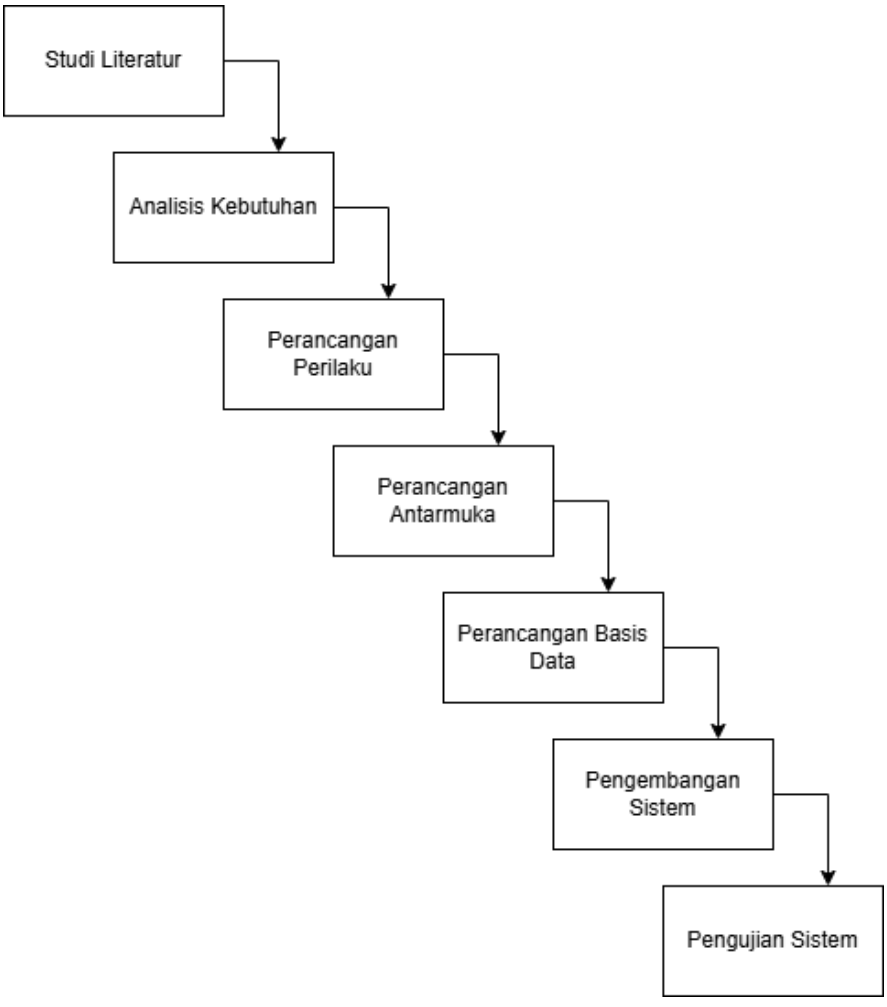
Dengan adanya penelitian ini, penulis berharap dapat memberikan manfaat sebagai berikut:

a. Mempermudah pengguna dalam mengakses *e-book* dengan aman

b. Meningkatkan kesadaran akan pentingnya perlindungan hak cipta dalam ekosistem digital
c. Menambah literatur dan referensi dalam bidang keamanan sistem informasi, dan
d. Menjadi acuan yang dapat dimanfaatkan oleh peneliti lain sebagai referensi penelitian selanjutnya.

1.6 Metode Penelitian

Untuk mengembangkan sebuah sistem distribusi *e-book* yang efektif dan efisien, penelitian ini dibagi dengan beberapa tahap dengan menggunakan metode air terjun atau *waterfall*. Metode *waterfall* merupakan suatu metode dalam pengembangan sistem dimana satu tahap dengan tahap yang lainnya dilakukan secara berurutan. Pada metode ini, tahap pertama akan diselesaikan terlebih dahulu sebelum masuk ke tahap berikutnya (Fachri, Surbakti, 2021). Adapun tahap-tahap tersebut adalah sebagai berikut:



Gambar 1.6 Diagram *waterfall* tahap pengembangan sistem.

a. Studi Literatur

Pada tahap studi literatur, penulis melaksanakan proses pengumpulan dan analisis berbagai sumber literatur yang relevan terhadap penelitian yang sedang dilakukan.

b. Analisis Kebutuhan

Pada tahap analisis kebutuhan, penulis melakukan pembuatan diagram UML (*Unified Modelling Language*) yang berupa perancangan perilaku dan diagram *use case*. Dalam dunia industri, UML merupakan standar bahasa yang digunakan untuk menentukan kebutuhan, membuat analisis dan desain, serta menggambarkan arsitektur dalam pemrograman berorientasi objek (Sari, Istikoma, 2018).

c. Perancangan Perilaku

Pada tahap perancangan perilaku, penulis melakukan proses perancangan diagram aktivitas dari setiap *use case* yang terdapat pada diagram UML untuk memberikan representasi visual yang jelas mengenai interaksi antara aktor dan sistem.

d. Perancangan Antarmuka

Pada tahap perancangan antarmuka, penulis melakukan proses pengembangan rancangan antarmuka yang akan diimplementasikan pada sistem. Proses ini bertujuan untuk memastikan bahwa kebutuhan fungsional dan estetika sistem dapat terpenuhi. Rancangan antarmuka dirancang menggunakan aplikasi perancangan antarmuka, seperti Figma.

e. Perancangan Basis Data

Pada tahap perancangan basis data, penulis membuat skema basis data menggunakan diagram relasi antar tabel untuk mendefinisikan tabel yang akan diimplementasikan pada basis data, hubungan antara tabel, dan mendefinisikan kolom-kolom yang diperlukan dalam setiap tabel.

f. Pengembangan Sistem

Pada tahap pengembangan sistem, penulis melaksanakan proses pembuatan kode program. Tahap pengembangan diawali dengan pembuatan tampilan *frontend* hingga pengerjaan *backend*, seperti pengaplikasian basis data.

g. Pengujian

Tahap pengujian dilakukan untuk menguji setiap laman pada sistem dan memastikan bahwa semua fitur dapat berjalan dengan baik. Sistem melewati proses pengujian

menggunakan metode *black box testing*. Tahap pengujian juga dilakukan untuk menghitung kecepatan algoritma asimetris yang diimplementasikan pada sistem.

1.7 Sistematika Kepenulisan

Pada laporan tugas akhir ini, terdapat sistematika kepenulisan dengan membagi laporan menjadi lima bab yang saling berhubungan guna memberikan gambaran penelitian yang jelas, yaitu:

a. Bab I: Pendahuluan

   Bab ini berisi tentang latar belakang, rumusan masalah, batasan masalah, tujuan, manfaat, metode penelitian, dan sistematika kepenulisan dari pengembangan sistem.

b. Bab II: Tinjauan Pustaka

   Bab ini berisi teori-teori dasar dan penelitian-penelitian terdahulu yang berkaitan dengan pengembangan sistem.

c. Bab III: Metode Penelitian

   Bab ini mendefinisikan kebutuhan melalui diagram *use case*, perancangan perilaku melalui diagram aktivitas, perancangan antarmuka, perancangan basis data, dan cara kerja kriptografi melalui diagram alir dalam sistem yang dikembangkan.

d. Bab IV: Hasil dan Pembahasan

   Bab ini menyajikan hasil dari pengembangan sistem yang dilakukan berupa tampilan antarmuka dan cara kerja sistem, serta pemaparan hasil dari pengujian sistem.

e. Bab V: Kesimpulan dan Saran

   Bab ini berisi kesimpulan dari hasil pengembangan sistem, serta saran yang diberikan untuk penelitian selanjutnya.

BAB II
TINJAUAN PUSTAKA

2.1 Landasan Teori

2.1.1 *E-book*

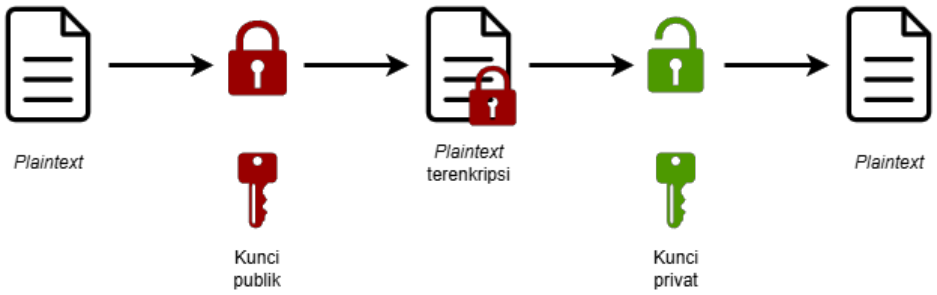
E-book (*electronic book*) atau yang bisa disebut juga sebagai buku digital adalah jenis buku yang diterbitkan dalam format digital, yang dapat diakses melalui *smartphone*, laptop, tablet, dan perangkat elektronik lainnya. Di era modern, popularitas buku digital semakin meningkat karena memiliki beberapa keunggulan dibandingkan dengan buku fisik. Salah satu keunggulan tersebut adalah portabilitas, di mana buku digital dapat dengan mudah dibawa ke mana saja dikarenakan tidak memerlukan ruang penyimpanan yang besar. Selain itu, beberapa format buku digital juga memiliki fitur pencarian kata sehingga memudahkan pembaca. Terakhir, buku digital memiliki dampak ramah lingkungan karena tidak memerlukan penggunaan kertas (Ruddamayanti, 2019).

2.1.2 Kriptografi

Kriptografi (*cryptography*) berasal dari bahasa Yunani yang terdiri dari dua suku kata, *kripto* dan *graphia*. *Kripto* memiliki arti menyembunyikan, sedangkan *graphia* memiliki arti tulisan (Amin, 2016). Kriptografi merupakan sebuah ilmu yang mempelajari teknik matematika yang berkaitan dengan aspek keamanan informasi, yang mencakup menjaga kerahasiaan, memverifikasi keaslian, integritas, dan autentikasi data (Nova et al., 2021). Kriptografi memiliki algoritma yang berisi aturan dan fungsi matematika untuk enkripsi (*enciphering*) dan dekripsi (*deciphering*) (Basri, 2016). Enkripsi (*encryption)*, atau *enciphering*, adalah sebuah proses yang bertujuan mengubah pesan yang dapat terbaca (*plaintext*) menjadi tidak terbaca atau sulit terbaca (*ciphertext*). Proses untuk mengembalikan *ciphertext* menjadi *plaintext* disebut dekripsi (*decryption*), atau *deciphering* (Simargolang, 2017). Berdasarkan jenis kuncinya, kriptografi terbagi menjadi dua, yaitu kriptografi simetris dan kriptografi asimetris. Kriptografi simetris adalah jenis kriptografi yang menggunakan kunci kriptografi yang sama dalam proses enkripsi dan dekripsi. Sedangkan untuk kriptografi asimetris, kunci yang digunakan untuk proses enkripsi dan dekripsi berbeda (Putri et al., 2018).

2.1.3 Kriptografi Asimetris

Kriptografi asimetris merupakan jenis kriptografi yang menggunakan sepasang kunci, yaitu kunci publik dan kunci privat. Kunci publik digunakan untuk mengenkripsi data, sedangkan kunci privat digunakan untuk mendekripsi data yang sebelumnya telah dienkripsi dengan kunci publik. Meskipun metode ini aman, proses enkripsi dan dekripsi dalam kriptografi asimetris cenderung lebih lambat dibandingkan dengan kriptografi simetris. Oleh karena itu, umumnya data akan dienkripsi terlebih dahulu menggunakan algoritma simetris, dan hasil enkripsi tersebut akan dienkripsi kembali dengan algoritma asimetris. Pendekatan ini memungkinkan pemanfaatan kecepatan algoritma simetris dan keamanan algoritma asimetris secara bersamaan. Salah satu algoritma yang menerapkan prinsip kriptografi asimetris adalah RSA (Rivest–Shamir–Adleman) (Basri, 2016).



Gambar 2.1.3 Ilustrasi proses enkripsi dan dekripsi pada algoritma asimetris.

2.1.4 RSA (Rivest–Shamir–Adleman)

Algoritma RSA (*Rivest–Shamir–Adleman*) merupakan salah satu dari sekian banyak algoritma kriptografi asimetris yang sering digunakan. Algoritma RSA ditemukan pada tahun 1976 oleh tiga peneliti dari MIT (*Massachusetts Institute of Technology*), yaitu Rivest, Shamir, dan Adleman. Cara kerja algoritma RSA adalah dengan memfaktorkan bilangan besar menjadi faktor-faktor prima. Proses pemfaktoran ini digunakan untuk menemukan kunci privat. (Rizki, Ariyani, 2021). Terdapat banyak *library* yang mendukung penerapan algoritma RSA, seperti OpenSSL dan phpseclib.

Proses Pembangkitan Kunci Pada Algoritma RSA

Untuk memulai proses pembangkitan kunci pada algoritma RSA, diperlukan langkah-langkah berikut (Dairi et al., 2023):

a. Memilih nilai p dan q, dua buah bilangan prima. Nilai p dan q bersifat rahasia.
b. Menghitung nilai n = p × q. Nilai n tidak perlu dirahasiakan.
c. Menghitung nilai m = (p - 1) (q - 1)
d. Memilih sebuah bilangan bulat untuk kunci publik (e), yang relatif prima terhadap m.
e. Menghitung kunci untuk dekripsi (d) menggunakan rumus e.d mod m = 1

Dari proses algoritma diatas, diperoleh:

f. Kunci publik adalah pasangan (e, n)
g. Kunci privat adalah pasangan (d, n).

Contoh Proses Penerapan Algoritma RSA

Langkah pertama, bangkitkan kunci publik dan kunci privat melalui proses berikut.

a. Memilih nilai bilangan prima p dan q, misalnya p = 3 dan q = 641
b. Menghitung nilai n = p × q, yaitu n = 3 × 641 = 1923
c. Menghitung nilai m = (p - 1) (q - 1), yaitu m = (3 - 1) (641 - 1) = 1280
d. Memilih nilai e yang relatif prima terhadap m, misalnya e = 427
e. Menghitung d dengan rumus e × d mod m = 1, sehingga d × 427 mod 1280 = 3. Nilai d yang didapat adalah 8.
f. Nilai kunci yang diperoleh adalah kunci publik: (427, 1923) dan kunci privat: (3, 1923).

Untuk melakukan proses enkripsi pada algoritma RSA, diperlukan langkah-langkah berikut.

a. Menyiapkan kunci publik (e, n), yaitu (427, 1923)
b. Menyiapkan *plaintext* (M), misalkan M = 10000000, kemudian konversi ke ASCII menjadi: 49 48 48 48 48 48 48 48.
c. Pecah M menjadi blok, yang akan menjadi:
   M1 = 494
   M2 = 848
   M3 = 484
   M4 = 848
   M5 = 484
   M6 = 800
d. Dengan menggunakan kunci publik (e, n) = (427, 1923), enkripsi blok-blok M menjadi:
   C1 = 494427 mod 1923 = 533
   C2 = 848427 mod 1923 = 209

C3 = 484427 mod 1923 = 874

C4 = 848427 mod 1923 = 209

C5 = 484427 mod 1923 = 874

C6 = 800427 mod 1923 = 1202

e. Menghasilkan nilai *ciphertext* (C) = 533 209 874 209 874 1202.

Langkah-langkah proses dekripsi sama seperti proses enkripsi, yang membedakan adalah pada proses dekripsi menggunakan kunci privat (d, n). Langkah-langkah proses dekripsi adalah sebagai berikut.

a. Menyiapkan kunci privat (d, n) yaitu (3, 1923)
b. Menyiapkan *ciphertext* (C) untuk proses dekripsi, yaitu 533 209 874 209 874 1202.
c. Pecah C menjadi blok, yang akan menjadi:

C1 = 5333 mod 1923 = 494

C2 = 2093 mod 1923 = 848

C3 = 8743 mod 1923 = 484

C4 = 2093 mod 1923 = 848

C5 = 8743 mod 1923 = 484

C6 = 12023 mod 1923 = 800

d. Menggabungkan C1 hingga C6 sehingga menjadi nilai *plaintext* semula, yaitu 10000000.

2.1.5 Hak Cipta

Hak cipta merupakan hak eksklusif yang memungkinkan pemegangnya untuk mengatur, menerbitkan, atau memperbanyak suatu karya yang merupakan gagasan, hasil ciptaan, atau informasi tertentu, serta memberikan izin penggunaan karya tersebut, dengan mematuhi batasan yang telah diatur dalam peraturan perundang-undangan yang berlaku. Hak cipta dapat mencakup ilmu pengetahuan, karya seni dan sastra, yang juga mencakup program komputer (Guswandi et al., 2021).

2.1.6 *Website*

Website atau situs web merupakan kumpulan halaman yang dapat menampilkan data berupa format teks, gambar, animasi, suara, video, atau kombinasi dari seluruh format tersebut. Situs web dapat berupa halaman yang bersifat statis atau dinamis, yang terhubung melalui *hyperlink* atau jaringan-jaringan halaman (Maharani et al., 2021).

Website merupakan wadah pertukaran dan penyebaran informasi yang efisien, dikarenakan penyebarannya yang cepat, mudah, dan jangkauan yang luas. *Website* dapat dengan mudah diakses menggunakan berbagai perangkat keras, seperti *smartphone*, laptop, tablet, dan komputer. Maka dari itu, media *internet* melalui *website* menjadi suatu hal yang penting dalam kehidupan bermasyarakat saat ini (Putra et al., 2022).

Selain itu, *website* menjadi salah satu elemen yang penting untuk membangun keberadaan daring, yang merupakan kunci utama agar sukses dalam bisnis. Akibatnya, kebutuhan untuk mengembangkan situs web yang menarik semakin besar agar dapat berkompetisi dengan pelaku bisnis digital lain (Sasvito, 2024).

2.1.7 PHP (*Hypertext Preprocessor*)

PHP, atau *Hypertext Preprocessor*, merupakan bahasa pemrograman yang digunakan untuk mengembangkan situs web dinamis. PHP memungkinkan situs web berinteraksi dengan basis data, seperti pengolahan data dan pemrosesan data. PHP merupakan bahasa pelengkap HTML, Artinya, perintah dalam PHP menyatu dengan tag-tag HTML. Semua perintah dalam PHP yang diberikan akan dijalankan di *server*, sedangkan *browser* hanya menerima dan menampilkan hasil akhirnya (Hermiati et al., 2021).

2.1.8 SQL (*Structured Query Language*)

SQL, atau *Structured Query Language*, adalah bahasa yang digunakan untuk mengelola basis data relasional. SQL memungkinkan pengguna untuk menambah, menghapus, mengambil, dan memperbarui data dalam basis data. Perintah SQL dapat dijalankan melalui bahasa pemrograman konvensional, seperti PHP, menggunakan fungsi-fungsi yang disediakan dalam bahasa tersebut (Kharisma, Nasution, 2023).

2.1.9 OpenSSL

OpenSSL merupakan proyek *open source* yang terdiri atas library algoritma kriptografi dan *toolkit* SSL. OpenSSL merupakan pilihan *library* yang dapat dimanfaatkan oleh pengembang *software* untuk mengimplementasikan algoritma kriptografi yang kuat ke dalam program mereka. Selain itu, OpenSSL juga merupakan sebuah alat yang menyediakan akses ke beragam fungsionalitasnya yang dapat diakses menggunakan *command-line tools*. *Command-line tools* yang terdapat pada OpenSSL dapat memberikan kemudahan dalam mengerjakan berbagai perintah umum, seperti mengelola kunci sertifikat. Selain itu,

command-line tools pada OpenSSL juga memiliki kemampuan untuk mengakses lebih banyak fungsi yang bersifat *higher-level*. OpenSSL memiliki dokumentasi yang berisi informasi tentang berbagai perintah dan opsi yang dapat dijalankan pada *command-line tools*. OpenSSL mendukung pembangkitan kunci RSA, DSA, dan ECDSA, dan dapat digunakan menggunakan berbagai bahasa pemrograman, termasuk C, Java, PHP, Perl, dan Python. (Viega, et al., 2002).

Pemilihan Ukuran Kunci dalam OpenSSL

Penerapan algoritma kriptografi sangat dipengaruhi oleh ukuran kunci yang digunakan. Menggunakan ukuran kunci yang terlalu kecil tidaklah aman, dan menggunakan ukuran kunci yang terlalu besar akan mengakibatkan keamanan yang "terlalu tinggi" dan menyebabkan proses operasi menjadi lambat. Sebagai contoh, penggunaan ukuran kunci *default* RSA, yaitu 512 bit, tidaklah aman. Jika pada *server* digunakan kunci RSA berukuran 512 bit pada saat ini, penyerang dapat dengan mudah mengambil kunci sertifikasi dan melakukan serangan *brute-force* untuk mencuri kunci privat. Pada saat ini, ukuran kunci RSA yang dapat dikatakan aman adalah setidaknya 2048 bit. Untuk situs *web* pada umumnya, penggunaan ukuran kunci yang lebih tinggi dari 2048 bit dapat menyebabkan pemborosan kinerja CPU dan mengakibatkan terganggunya *user experience* (Ristic, 2013).

2.2 Kajian Pustaka

Untuk mengembangkan sebuah sistem distribusi *e-book* berbasis kriptografi asimetris menggunakan algoritma RSA, penulis melakukan pengumpulan hasil dari penelitian sebelumnya dari berbagai sumber, yang akan digunakan sebagai referensi. Berbagai hasil penelitian ini dibagi menjadi beberapa bagian sesuai dengan topik yang diangkat.

2.2.1 Sistem Pembaca Karya Tulis Digital

Pada saat ini, banyak penulis yang berupaya untuk memperkenalkan karya mereka dengan lebih luas. Karya-karya tersebut dapat berupa majalah, artikel, *e-book*, dan lain sebagainya. Untuk mendukung kebutuhan itu, penulis dapat memanfaatkan platform digital berupa aplikasi pembaca daring. Penelitian yang dilakukan oleh Purnama dan Permana (2021) berfokus pada pembangunan sistem pembaca majalah daring, yang mampu mempermudah pengguna untuk mengunggah majalah, *e-book,* dan sebagainya, secara gratis. Sistem ini dikembangkan menggunakan bahasa pemrograman PHP dan basis data MySQL.

Dalam sistem ini, pengguna dapat melakukan pendaftaran akun, pencarian berdasarkan kategori, pengunggahan, dan membaca berbagai karya tulis digital yang tersedia.

2.2.2 Sistem Penjualan Buku

Penelitian yang dilakukan oleh Aldisa dan Abdullah (2022) membahas tentang perancangan sebuah sistem informasi berbasis web yang dapat melakukan penjualan buku dengan fitur kategori dan pencarian. Sistem ini bertujuan untuk membantu pemilik toko buku agar proses penjualan dan pemasaran buku dapat berjalan dengan lancar. Pengembangan sistem ini menggunakan metode *Agile*, yaitu metode yang dilakukan secara bertahap, yang dimana sistem akan selalu diperbarui menyesuaikan kondisi setelah sistem dijalankan. Tahapan dalam metode ini mencakup perencanaan, rancangan, tes perangkat lunak, dokumentasi, dan *deployment*. Perancangan sistem ini juga dimodelkan menggunakan diagram *use case*, yaitu sebuah diagram untuk menggambarkan interaksi antara sistem dan aktor. Fitur utama dalam sistem ini adalah melakukan input data buku, keranjang belanja, pembayaran dan proses pengiriman, dan menampilkan laporan bulanan.

Pada penelitian yang dilakukan oleh Pertama et al. (2023) juga membahas tentang penjualan buku bekas berbasis *mobile* guna membantu proses jual beli buku pada Pertokoan Ramayana Pasar Bawah. Proses jual beli pada Pertokoan Ramayana Pasar Bawah masih dilakukan secara konvensional melalui tatap muka dan pemasarannya masih dilakukan dengan penyebaran brosur dan spanduk, sehingga menjadi kurang efektif. Penelitian ini bertujuan untuk memberikan kemudahan dalam berjualan secara daring untuk para penjual maupun pembeli. Aplikasi yang dikembangkan dalam penelitian ini menggunakan bahasa pemrograman PHP untuk pihak admin, dan Java untuk pihak *customer*. Pengembangan aplikasi pada penelitian ini menggunakan metode *waterfall*, dengan tahapan mendefinisikan kebutuhan, desain sistem, implementasi, *testing*, dan *maintenance*. Pada tahap mendefinisikan kebutuhan, peneliti melakukan wawancara secara langsung ke para pemilik toko buku dan observasi proses penjualan di Pertokoan Ramayana Pasar Bawah, kemudian melakukan studi literatur dengan membaca penelitian-penelitian terdahulu yang relevan. Pada tahap desain sistem, peneliti mendefinisikan sistem menggunakan diagram UML, yaitu diagram *use case*, diagram aktivitas, dan diagram kelas. Aktivitas utama yang dapat dilakukan dalam aplikasi adalah menambah data barang, keranjang, dan mengelola laporan penjualan. Pada tahap *testing*, pengujian dilakukan menggunakan metode ISO25010 menggunakan karakteristik pengujian *functional suitability* dan *usability*. Berdasarkan

perhitungan dalam pengujian, dapat disimpulkan bahwa sistem mendapat nilai persentasi 100% dalam *functional suitability* dan nilai persentasi 94,4 % dalam *usability*. Dari hasil di atas, dapat disimpulkan bahwa sistem dapat mudah digunakan dan dimanfaatkan bagi pihak toko maupun pelanggan.

2.2.3 Pembajakan *E-book*

Pada penelitian yang dilakukan oleh Uyun dan Mustofa (2023) menjelaskan tentang maraknya tindakan pembajakan menggunakan teknologi digital. Penelitian ini menggunakan metode analisis berdasarkan fakta empiris yang terjadi di masyarakat. Dengan berkembangnya teknologi digital, tindakan pembajakan menjadi semakin mudah dilakukan. Pembajakan yang sering dijumpai saat ini adalah pembajakan komersial, yaitu tindakan pembajakan yang bertujuan untuk memperoleh keuntungan pribadi. Tindakan ini sangat merugikan pemilik asli hak cipta. Dalan konteks buku digital atau *e-book*, hak cipta dipegang oleh penulis dan penerbit. Pembajakan *e-book* sangat merugikan penulis dan penerbit dikarenakan keuntungan dari penjualan *e-book* tidak akan diperoleh akibat orang lain yang menduplikasi *e-book* tersebut, sehingga keuntungan akan diterima oleh pembajak alih-alih pemilik hak cipta.

Di Indonesia, tindakan pembajakan buku sudah dianggap lumrah. Hal ini disebabkan oleh banyak faktor, salah satunya adalah mahalnya harga buku *original* saat ini, sehingga orang-orang akan memilih jalan yang lebih mudah untuk mendapatkan buku dengan harga murah. Dengan banyaknya pembajak buku dan penikmat buku hasil bajakan, akan memunculkan fenomena normalisasi pembajakan.

2.2.4 Penerapan Algoritma RSA

Untuk membuktikan keamanan algoritma RSA, perlu dilakukan pengujian pada media sebagai data yang akan diamankan. Pengamanan data dapat diaplikasikan pada berbagai format multimedia yang ada dalam komputer, termasuk format teks, gambar, audio, dan video. Dalam penelitian yang dilakukan oleh Diarse dan Bendi (2016), fokus diberikan pada keamanan algoritma RSA menggunakan media berformat MP3. Tujuan dari penelitian ini adalah untuk secara khusus membuktikan keamanan algoritma RSA dengan menerapkan enkripsi pada file audio MP3 menggunakan metode pemodelan sistem, yang mencakup penyusunan diagram alur untuk proses pembentukan kunci, proses enkripsi, dan proses dekripsi. Metode pemodelan sistem menggunakan *Unified Modelling Language* (UML) untuk

memberikan representasi visual yang jelas. Manfaat dari studi ini adalah untuk memberikan bukti yang kuat terkait keamanan penggunaan algoritma RSA pada data multimedia, khususnya pada *file* audio MP3. Subjek yang terlibat dalam studi mencakup pengirim (*sender*) yang bertanggung jawab atas proses enkripsi data dan penerima (*receiver*) yang menerima data terenkripsi. Analisis dilakukan melalui beberapa tahapan, termasuk pembentukan kunci, proses enkripsi, dan proses dekripsi. Pembentukan kunci melibatkan input bilangan p dan q, dan menghasilkan kunci publik, kunci privat, dan modulus. Enkripsi melibatkan input *file* audio MP3, menghasilkan *file* audio MP3 terenkripsi, dan menggunakan kunci publik. Dekripsi melibatkan input file audio MP3 terenkripsi, menghasilkan *file* audio MP3 asli, dan menggunakan kunci privat. Hasil dari penelitian menunjukkan bahwa algoritma RSA dapat diimplementasikan secara efektif untuk proses enkripsi dan dekripsi pada *file* audio MP3.

Pada penerapan algoritma RSA yang dilakukan oleh Zulfikar et al. (2019), penelitian bertujuan membangun sistem yang dapat meningkatkan keamanan pada data dan informasi dalam *email* sebelum dilakukan proses pengiriman. *Email* saat ini menjadi salah satu media utama dalam komunikasi jarak jauh. Namun, semakin sering muncul permasalahan keamanan dalam bentuk kasus *cyber* seperti *spoofing*, *spam*, dan penyebaran *malware*. Oleh karena itu, perlu diambil langkah antisipatif untuk meningkatkan keamanan data dan informasi pada *email* dengan menggunakan kriptografi. Pendekatan yang digunakan dalam studi ini adalah melakukan enkripsi pada *email* menggunakan metode kriptografi *Blowfish* dan mengenkripsi kunci simetris menggunakan kriptografi RSA. Manfaat dari studi adalah memperkuat pengamanan informasi dalam email. Subjek yang terlibat dalam studi mencakup pengirim email dan penerima email. Analisis dilakukan menggunakan bahasa pemrograman Java dengan IDE Netbeans 8.2. Diperlukan dua alamat *email*, satu sebagai pengirim dan satu sebagai penerima. Analisis dilakukan dalam dua tahapan, yaitu pada masing-masing algoritma enkripsi dan dekripsi secara paralel. Selanjutnya, dilakukan analisis keamanan pada ciphertext kunci simetris dengan melihat ketersediaan dan kemungkinan kunci yang dihasilkan dalam serangan *brute-force*. Dari hasil percobaan, data berukuran 4,68 KB berhasil terenkripsi dengan perubahan ukuran sekitar 0,09 KB yang tidak signifikan dalam mempengaruhi waktu proses pengiriman *email*. Hasil dari serangan *brute-force* menunjukkan bahwa algoritma kriptografi yang digunakan terbilang aman, dan panjang karakter kunci memengaruhi tingkat kesulitan untuk memecahkan *plaintext* dengan serangan *brute-force*.

Pada penelitian yang dilakukan oleh Dairi et al. (2023) yang membahas tentang penerapan sistem informasi perpustakaan, juga menerapkan algoritma RSA. Perpustakaan menyimpan informasi atau data tentang buku yang dimilikinya, yang perlu dijaga dan disimpan dengan baik. Namun, banyak proses pelayanan yang masih dilakukan secara konvensional, di mana pendataan dilakukan manual dengan menuliskan informasi di dalam buku. Hal ini mengakibatkan lambatnya proses pencarian data, dan keamanan data tersebut sulit dijaga karena siapapun dapat melihat dan membacanya. Tujuan dari penelitian adalah membantu tenaga pengelola perpustakaan dalam mencari informasi atau referensi tentang data buku yang diperlukan, sekaligus menjaga kerahasiaan data perpustakaan agar tetap terlindungi. Metode yang digunakan dalam penelitian adalah menggunakan algoritma kriptografi RSA dalam sistem informasi perpustakaan. Subjek yang terlibat adalah pengelola perpustakaan. Analisis algoritma RSA terbagi menjadi tiga tahapan atau proses, yaitu pembangkitan kunci, tahap enkripsi, dan tahap dekripsi. Hasil dari penelitian menunjukkan bahwa penggunaan algoritma RSA dapat terbukti efektif dalam menjaga kerahasiaan data perpustakaan. Dengan menerapkan kriptografi RSA, informasi tentang buku dapat tetap aman dan hanya dapat diakses oleh pihak yang berwenang, meningkatkan keamanan data perpustakaan secara signifikan.

Pada penelitian yang dilakukan oleh Rizki dan Ariyani (2021), penerapan algoritma RSA digunakan untuk pengamanan data sebuah kantor guna melindungi data dari pencurian. Pencurian data merupakan salah satu dampak negatif dari kemajuan teknologi informasi. Untuk melindungi data dari pencurian, studi ini dilakukan dengan merancang sebuah sistem aplikasi yang menggunakan bahasa pemrograman Java dengan menerapkan algoritma RSA sebagai metode pengamanan data. Hasil dari penelitian menunjukkan bahwa proses enkripsi dan dekripsi menggunakan algoritma RSA dapat berjalan dengan baik. Namun, ukuran *file* yang digunakan mempengaruhi kecepatan penggunaan aplikasi. Semakin besar ukuran *file*, maka semakin banyak waktu yang diperlukan dalam proses enkripsi dan dekripsi.

2.2.5 Penggabungan Algoritma RSA dengan Algoritma Lain

Pada penelitian yang dilakukan oleh Saputra et al. (2023), diterapkan algoritma RSA Cipher. Penerapan algoritma ini disebut juga pendekatan *hybrid* atau penggabungan antara dua jenis algoritma berbeda, dalam kasus ini yaitu menggabungkan kriptografi simetris dengan kriptografi asimetris. Tujuan dari penelitian ini adalah melindungi pesan agar aman ketika dikirimkan ke penerima. Metode yang diterapkan dalam penelitian ini adalah

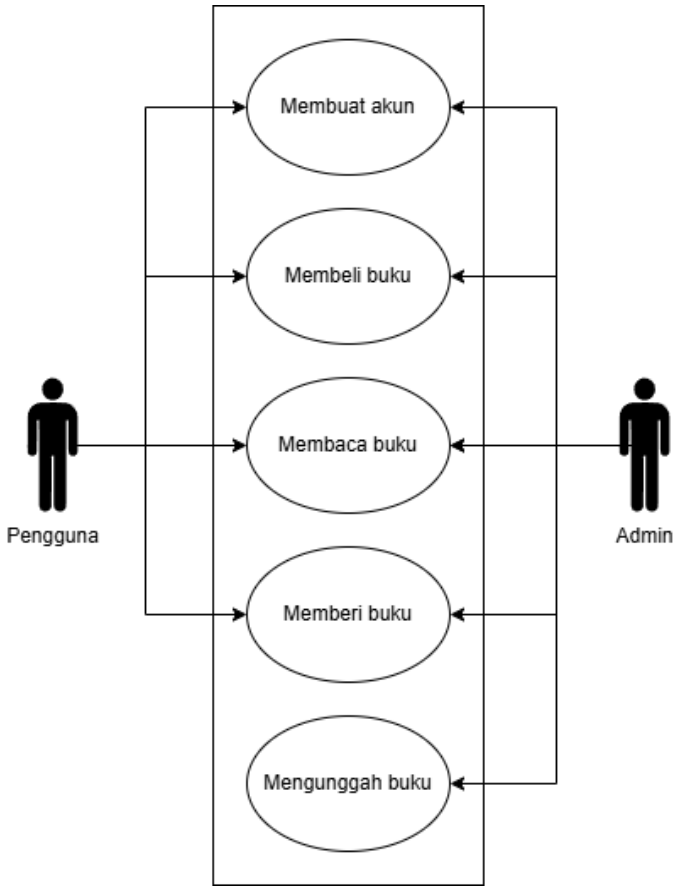
pengumpulan data dan informasi, perancangan program, dan implementasi program. Hasil dari pengujian program menunjukkan bahwa pesan dapat terenkripsi dengan baik menggunakan algoritma RSA Cipher. Hal ini menunjukkan bahwa pendekatan *hybrid* merupakan solusi yang efektif sebagai metode enkripsi.

Penerapan pendekatan *hybrid* juga terdapat pada penelitian yang dilakukan oleh (Surbakti, 2023). Penelitian ini menerapkan penggabungan antara algoritma asimetris RSA dengan algoritma *Blum Blum Shub* (BBS) untuk mengamankan *file* basis data *e-absensi* milik Badan Kepegawaian Daerah Kota Binjai. Penelitian ini dilatarbelakangi oleh diperlukannya pengamanan pada *file* basis data *e-absensi* dikarenakan terdapat banyak data pribadi pegawai yang tersimpan, seperti Nomor Induk Pegawai (NIP), data kehadiran dan kepulangan, izin, cuti, dan besaran potongan disiplin maupun tunjangan bulanan. Hasil dari penelitian ini berupa sebuah sistem yang dapat mengacak isi dari sebuah *file* teks, yang hanya dapat dipulihkan oleh pihak yang berwenang menggunakan kunci privat. Hal ini menunjukkan bahwa pendekatan *hybrid* menggunakan kombinasi algoritma RSA dan BBS dapat meningkatkan keamanan dalam proses penyandian pesan dengan baik.

BAB III
METODOLOGI PENELITIAN

3.1 Analisis Kebutuhan

Aktivitas utama pada pengembangan sistem didefinisikan menggunakan diagram *use case*. Diagram *use case* adalah sebuah pemodelan yang digunakan untuk menghubungkan antara satu atau lebih peran dengan sistem yang akan dirancang. Diagram *use case* juga mendefinisikan fitur-fitur apa saja yang akan diimplementasikan ke dalam sistem dan siapa saja aktor yang berhak menggunakannya (Hafsari et al., 2023). Dalam sistem ini, terdapat dua aktor, yaitu pengguna umum dan pengguna yang memiliki hak sebagai admin. Aktivitas utama dalam sistem yang dapat dilakukan aktor pengguna adalah membuat akun, membeli buku, membaca buku, memberi buku, dan mengunggah buku. Aktor admin memiliki aktivitas serupa dengan pengguna, ditambah dengan aktivitas mengunggah buku.

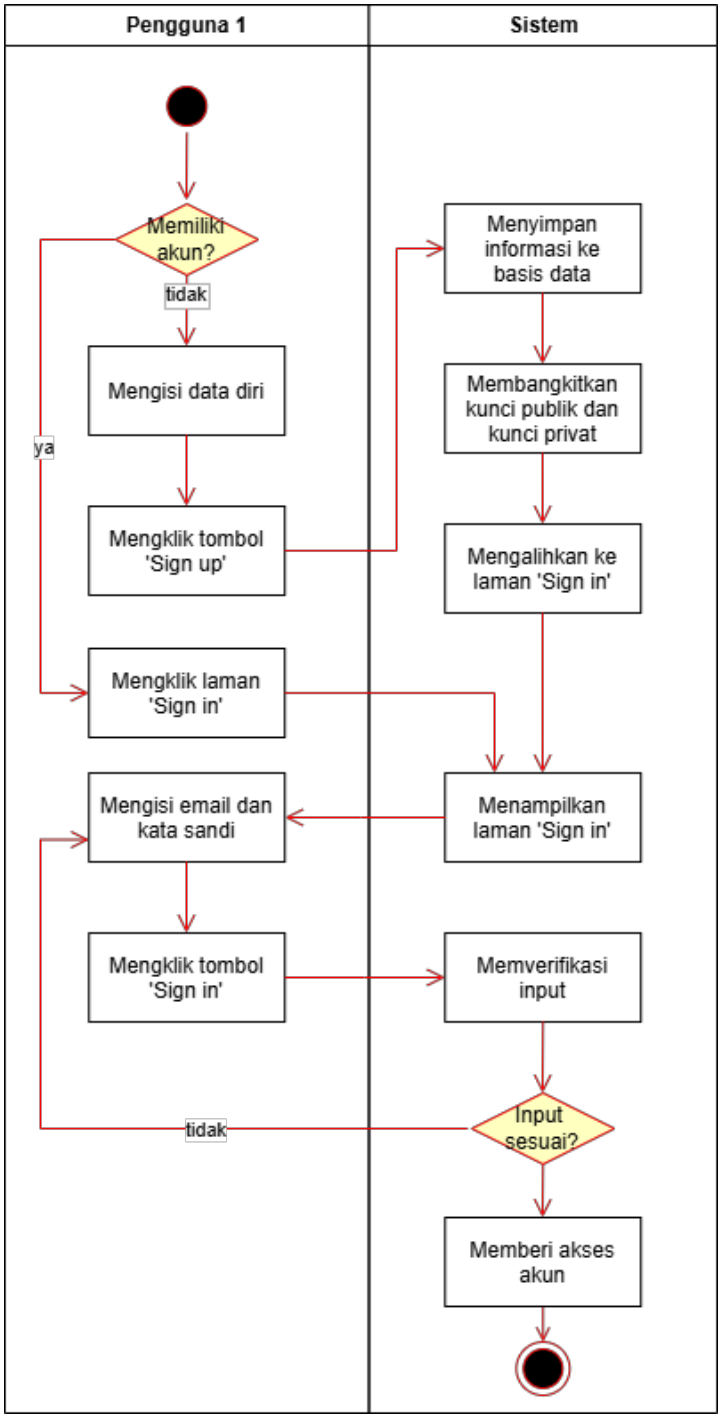


Gambar 3.1 Diagram *use case*.

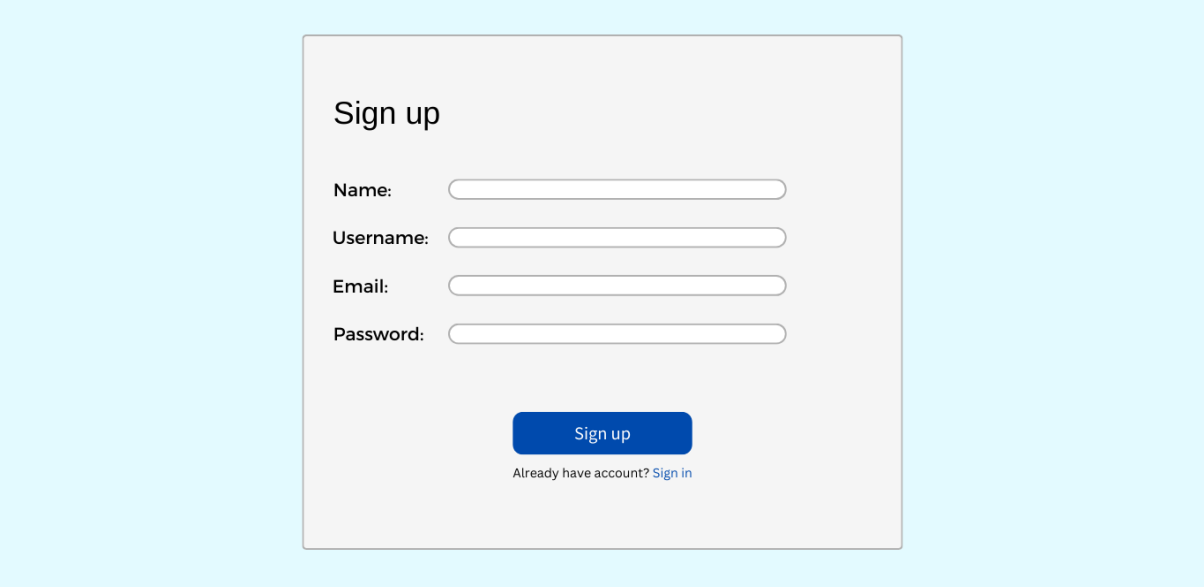
3.2 Perancangan Perilaku dan Antarmuka

3.2.1 Membuat Akun

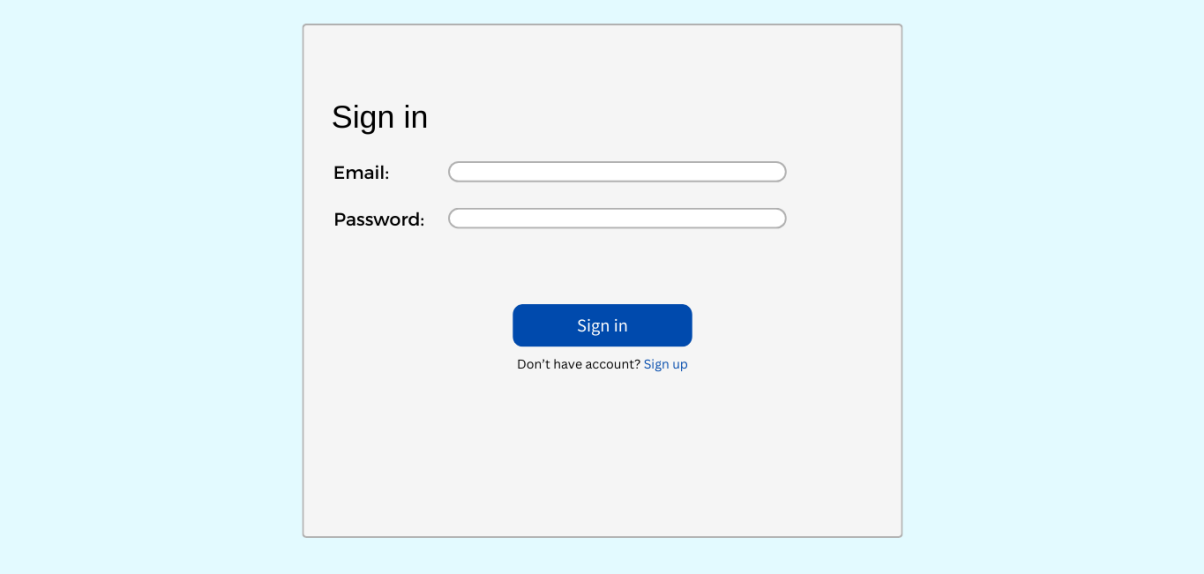
Membuat akun adalah langkah yang harus dilakukan pengguna sebelum dapat menikmati fitur-fitur utama yang ada di dalam sistem, seperti membeli, membaca, dan memberi buku. Pada laman ‘Sign in’, terdapat form untuk email dan kata sandi yang harus diisi oleh pengguna. Jika belum memiliki akun, pengguna dapat membuat akun melalui laman ‘Sign up’. Pengguna perlu mengisi form untuk nama lengkap, *username*, alamat *email*, kata sandi, dan konfirmasi kata sandi. Setelah mengklik tombol ‘Sign up’, sistem akan menyimpan informasi pengguna ke dalam basis data. Selanjutnya, pengguna akan dialihkan ke laman ‘Sign in’ untuk masuk dengan alamat email dan kata sandi yang telah didaftarkan sebelumnya.



Gambar 3.2.1 Diagram aktivitas membuat akun.



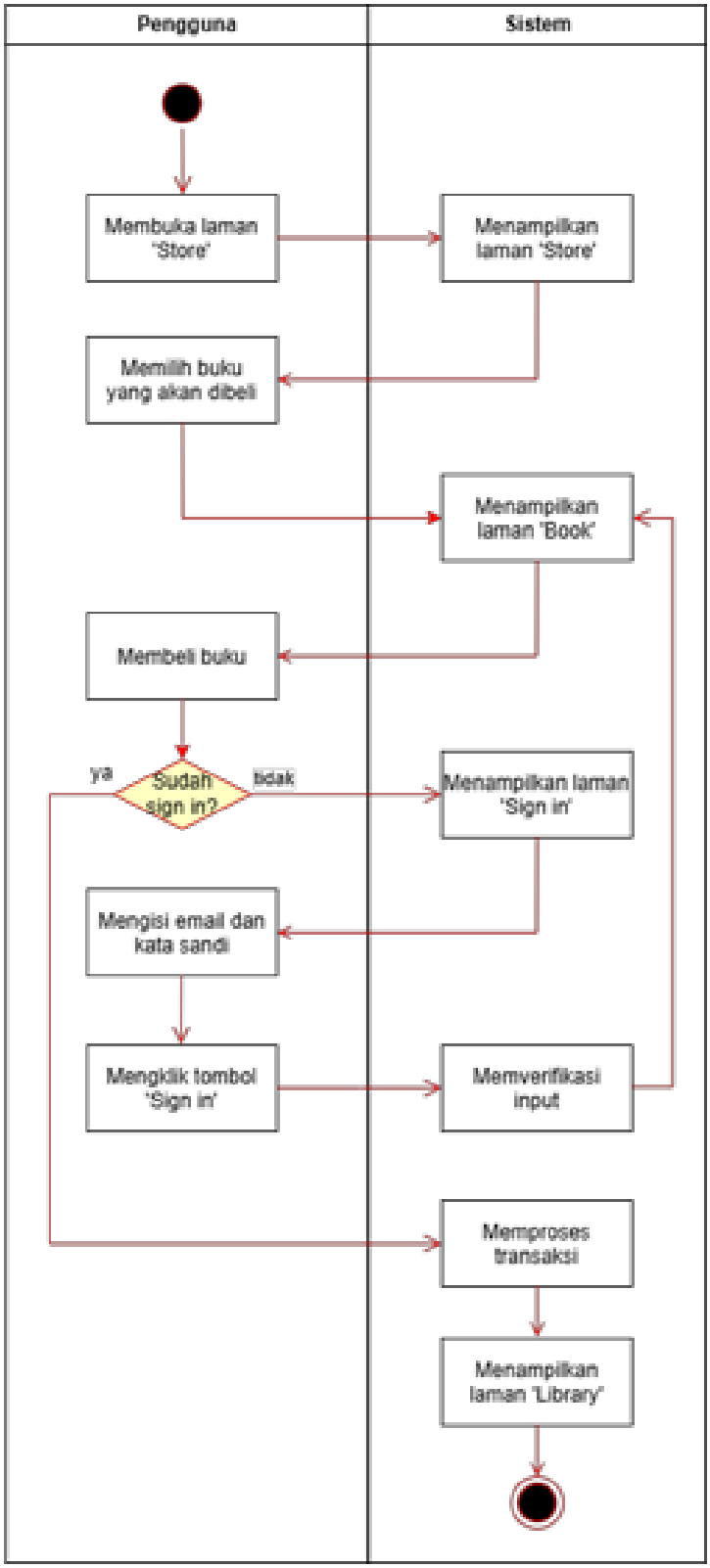
Gambar 3.2.1 Rancangan antarmuka laman ‘Sign up’.



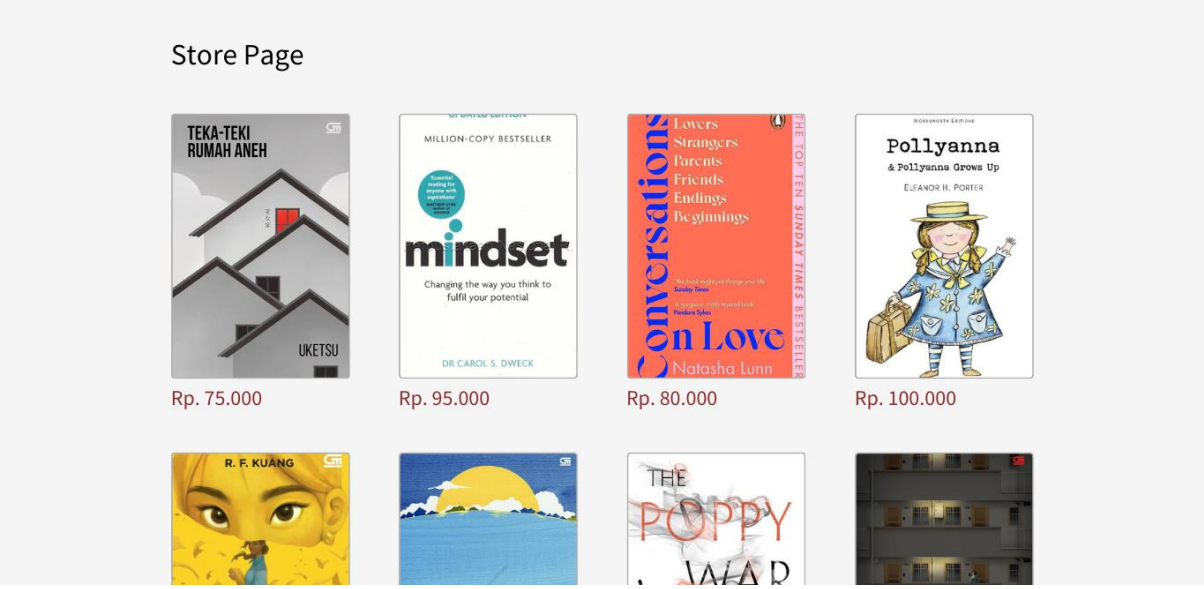
Gambar 3.2.1 Rancangan antarmuka laman ‘Sign in’.

3.2.2 Membeli Buku

Untuk membeli buku, pengguna dapat melihat daftar buku yang dijual melalui laman ‘Store’. Setelah memilih sebuah buku, pengguna akan diarahkan ke laman ‘Book’ yang menampilkan informasi lebih mendetail mengenai buku tersebut. Untuk melakukan pembelian, pengguna dapat mengklik tombol ‘Buy now’ yang terletak di bawah sampul buku. Setelah melakukan pembelian, buku yang telah dibeli akan ditampilkan pada laman ‘Library’.



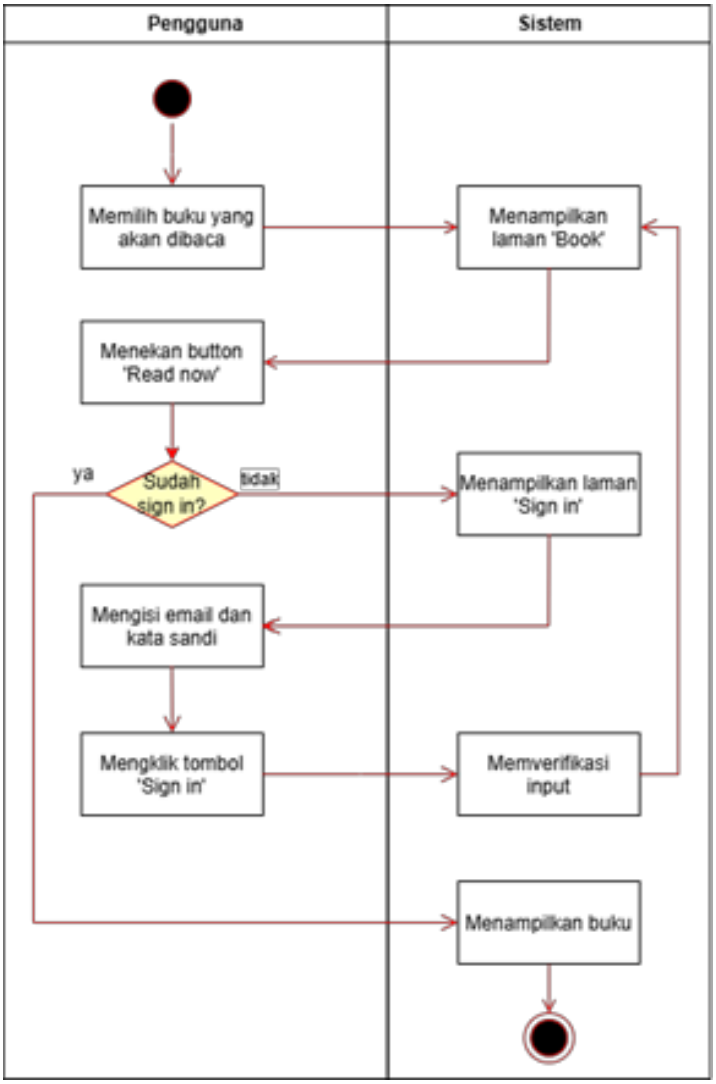
Gambar 3.2.2 Diagram aktivitas membeli buku.



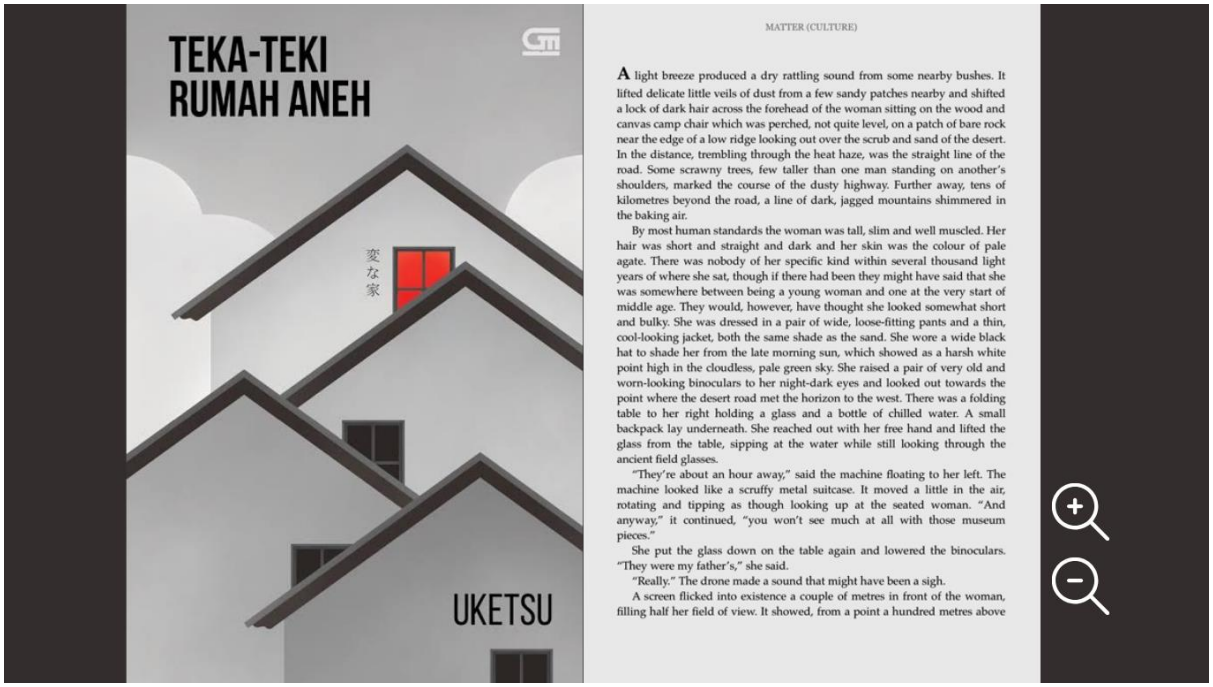
Gambar 3.2.2 Rancangan antarmuka laman ‘Store’ untuk membeli buku.

3.2.3 Membaca Buku

Pengguna yang sudah memiliki suatu buku dapat langsung membaca buku tersebut dengan mengklik tombol ‘Read now’ yang terletak pada laman ‘Book’. Tombol ini hanya akan terlihat jika pengguna sudah memiliki akses terhadap buku tersebut.



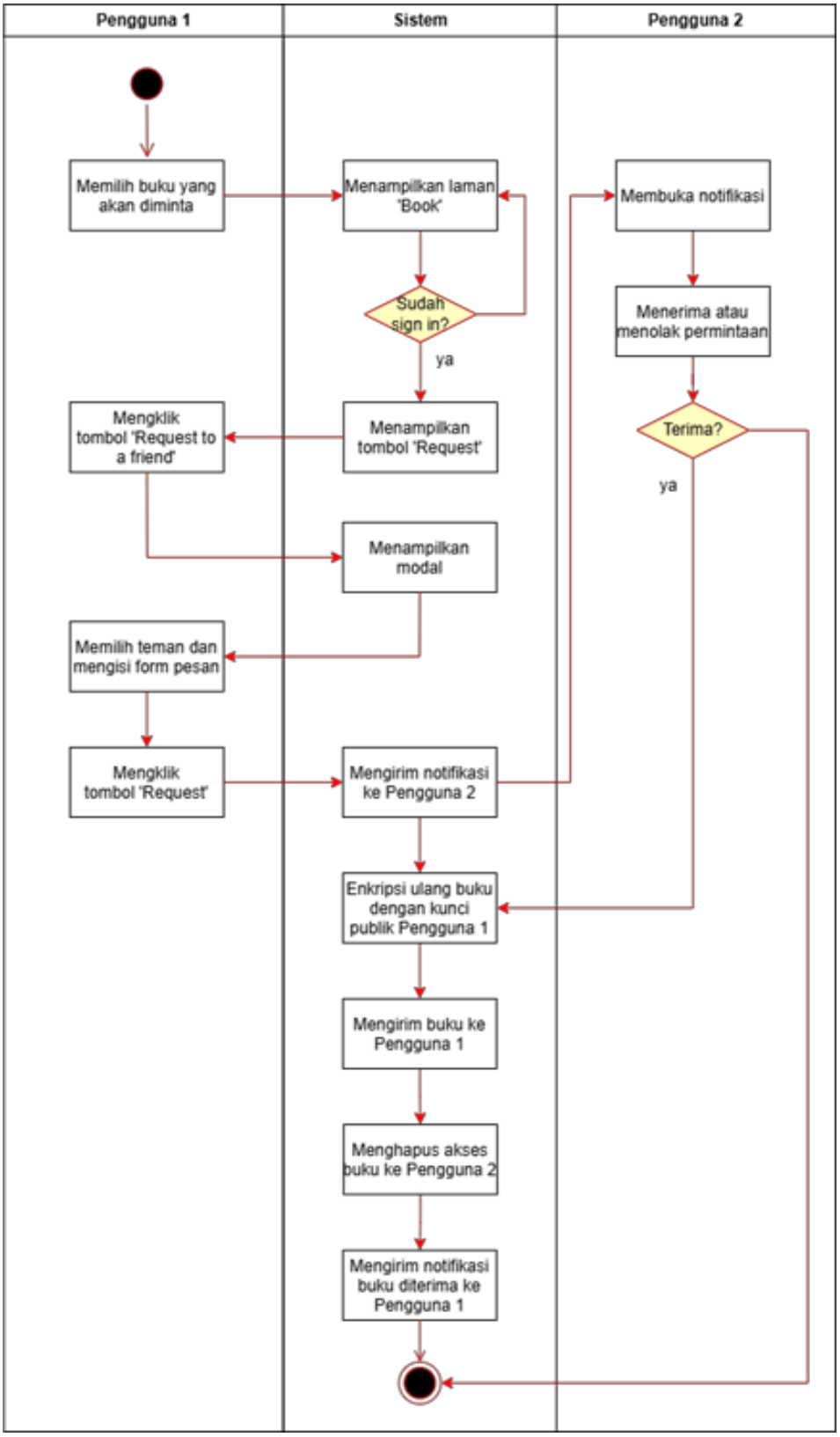
Gambar 3.2.3 Diagram aktivitas membaca buku.



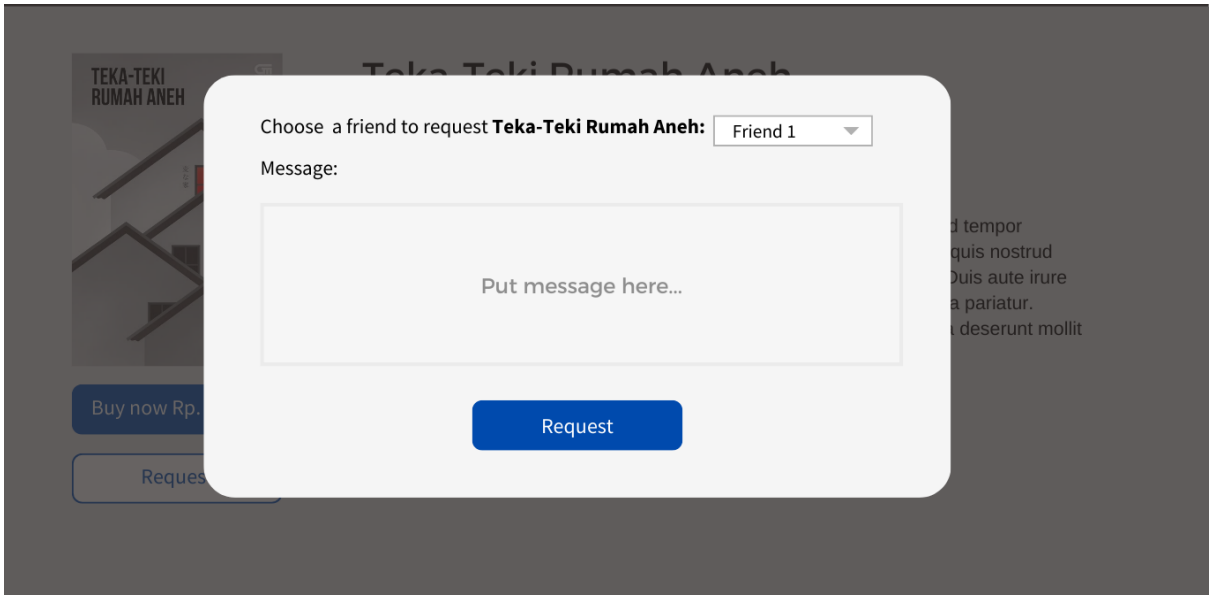
Gambar 3.2.3 Rancangan antarmuka membaca buku.

3.2.4 Memberi Buku

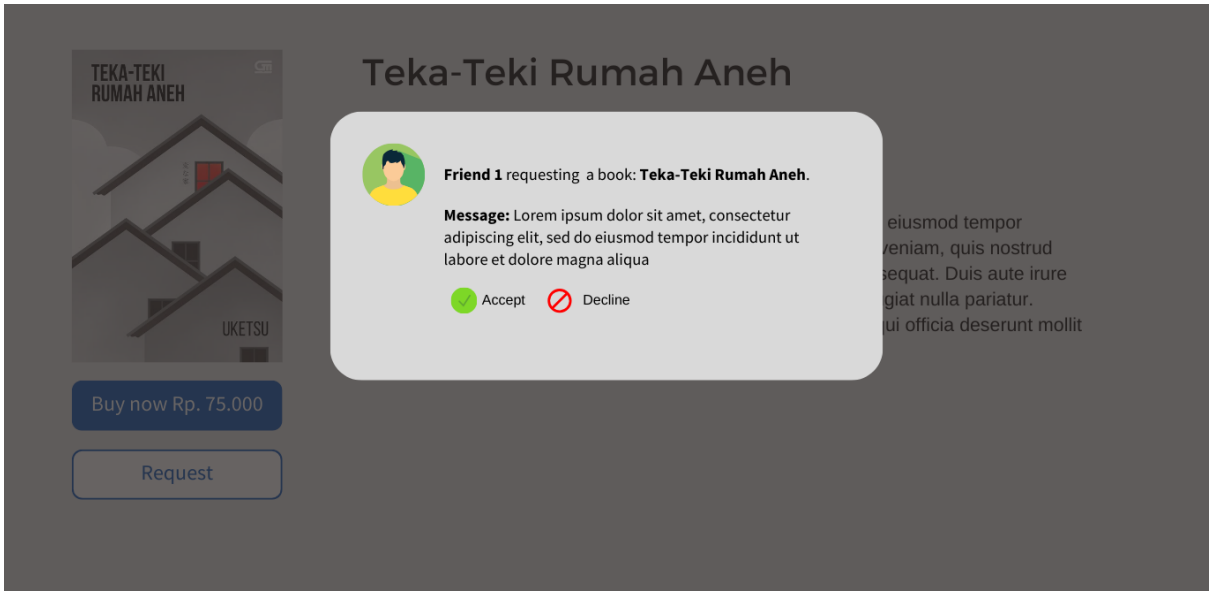
Memberi buku merupakan salah satu komponen utama dalam sistem. Fitur ini memungkinkan setiap pengguna untuk menerima dan memberikan buku dengan syarat bahwa kedua pengguna sudah saling berteman. Pengguna dapat mengajukan permintaan ke pengguna lain melalui tombol 'Request to a friend' pada laman 'Book'. Sistem akan menampilkan sebuah modal yang berisi daftar nama pengguna yang memiliki buku tersebut, beserta kolom pesan yang harus diisi. Setelah permintaan berhasil terkirim, sistem akan mengirim notifikasi ke pengguna tujuan yang berisi informasi nama pengguna yang melakukan permintaan, judul buku yang diminta, isi pesan, tombol persetujuan dan penolakan. Pada proses ini, setelah buku berhasil terkirim, buku akan berpindah hak milik dari pengguna pemberi ke penerima. Buku yang baru saja diterima dapat dibaca atau diberikan kepada pengguna lain. Proses ini memiliki keterkaitan seperti model bisnis di dunia nyata, yang di mana seorang pemilik buku dapat memberikan buku kepada orang lain.



Gambar 3.2.4 Diagram aktivitas memberi buku.



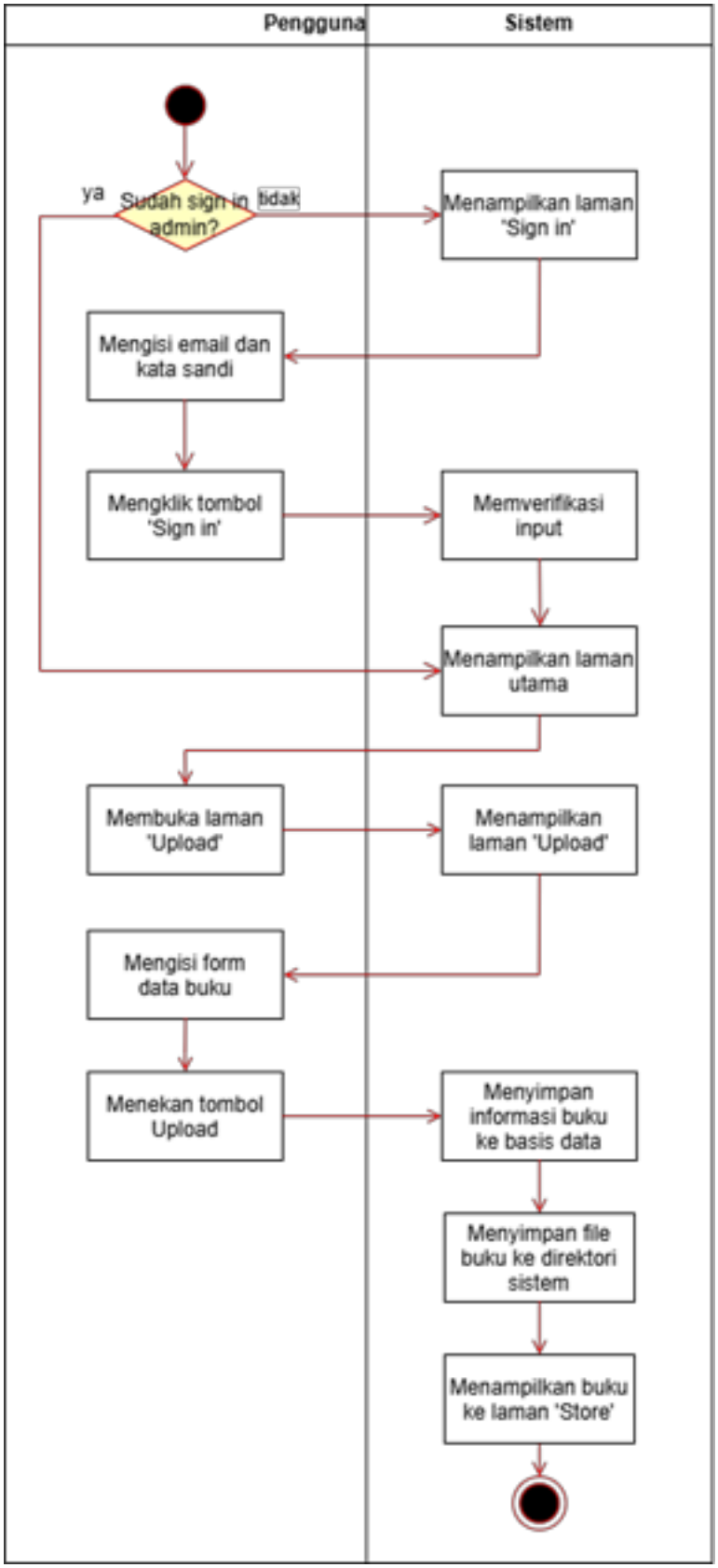
Gambar 3.2.4 Rancangan antarmuka *modal* pada laman ‘Book’ untuk proses permintaan.



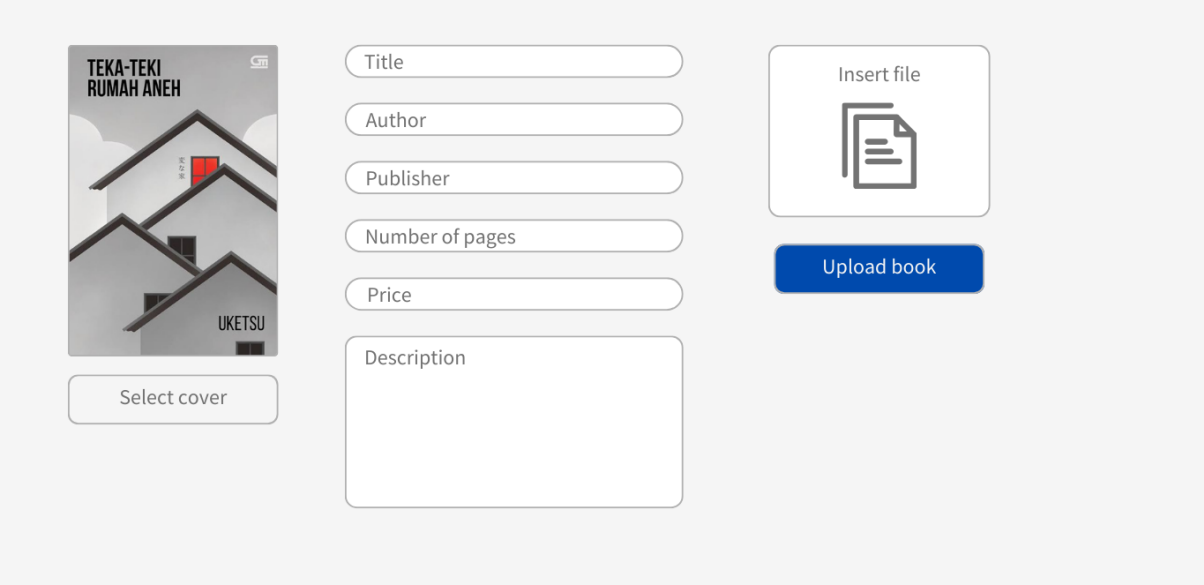
Gambar 3.2.4 Rancangan antarmuka notifikasi permintaan buku.

3.2.5 Mengunggah Buku

Mengunggah buku adalah fitur yang hanya dapat dilakukan oleh pengguna yang memiliki *role* admin. Pada laman mengunggah buku, admin akan mengisi identitas buku yang akan diunggah yang berupa judul, sampul, penulis, penerbit, jumlah halaman, harga, deskripsi, dan *file* buku. Setelah buku diunggah, buku akan langsung ditampilkan pada laman ‘Store’.



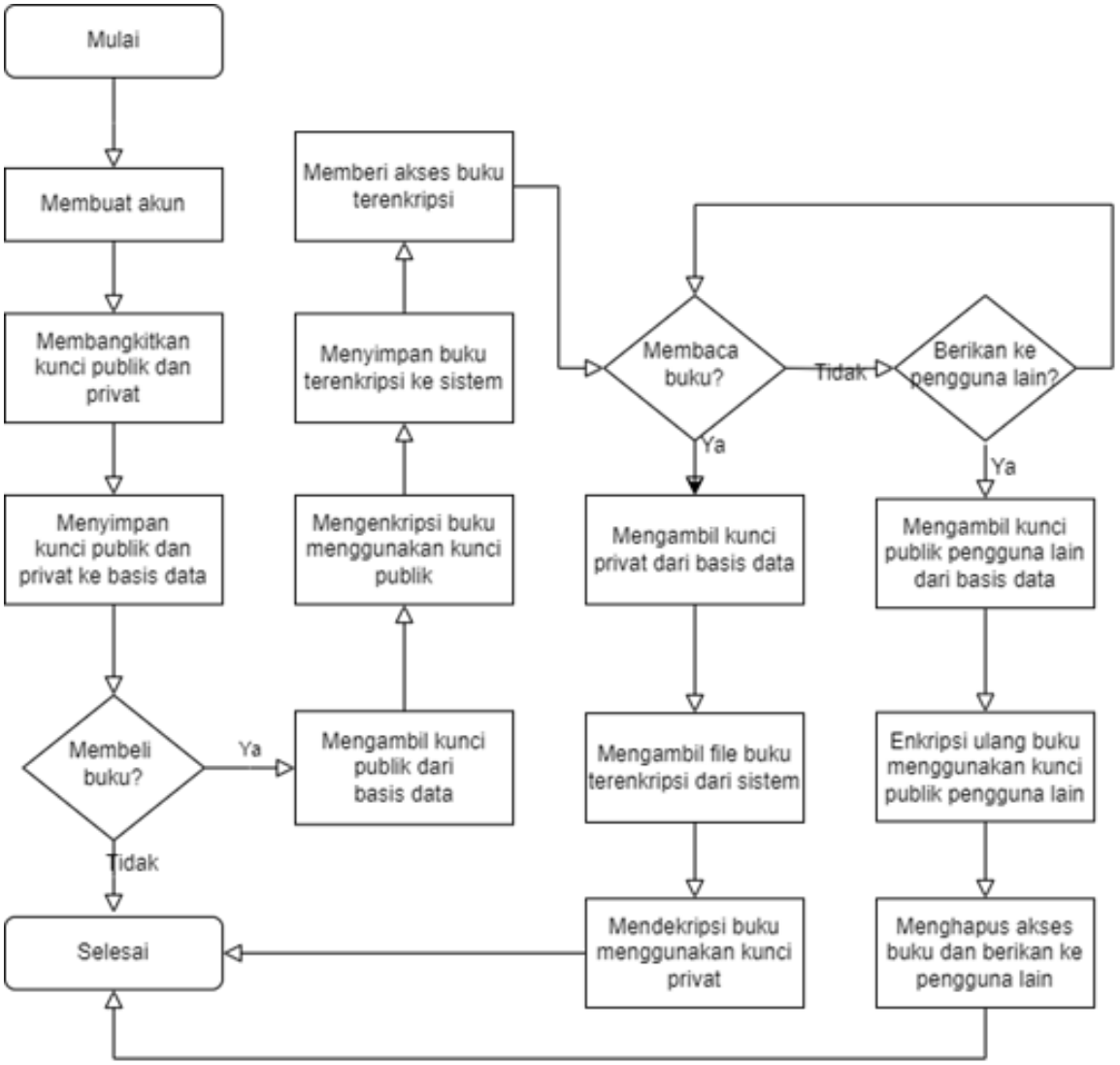
Gambar 3.2.5 Diagram aktivitas mengunggah buku.



Gambar 3.2.5 Rancangan antarmuka mengunggah buku.

3.3 Cara Kerja Kriptografi

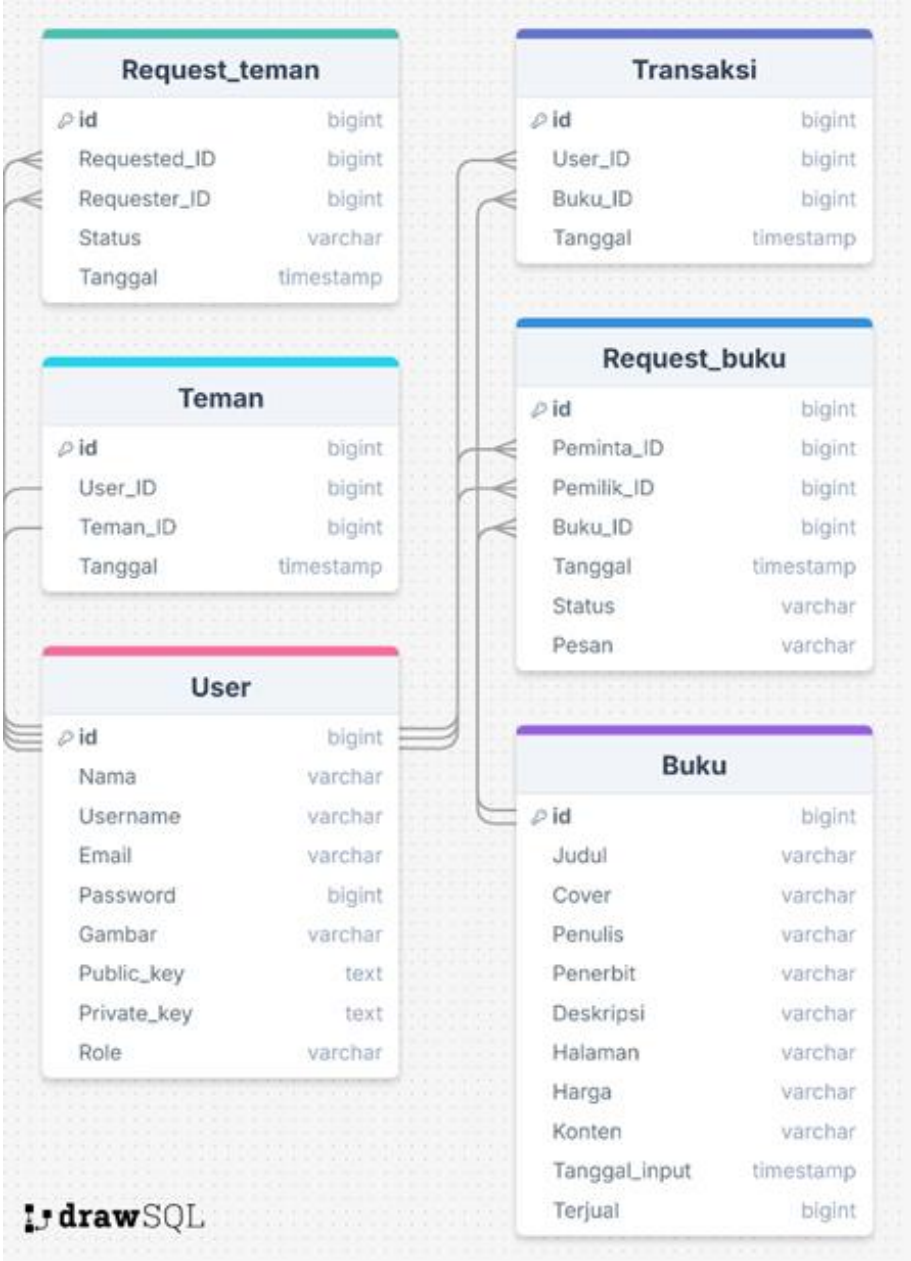
Proses kriptografi dalam sistem dijalankan pada saat pembelian buku, pemberian buku, dan membaca buku. Proses ini melibatkan kunci publik dan kunci privat yang dimiliki setiap pengguna. Pengguna harus terdaftar ke dalam sistem terlebih dahulu untuk mendapatkan pasangan kunci publik dan kunci privat, yang akan disimpan ke basis data. Setelah terdaftar, pengguna dapat melakukan pembelian yang dimana proses enkripsi menggunakan kunci publik akan berjalan. Buku yang terenkripsi kemudian akan disimpan ke dalam direktori sistem. Setelah memiliki akses terhadap buku tersebut, pengguna dapat membaca dan memberikan kepada pengguna lain. Sebelum dapat dibaca, buku akan melalui proses dekripsi terlebih dahulu menggunakan kunci privat pengguna yang diperoleh dari basis data. Jika akan memberikan kepada pengguna lain, buku akan melalui proses enkripsi ulang menggunakan kunci publik pengguna tujuan.



Gambar 3.3 Diagram alir cara kerja kriptografi.

3.4 Perancangan Basis Data

Basis data digunakan untuk menyimpan informasi data yang masuk ke dalam sistem. Dalam pengembangan sistem, basis data yang digunakan adalah SQL. Basis data ini terdiri atas enam tabel utama, yaitu tabel ‘User’, ‘Buku’, ‘Transaksi’, ‘Request_teman’, ‘Teman’, dan ‘Request_buku’.



Gambar 3.4 Rancangan basis data.

a. Tabel ‘User’

Tabel ‘User’ adalah tabel yang menyimpan data pengguna terdaftar. Tabel ini terdiri dari kolom-kolom data diri pengguna, yaitu: ‘ID’, ‘Nama’, ‘Username’, ‘Email’, ‘Password’, dan ‘Gambar’. Setelah pengguna mendaftar, sistem akan memberikan pasangan kunci publik dan kunci privat yang akan disimpan pada masing-masing kolom ‘Public_key’ dan ‘Private_key’. Sepasang kunci ini nantinya akan digunakan dalam proses enkripsi dan dekripsi buku. Pada tabel ini, juga terdapat kolom ‘Role’ yang menentukan peran pengguna, apakah sebagai admin atau pengguna biasa.

b. Tabel ‘Buku’

Tabel ‘Buku’ merupakan tabel yang digunakan untuk menyimpan data buku. Tabel ini memiliki kolom-kolom yang memuat informasi buku, yaitu: ‘ID’, ‘Judul’, ‘Cover’, ‘Penulis’, ‘Penerbit’, ‘Deskripsi’, ‘Halaman’, ‘Harga’, ‘Konten’ (berisi nama *file* buku yang tersimpan dalam direktori sistem), ‘Tanggal_input’, dan ‘Terjual’ (menunjukkan jumlah buku yang telah terjual).

c. Tabel ‘Transaksi’

Tabel ‘Transaksi’ berfungsi untuk menyimpan data pembelian buku. Tabel ini memiliki kolom ‘ID,’ ‘User_ID’, ’Buku_ID’, dan ‘Tanggal’. Kolom ‘User_ID’ dan ‘Buku_ID’ masing-masing merujuk pada kolom ‘ID’ pada tabel ‘User’ dan ‘Buku’.

d. Tabel ‘Request_teman’

Tabel ‘Request_teman’ adalah tabel yang digunakan untuk menyimpan data permintaan pertemanan. Tabel ini memiliki kolom ‘ID’, ‘Requested_ID’, ‘Requester_ID’, dan ‘Tanggal’. Kolom ‘Requested_ID’ menyimpan ID pengguna yang menerima permintaan pertemanan, sedangkan kolom ‘Requester_ID’ menyimpan ID pengguna yang mengirimkan permintaan tersebut. Kedua ID ini diperoleh dari kolom ‘ID’ pada tabel ‘User’.

e. Tabel ‘Teman’

Tabel ‘Teman’ berfungsi untuk menyimpan informasi pengguna yang telah menjalin pertemanan. Tabel ini memiliki kolom-kolom berupa ‘ID’, ‘User_ID’, ‘User2_ID’, dan ‘Tanggal’.

f. Tabel ‘Request_buku’

Tabel ‘Request_buku’ merupakan tabel yang digunakan untuk menyimpan data permintaan buku. Tabel ini memiliki kolom ‘ID’, ‘Peminta_ID’, ‘Pemilik_ID’, ‘Buku_ID’, ‘Tanggal’, ‘Status’, dan ‘Pesan’. Kolom ‘Peminta_ID’ menyimpan ID pengguna yang mengajukan permintaan, sedangkan kolom ‘Pemilik_ID’ menyimpan ID pengguna pemilik buku yang diminta. Kedua ID tersebut diambil dari tabel ‘User’, sementara data pada kolom ‘Buku_ID’ diperoleh dari kolom ‘ID’ pada tabel ‘Buku’. Kolom ‘Status’ memuat informasi tentang status permintaan, yaitu diterima (‘Accepted’), ditolak (‘Declined’), dan menunggu konfirmasi (‘Pending’).

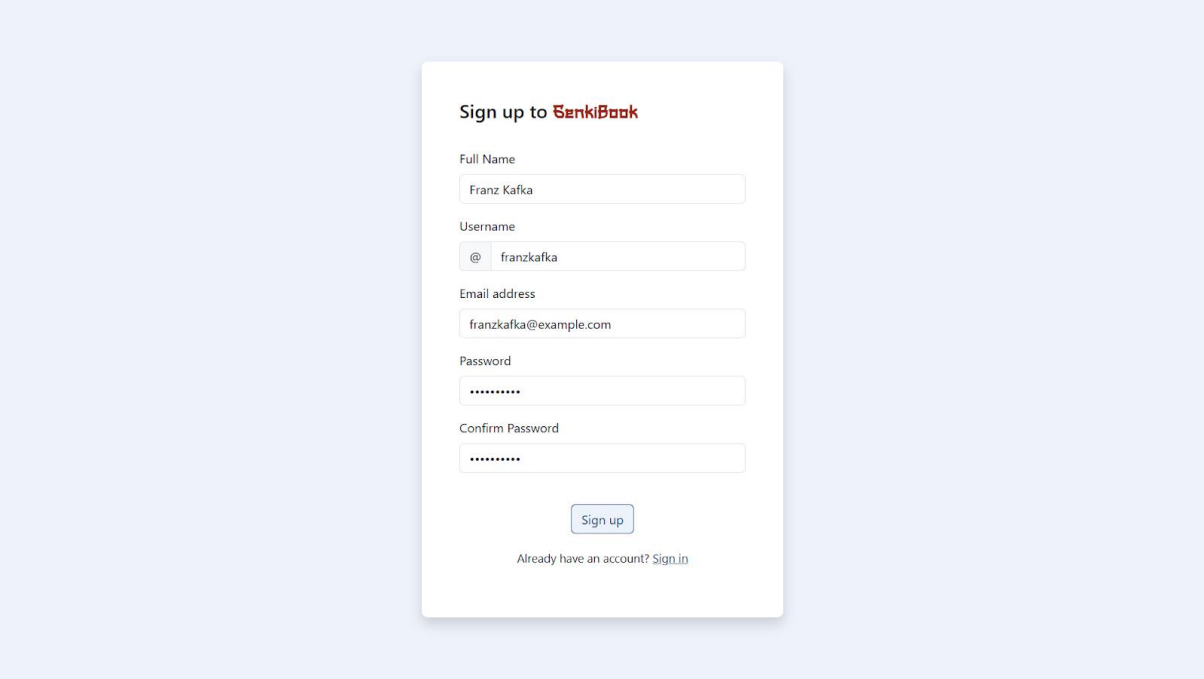
BAB IV
HASIL DAN PEMBAHASAN

4.1 Hasil Implementasi Sistem

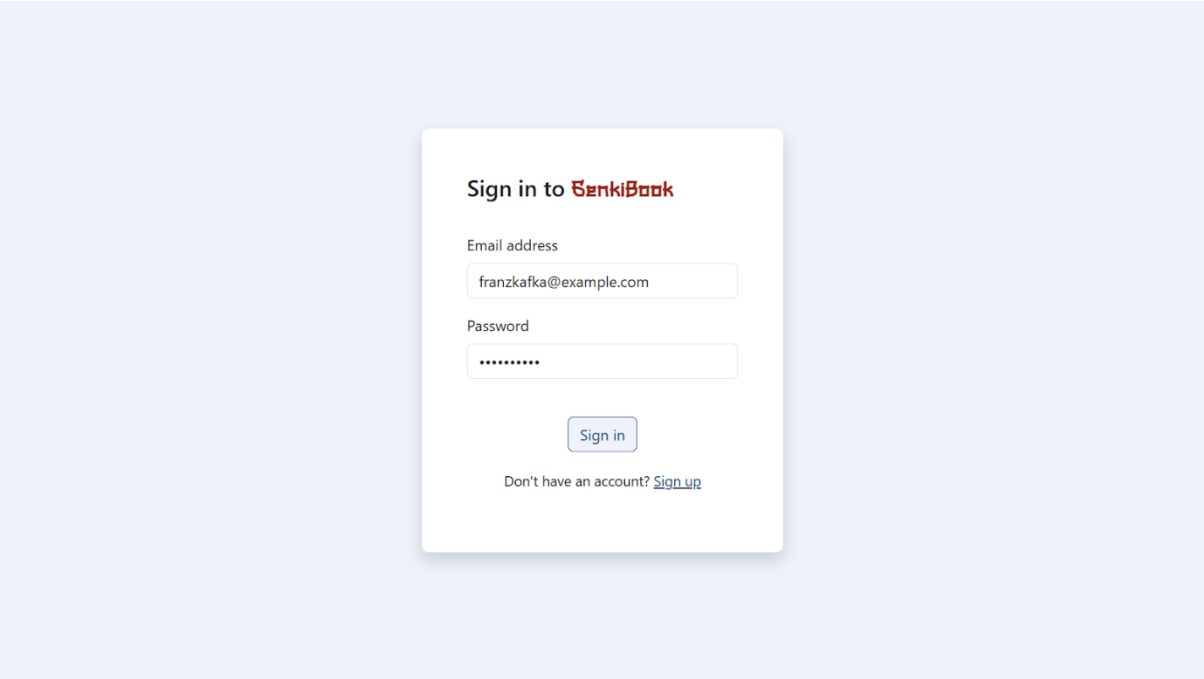
Pada tahap ini, sistem yang dirancang telah melewati tahap pengembangan sehingga sistem telah dapat dijalankan. Sistem ini dikembangkan dengan bantuan aplikasi *text editor* Microsoft Visual Studio Code menggunakan bahasa HTML dan CSS untuk frontend, serta PHP dan basis data SQL untuk *backend*. Sistem ini juga menggunakan *framework* Bootstrap untuk membantu mengembangkan tampilan *website* dan OpenSSL untuk implementasi algoritma RSA.

4.1.1 Pembuatan Akun Pengguna

Syarat utama bagi pengguna untuk dapat melakukan pembelian dan pemberian buku adalah memiliki akun. Untuk membuat akun, pengguna dapat mengisi form pada laman "Signup" yang mencakup nama lengkap, nama pengguna, alamat email, kata sandi, dan konfirmasi kata sandi. Setelah mengisi form, pengguna dapat mengklik tombol "Sign Up" dan akan diarahkan menuju halaman "Login" untuk melakukan proses masuk ke dalam akun. Pada tahap pembuatan akun, sistem akan membangkitkan kunci publik dan kunci privat yang kemudian akan digunakan untuk proses enkripsi dan dekripsi dalam transaksi, pemberian buku, serta membaca buku.



Gambar 4.1.1 Antarmuka laman ‘Sign Up’.



Gambar 4.1.1 Antarmuka laman ‘Sign In’.

```
$rsa = openssl_pkey_new([
"private_key_bits" => 2048,
"private_key_type" => OPENSSL_KEYTYPE_RSA,
]);
```

```
// Ekspor kunci privat ke $privateKey
openssl_pkey_export($rsa, $privateKey);

// Ekspor kunci publik ke $publicKey
$details = openssl_pkey_get_details($rsa);
$publicKey = $details['key'];
```

Gambar 4.1.1 Kode program pembangkitan kunci publik dan kunci privat.

```
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAknINkbOtLpwmZdc6jmNH
yP1uMuY3RSE0G8bnrbFGmyi1NdBODJ7vgDFrPSkMLCv/3Gx2xj8fsh7B4nHz62Ce
wMC1BOYqhZ1GSQ756fZM1gKHsJBj4z5px5B/0YOS38EYJTWgVHMXnFHLrHsQIsfJ
u0/XdV7g21LYfmFpqBbh7fPg6W0h2snvkgsorwb5ll1IQGvOKfQJfqXzjUqKg3cN
6/AyHz+ldZEOEJmY1Sg8kWjUc6OC8tJg/2Hoj7E4QeWa9r3BBUDOyGh6KEdY7U7T
jf583LXXZNu/hbLMzCFpsZOC0yK2CVqrNMkia/xN6Dqlqhd8eA6OPRRn64pM0eTh
CwIDAQAB
-----END PUBLIC KEY-----
```

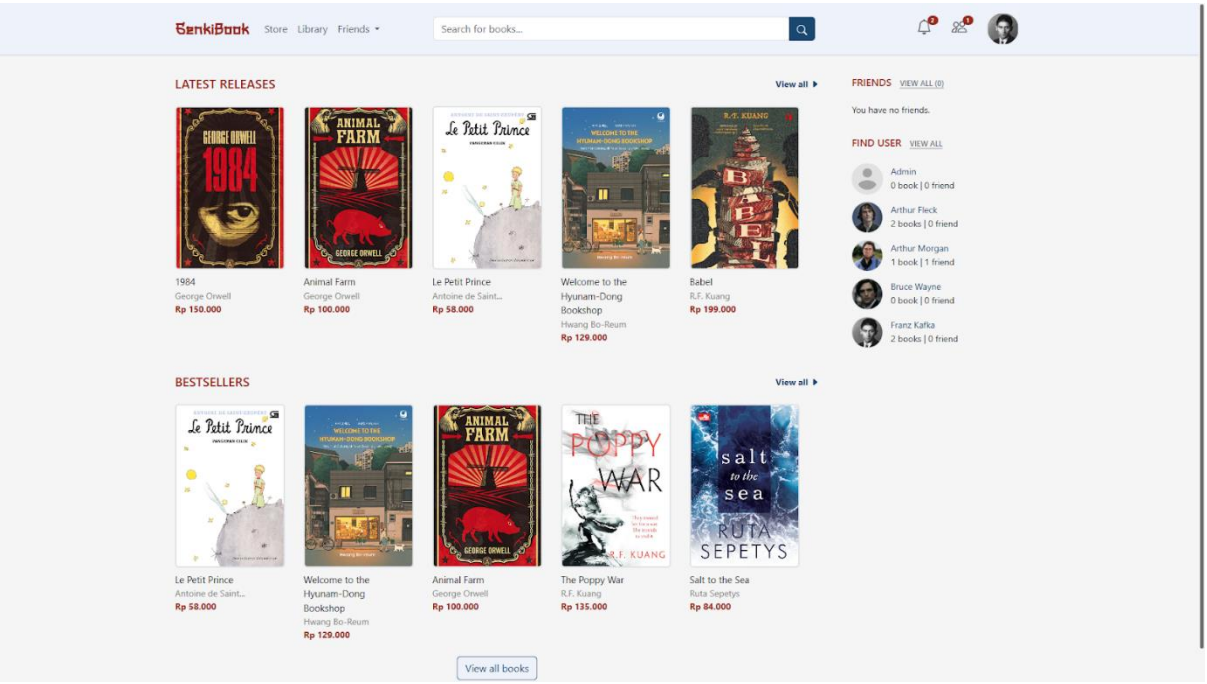
Gambar 4.1.1 Hasil pembangkitan kunci publik.

```
-----BEGIN PRIVATE KEY-----
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQCiDpzIBFeN887O
qYuzkWcEiDNc3mwZyJ7qZ/rpG2Q/mGBqrmiMpwHXW5vUuTu+I7ctmUWAxLmflYwZ
mi+ygm+Rlgu1wzBJxGjeqyRrH0xonaqjzehVIZlW3W8QT+JP8Udf5Yk5vgPcFrv4
xI9cYjMzpDW11HIUEWc6QT8CXysriaz8hFFCWUrg9q2jgesP+SguGhNrObOqnOg+
LCwy3bheZlP+7Tapb/vjGnufIrsYaysZvkwaR+dZ9dCNCsiK9knPU7IJ0kAU5iBS
qVHER5ivLb0smXhirz8JlbqH9u3uaezG/MlsUWPkOkGgw2VcqXrgRJ0w68G0tFS4
qEoJlJTxAgMBAAECggEATLR16QaFGp+IB7GgekIcbLy68v4kVJ/s+C53SNa6QI+z
M0uSGOEDsheeTrXOXVUyYtblWunCopJ6WbPtV6T9gf9vU30r4f6hVKPU/Q83b10R
Y68WhRT+K2tsImBtUkF18yIGLdqOoSHxnvIKmUOx0IOtGH+R74W9QomXdVvuZxBm
FJwDZVV6g/LrYry+qtt4AtJ6XfhmYQGHn6rtXgSRNSKGYUqpy4BPWG0Gh7/ioqoE
1I2V0BClUpPDzlzwMwk6qT5Q0aY1WOA8pJYZYOtrJvEMYKtcpwAfyBFiXquAlmVX
wei/zlGcrsDXkG2Zbvpi/yjnYGQI+BZsaBDR/UpHMQKBgQDaUSEuZvHNRistyCUg
9VrdKQClocTZu/icQzviKZ3Otq4Aa/B9akR5rtVCCl88/DLHc3iikD+PDQ5mMsX5
CFMcCG0wwdVE876EsWUL5QhiYkcXevzzRQwuxRO1wT2996cse4+wMoUDYWcUrK6E
9JUEmJMbKQ3Wyy/AugYbdi5hzwKBgQC+B4DpeQ6xQUpVQlKT11WDYjxYOiIOkrT+
wflCeAS6/yKgMbH+jUoeibuT7PtkvJ15Fdy74TG6rfJ8ycYPc+cZ8zFsQOYc11y1
xJDXly1rKhsTAw01X/MXmC5ZSKwOHKymJ/fcyld13bl5VJAfyGhLJ6xvsu88tlsc
vRBKH10NPwKBgQDD4Zs1+SPnnJfNYhD+O2alnM55zmXDPsbX3fNy/wgamwoQUsja
nmiGDXpG4OuG2nntPwv0QBznCz3qMJA022VGd8EQyDnEvjYo9MnHHF6jd651wOII
m+FMbYM7xwDQ283hOZQ48XsrB0/n2vBTVugF0afb7MAAAxr7f21PYoBHPQKBgAbI
9c1gSSoDDshkidZFfOAoDceIq9ahX10KSAAbkO+sVGwr2hMgsFjOyifJ+l/qbCT6
ptr+e2wS8emKusuqc8H1cPpQhubYubKzxggsma6N3lGbdklFl8Rr5pvBgIMweumj
27HCd8T5mbm/TzYTTcYBMKL8XJZqXG52QbKj1Aq5AoGBAJMmGov2RxmUYSXsojgt
hSkjUmUwdR8kD3AfqYNmHe0aUcgztPpOe6vv67+4L1z8WBhnZW81qBcX1mcvoEs1
MchqWdd8mHlXpFyfs88fqfXvGAIEXO9n6a5UTU2UtR4BOs3ys6PCnGF8O2sfUFz9
dE9ohqXWFagQXFejVmqrKsmq
-----END PRIVATE KEY-----
```

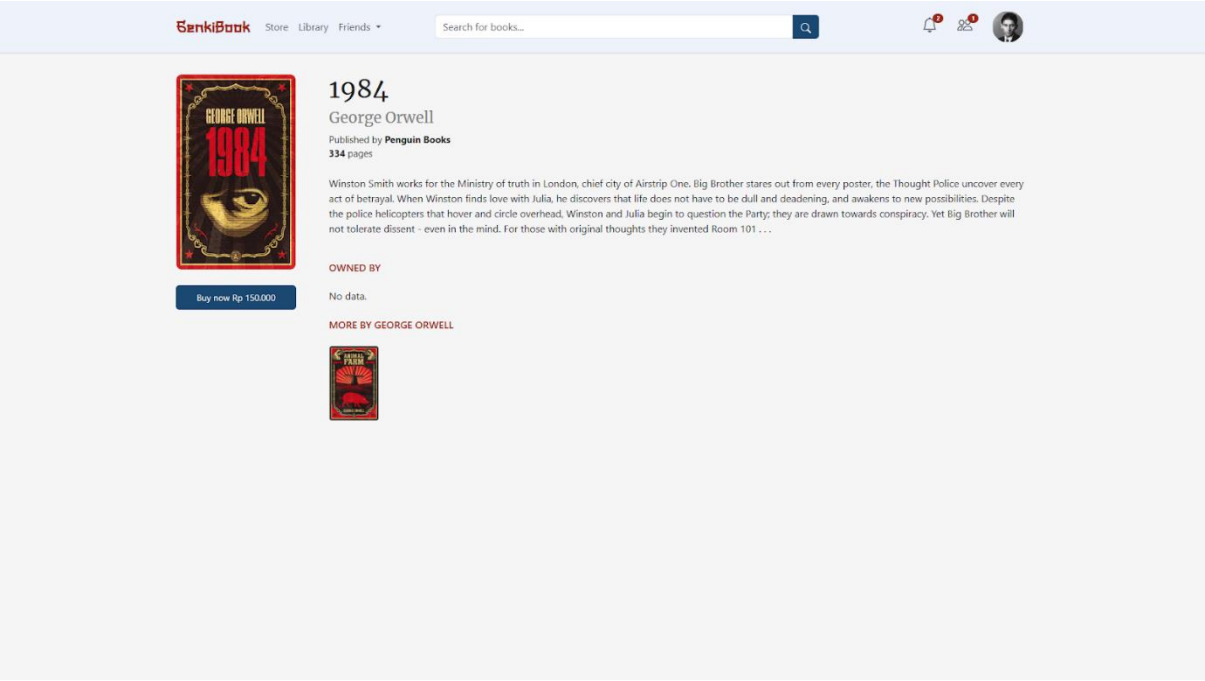

Gambar 4.1.1 Hasil pembangkitan kunci privat.

4.1.2 Pembelian Buku

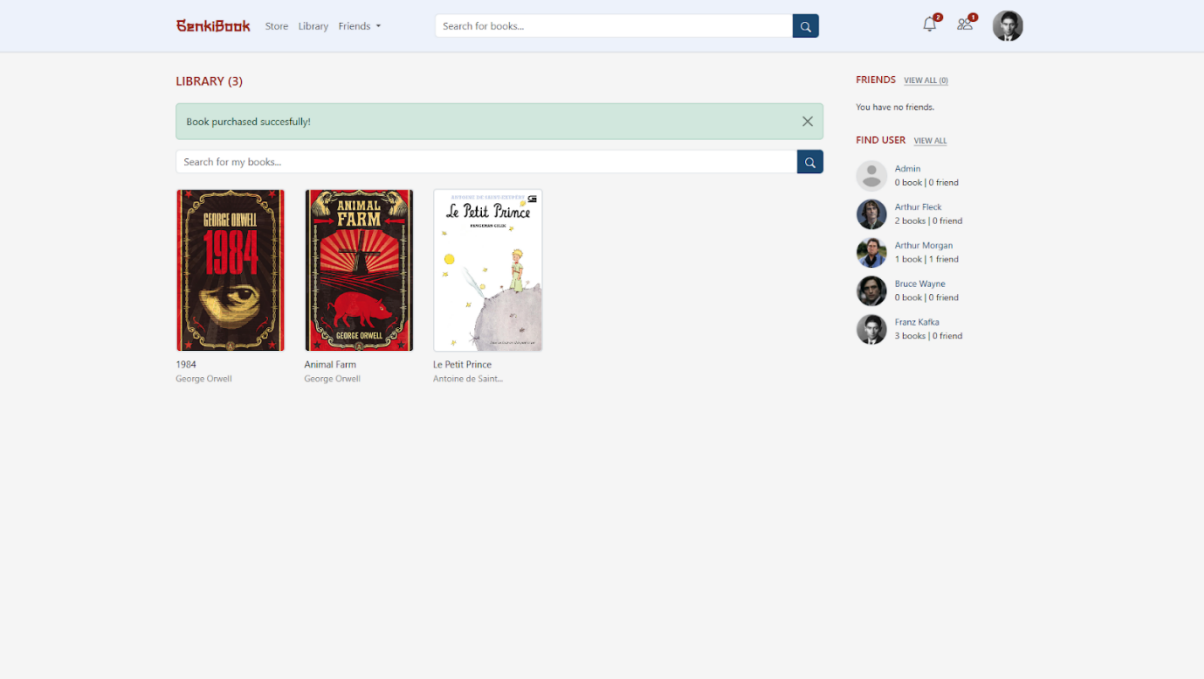
Untuk membeli buku, pengguna dapat mengklik buku yang diinginkan pada laman ‘Store’, kemudian akan diarahkan ke laman ‘Book’. Pengguna dapat membeli buku dengan mengklik tombol ‘Buy Now’. Pada proses *backend*, sistem akan mengambil dan membaca *file* buku dari direktori sistem. *File* buku yang terbaca akan dienkripsi oleh sistem menggunakan fungsi dari *library* OpenSSL. Proses enkripsi menggunakan kunci publik pengguna yang diperoleh dari basis data. *File* yang berhasil terenkripsi akan disimpan kembali ke direktori sistem. Setelah transaksi berhasil, pengguna akan dialihkan ke laman ‘Library’.



Gambar 4.1.2 Antarmuka laman ‘Store’.



Gambar 4.1.2 Antarmuka laman ‘Book’.

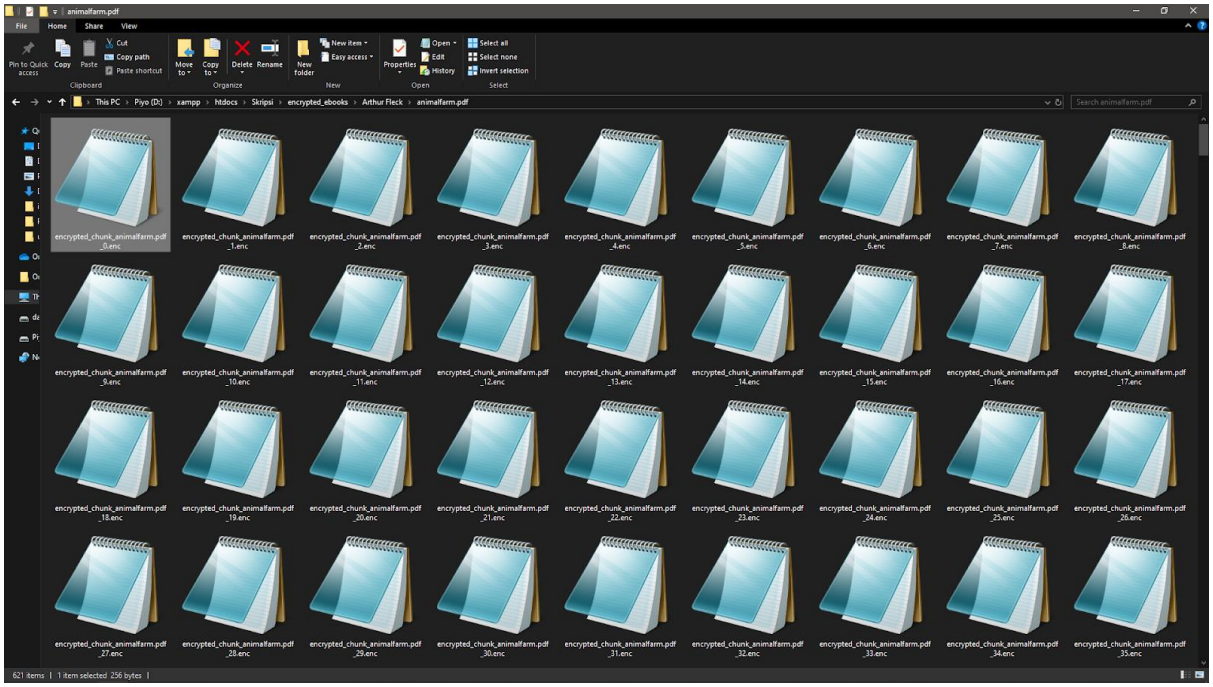


Gambar 4.1.2 Antaramuka laman ‘Library’ setelah transaksi berhasil.

```
// Membaca file e-book dari direktori
$pdf_file = file_get_contents($target_file);

// Memecah file menjadi blok 245 bit
$chunks = str_split($pdf_file, 245);

// Enkripsi setiap blok menggunakan RSA
$encrypted_chunks = [];
foreach ($chunks as $chunk) {
    if (openssl_public_encrypt($chunk, $encrypted_chunk, $public_key)) {
        $encrypted_chunks[] = $encrypted_chunk;
    } else {
        die("Encryption failed for chunk: " . openssl_error_string());
    }
}
// Menyimpan blok terenkripsi ke direktori
$encrypted_path = "encrypted_ebooks/{$nama}/{$konten}/";

// Membuat direktori baru jika direktori tidak ada
if (!file_exists($encrypted_path)) {
    mkdir($encrypted_path, 0777, true);
}

foreach ($encrypted_chunks as $index => $encrypted_chunk) {
file_put_contents("{$encrypted_path}encrypted_chunk_{$konten}_$index.enc",
```

```
$encrypted_chunk);
 }
```

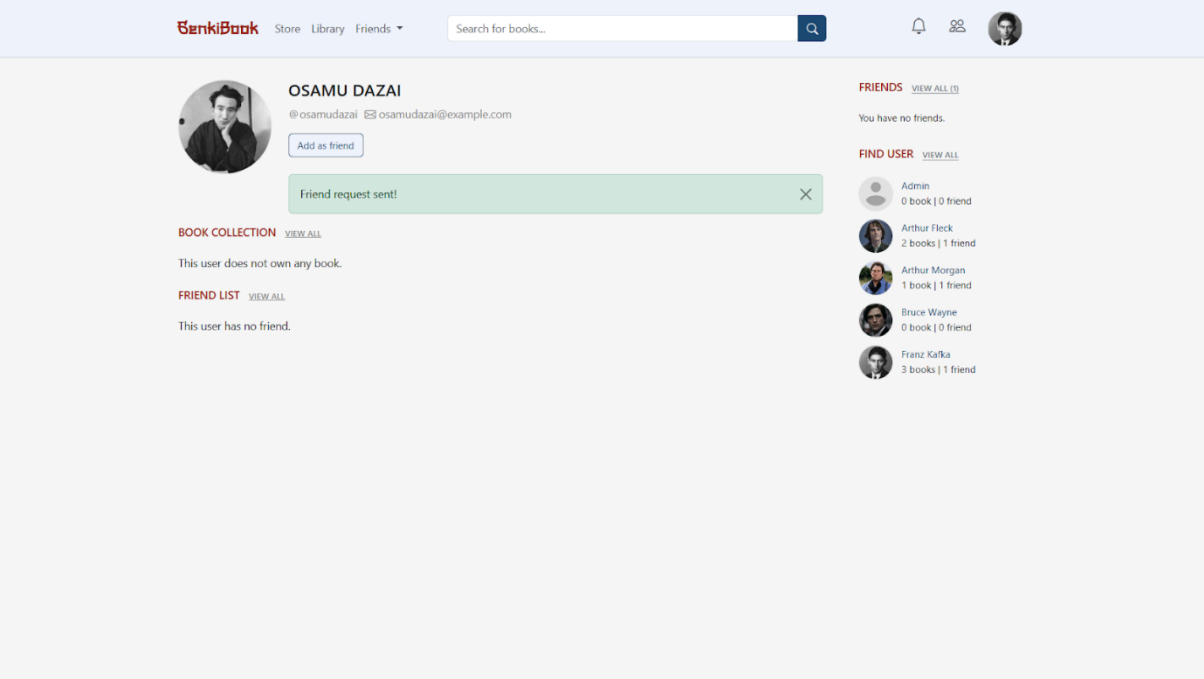
Gambar 4.1.2 Kode program proses enkripsi pada saat pembelian buku.



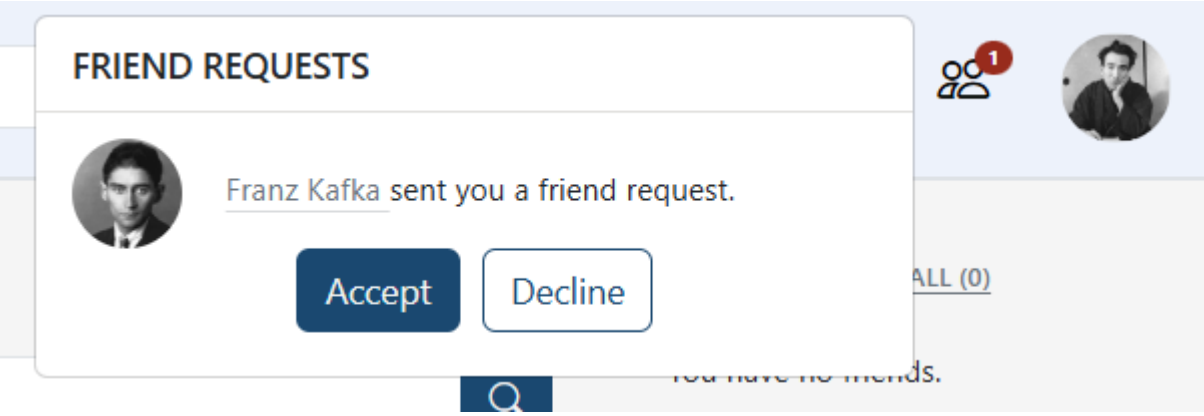
Gambar 4.1.2 *File* blok hasil enkripsi buku menggunakan algoritma RSA.

4.1.3 Pertemanan Antar Pengguna

Proses pertemanan antar pengguna melibatkan dua pihak, yaitu Pengguna A sebagai pengirim permintaan dan Pengguna B sebagai penerima permintaan. Pengguna A dapat mencari Pengguna B dengan membuka laman ‘User’ atau melalui kolom pencarian. Jika ingin menambahkan Pengguna B sebagai teman, Pengguna A dapat mengirimkan permintaan pertemanan melalui laman ‘Profile’ milik Pengguna B. Setelah permintaan pertemanan terkirim, sistem akan mengirimkan notifikasi ke Pengguna B beserta tombol persetujuan dan penolakan. Apabila permintaan pertemanan ditolak, sistem akan membatalkan seluruh proses permintaan pertemanan. Namun, jika permintaan diterima oleh Pengguna B, sistem akan memperbarui basis data dengan menambahkan informasi bahwa Pengguna A dan Pengguna B telah berstatus teman.



Gambar 4.1.3 Antarmuka laman ‘Profile’ Pengguna A setelah permintaan pertemanan terkirim.

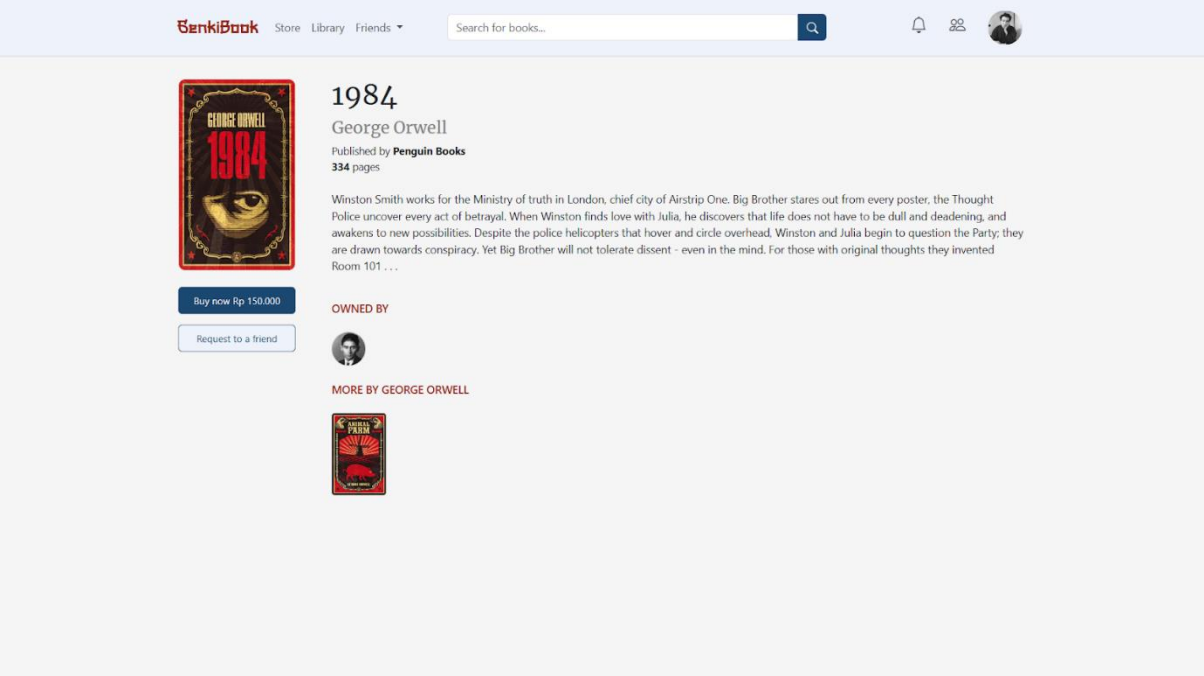


Gambar 4.1.3 Antarmuka notifikasi permintaan pertemanan pada Pengguna B.

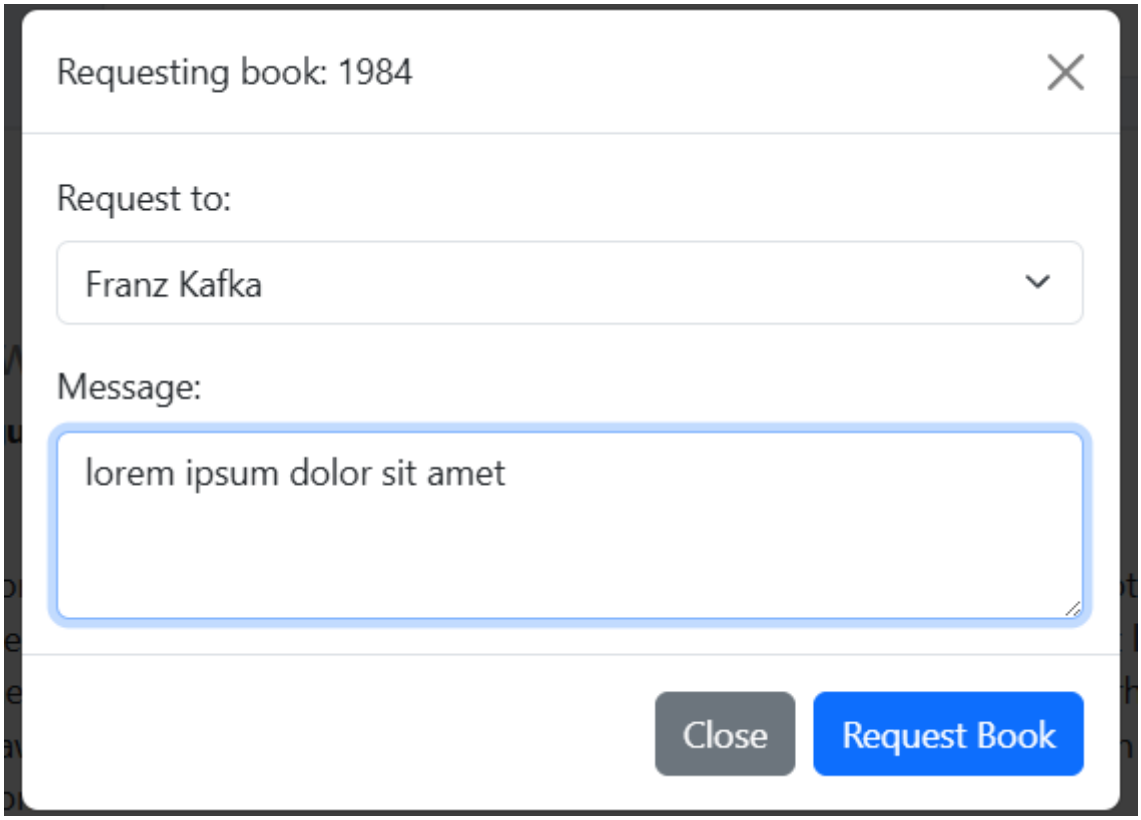
4.1.4 Pemberian Buku

Proses pemberian buku melibatkan dua pengguna, yaitu Pengguna A sebagai penerima buku dan Pengguna B sebagai pemberi buku. Sebelum pemberian buku dapat dilakukan, kedua pengguna harus sudah berteman. Pengguna A dapat mengajukan permintaan dengan membuka laman buku yang diinginkan dan menekan tombol *request*, yang akan memunculkan *modal* berisi formulir untuk memilih teman tujuan dan menyertakan alasan permintaan buku. Setelah formulir diisi dan permintaan dikirim, sistem akan mengirimkan notifikasi kepada Pengguna B. Pengguna B dapat memilih untuk menerima atau menolak permintaan tersebut. Jika permintaan ditolak, sistem akan membatalkan seluruh proses

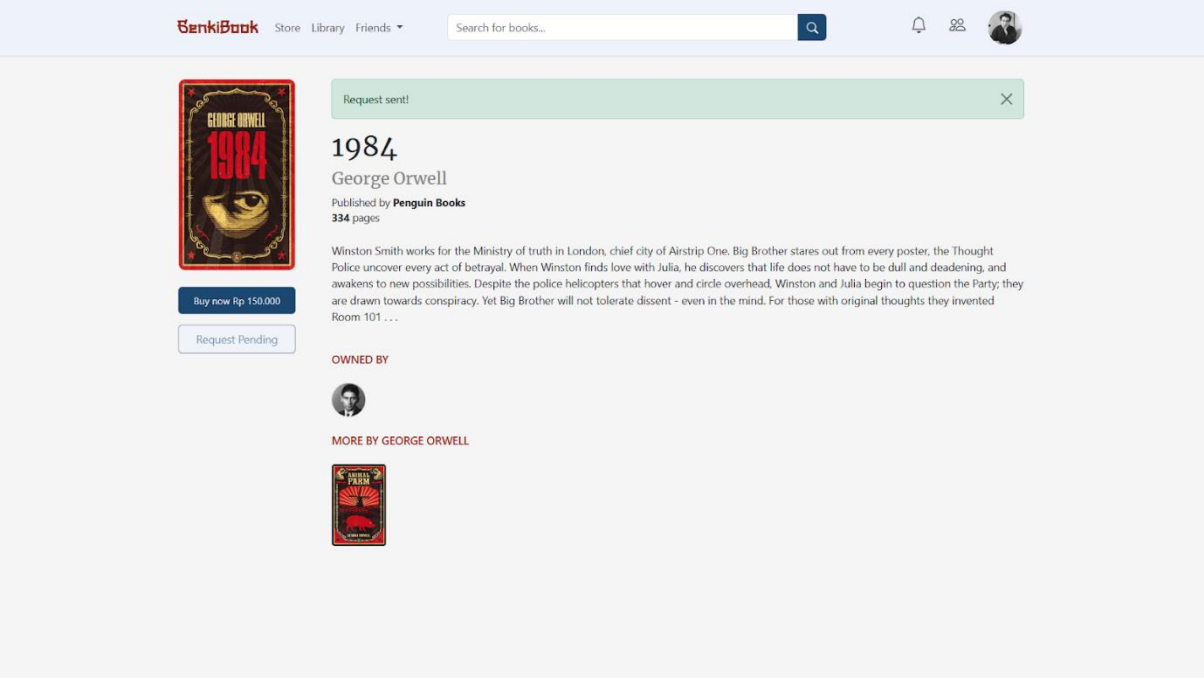
permintaan. Jika permintaan diterima, buku yang telah dienkripsi menggunakan kunci publik Pengguna B akan dienkripsi ulang menggunakan kunci publik Pengguna A. Tujuan dari proses enkripsi ulang adalah agar proses dekripsi dapat dilakukan oleh Pengguna A menggunakan kunci privat miliknya. Setelah proses enkripsi berhasil, sistem akan menghapus akses buku dari Pengguna B dan memberikannya kepada Pengguna A.



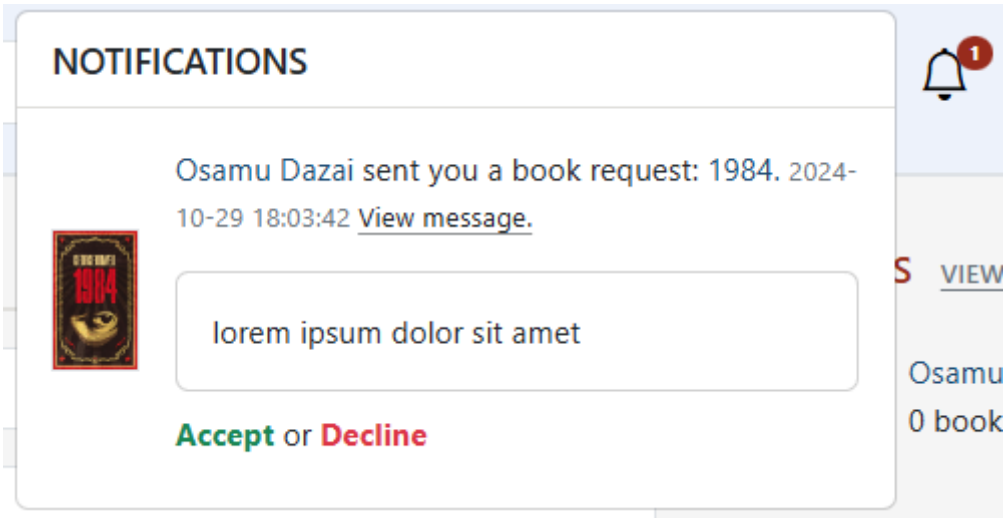
Gambar 4.1.4 Antarmuka laman ‘Book’ dengan tombol *request*.



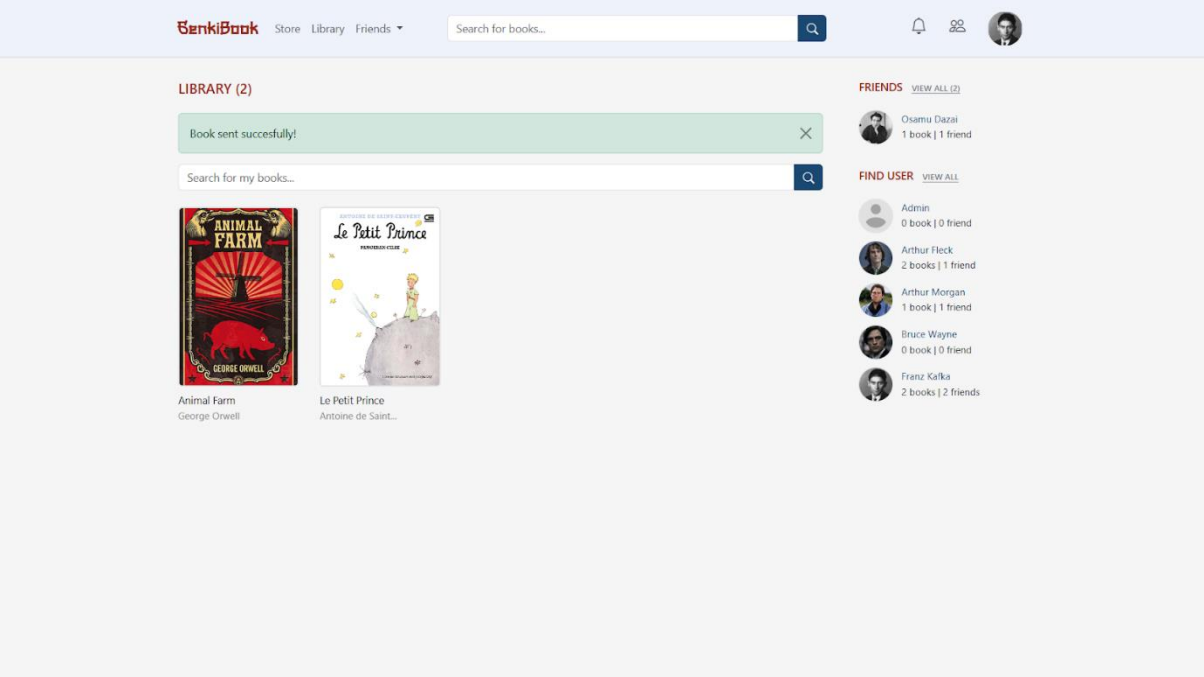
Gambar 4.1.4 Antarmuka *modal* pada laman ‘Book’ setelah mengklik tombol *request*.



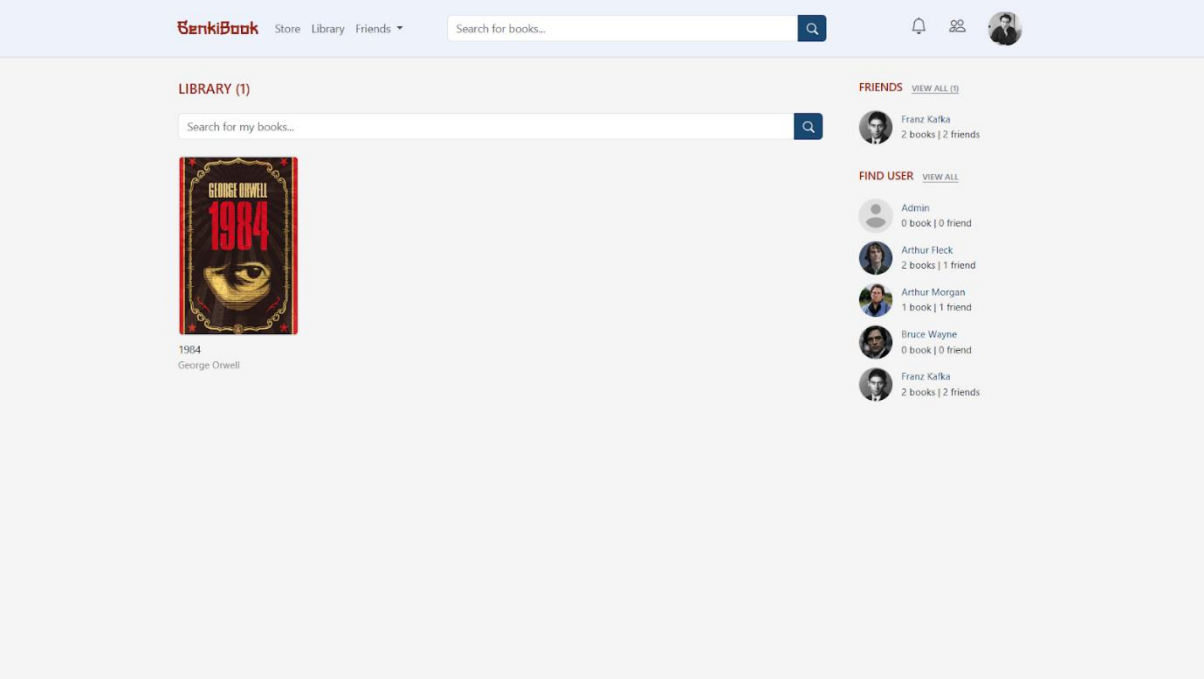
Gambar 4.1.4 Antarmuka laman ‘Book’ setelah permintaan terkirim.



Gambar 4.1.4 Antarmuka notifikasi permintaan buku dari pengguna A.



Gambar 4.1.4 Antarmuka laman ‘Library’ Pengguna B setelah buku berhasil terkirim ke Pengguna A.



Gambar 4.1.4 Buku yang diterima Pengguna B dari Pengguna A.

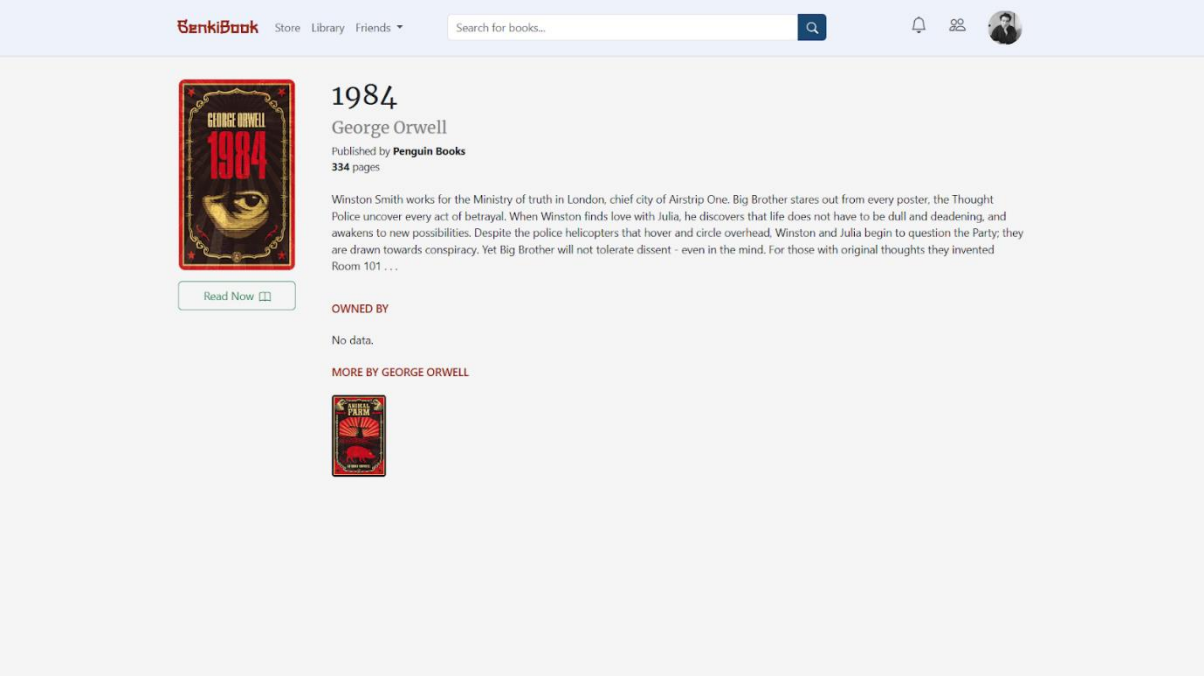
```
// Membaca file e-book dari direktori
$pdf_file = file_get_contents($target_file);

// Memecah file menjadi blok 245 bit
$chunks = str_split($pdf_file, 245);

// Enkripsi setiap blok menggunakan RSA
$encrypted_chunks = [];
foreach ($chunks as $chunk) {
    if (openssl_public_encrypt($chunk, $encrypted_chunk, $public_key)) {
        $encrypted_chunks[] = $encrypted_chunk;
    } else {
        die("Encryption failed for chunk: " . openssl_error_string());
    }
}
// Menyimpan blok terenkripsi ke direktori
$encrypted_path = "encrypted_ebooks/{$nama}/{$konten}/";

// Membuat direktori baru jika direktori tidak ada
if (!file_exists($encrypted_path)) {
    mkdir($encrypted_path, 0777, true);
}

foreach ($encrypted_chunks as $index => $encrypted_chunk) {
file_put_contents("{$encrypted_path}encrypted_chunk_{$konten}_$index.enc",
```

```
$encrypted_chunk);
 }
```

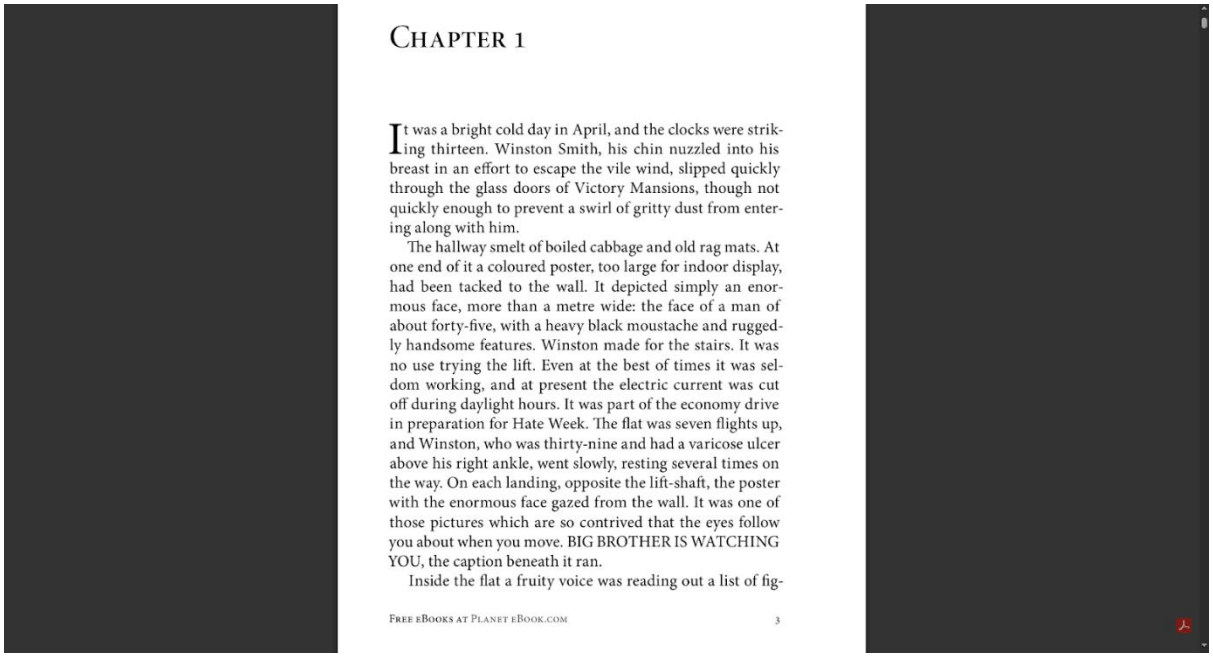
Gambar 4.1.4 Kode program proses enkripsi ulang pada saat pengiriman buku.

4.1.5 Membaca Buku

Pengguna dapat membaca buku setelah memperoleh akses, baik melalui pembelian maupun pemberian dari pengguna lain. Untuk membaca buku, pengguna dapat membuka laman buku yang akan dibaca dan menekan tombol ‘Read Now’. Setelah tombol diklik, sistem akan membuka *tab* baru dan melakukan proses dekripsi menggunakan kunci privat pengguna sebelum buku dapat ditampilkan. Setelah proses dekripsi selesai, tampilan buku akan muncul pada laman.



Gambar 4.1.5 Antarmuka laman ‘Book’ setelah pengguna memiliki akses terhadap buku.



CHAPTER 1

It was a bright cold day in April, and the clocks were striking thirteen. Winston Smith, his chin nuzzled into his breast in an effort to escape the vile wind, slipped quickly through the glass doors of Victory Mansions, though not quickly enough to prevent a swirl of gritty dust from entering along with him.

The hallway smelt of boiled cabbage and old rag mats. At one end of it a coloured poster, too large for indoor display, had been tacked to the wall. It depicted simply an enormous face, more than a metre wide: the face of a man of about forty-five, with a heavy black moustache and ruggedly handsome features. Winston made for the stairs. It was no use trying the lift. Even at the best of times it was seldom working, and at present the electric current was cut off during daylight hours. It was part of the economy drive in preparation for Hate Week. The flat was seven flights up, and Winston, who was thirty-nine and had a varicose ulcer above his right ankle, went slowly, resting several times on the way. On each landing, opposite the lift-shaft, the poster with the enormous face gazed from the wall. It was one of those pictures which are so contrived that the eyes follow you about when you move. BIG BROTHER IS WATCHING YOU, the caption beneath it ran.

Inside the flat a fruity voice was reading out a list of fig-

FREE EBOOKS AT PLANET EBOOK.COM 3

Gambar 4.1.5 Antarmuka membaca buku setelah melalui proses dekripsi.

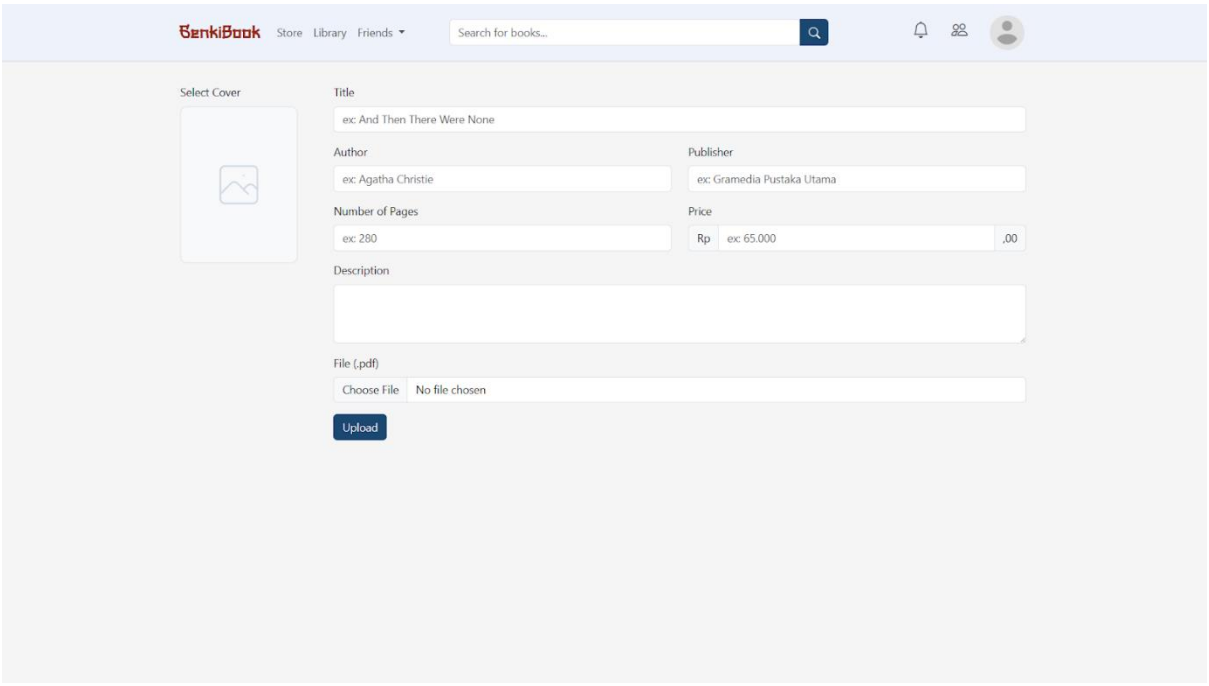
```
$chunk_files                                                                    =
glob("encrypted_ebooks/{$nama}/{$konten}/encrypted_chunk_{$konten}_*.enc");

$chunk_count = count($chunk_files);
if ($chunk_count == 0) {
    die("No encrypted chunks found.");
}

$encrypted_chunks = [];
for ($i = 0; $i < $chunk_count; $i++) {

$encrypted_chunk                                                                =
file_get_contents("encrypted_ebooks/{$nama}/{$konten}/encrypted_chunk_{$konten}_$i.
enc");

  if ($encrypted_chunk === false) {
      die("Failed to read chunk file.");
  }
  $encrypted_chunks[] = $encrypted_chunk;
}

//Proses dekripsi blok dengan kunci privat pengguna
$decrypted_chunks = [];
foreach ($encrypted_chunks as $index => $encrypted_chunk) {
    $decrypted_chunk = null;
    $success                                                                    =
```

```
openssl_private_decrypt($encrypted_chunk,$decrypted_chunk,$private_key);
    if ($success) {
        $decrypted_chunks[] = $decrypted_chunk;
    } else {
        $error_message = openssl_error_string();
        die("Decryption failed for chunk $index: $error_message");
    }
}
```

Gambar 4.1.5 Kode program proses dekripsi pada saat akan membaca buku.

4.1.6 Mengunggah Buku

Proses mengunggah buku hanya melibatkan pengguna yang memiliki *role* sebagai admin. Pengguna admin dapat mengunggah buku melalui laman 'Upload', yang dapat diakses pada *navbar* dengan mengklik gambar profil. Pada laman 'Upload', terdapat *form* untuk mengisi informasi buku yang akan diunggah, yaitu judul, sampul, nama penulis, nama penerbit, jumlah halaman, harga, deskripsi, dan *file* buku.



Gambar 4.1.6 Antarmuka laman 'Upload'.

4.2 Waktu Enkripsi dan Dekripsi

Tabel 4.2 Perbandingan waktu enkripsi dan dekripsi dari lima judul buku

No.	Judul	Ukuran *file*	Waktu enkripsi (detik)	Waktu dekripsi (detik)
1.	*1984*	1,311 KB	19	19
2.	*Animal Farm*	149 KB	2	3
3.	*The Little Prince*	2,111 KB	33	47
4.	*Sherlock*	337 KB	4	5
5.	*Hamlet*	682 KB	12	10

Hasil tabel di atas menunjukkan bahwa proses enkripsi dan dekripsi menggunakan algoritma asimetris saja kurang efisien dikarenakan memakan waktu yang lama, terlebih jika *file e-book* berukuran besar. Proses yang lama dapat menyebabkan terganggunya *user experience* untuk pengguna dengan spesifikasi sistem yang kurang memadai. Hal ini disebabkan oleh *file e-book* harus dipecah terlebih dahulu menjadi blok-blok kecil berukuran 256 bit sebelum melalui proses enkripsi, serta menggabungkan kembali blok-blok tersebut saat melalui proses dekripsi. Jumlah blok bervariasi, tergantung pada ukuran *file*.

4.3 Pengujian Sistem Menggunakan Metode *Black Box*

Pengujian dengan metode *black box* bertujuan untuk memastikan seluruh alur pada sistem dapat berjalan dengan semestinya sesuai dengan kebutuhan fungsional yang sebelumnya telah didefinisikan. Pada penelitian ini, penulis melakukan *black box testing* dengan menyiapkan daftar alur pengujian sistem dan menguji apakah sistem sudah berjalan dengan semestinya atau tidak (Fahrezi et al., 2022).

Tabel 4.3 Hasil pengujian sistem menggunakan metode black box.

Alur pengujian sistem	Input	Output harapan	Status
Sign up dengan isi *form* valid.	Mengisi *form* dan mengklik tombol 'sign up'	Mengalihkan ke laman 'Sign in'	Berhasil
Sign up dengan *form* kosong	Tidak mengisi *form* dan mengklik tombol 'sign up'	Pesan untuk mengisi *form* yang wajib diisi	Berhasil
Sign in dengan isi *form* valid.	Mengisi *form* dan mengklik tombol 'sign in'	Mengalihkan ke laman 'Store'	Berhasil
Sign in dengan email atau password yang salah.	Mengisi *form* dan mengklik tombol 'sign in'	Pesan error "Email atau password salah"	Berhasil
Memilih salah satu buku	Mengklik gambar buku pada laman 'Store'	Mengalihkan ke laman 'Book'	Berhasil
Pembelian buku setelah *sign in*	Mengklik tombol pembelian	Pesan "Transaksi berhasil"	Berhasil
SPembelian buku tanpa *sign in*	Mengklik tombol pembelian	Mengalihkan ke laman 'Sign in'	Berhasil
Membuka laman 'Library' setelah *sign in*	Mengklik 'Library' pada *navbar*	Mengalihkan ke laman 'Library'	Berhasil
Membuka laman 'Library' tanpa *sign in*	Mengklik 'Library' pada *navbar*	Mengalihkan ke laman 'Sign in'	Berhasil
Menambah pengguna lain sebagai teman	Mengklik tombol 'add' pada laman 'Profile'	Pesan 'Friend request sent!"	Berhasil
Menambah pengguna lain sebagai teman tanpa *sign in*	Mengklik tombol 'add' pada laman 'Profile'	Mengalihkan ke laman 'Sign in'	Berhasil
Menambah pengguna lain sebagai teman saat sudah berteman	Mengklik tombol 'add' pada laman 'Profile'	Pesan 'You are already friends with this user'	Berhasil
Menambah pengguna lain	Mengklik		Berhasil

sebagai teman saat sudah mengirim permintaan yang sama	tombol ‘add’ pada laman ‘Profile’	Pesan ‘Friend request already sent’	
Menerima permintaan pertemanan	Mengklik tombol ‘Accept'	Menambahkan teman baru dan mengalihkan ke laman ‘Friends’	Berhasil
Menolak permintaan pertemanan	Mengklik tombol ‘Decline’	Menolak permintaan dan melakukan *refresh* laman	Berhasil
Melakukan permintaan buku	Mengklik tombol ‘request’	Menampilkan *modal* berisi *form*	Berhasil
Mengisi *form* permintaan buku	Pilih teman, isi *form* pesan, dan mengklik tombol ‘request	Pesan ‘Request sent!’	Berhasil
Mengisi *form* permintaan buku tanpa mengisi pesan	Pilih teman dan mengklik tombol ‘request	Pesan untuk mengisi *form* yang wajib diisi	Berhasil
Menerima permintaan buku	Mengklik tombol ‘Accept'	Pesan ‘Book sent succesfully!’	Berhasil
Menolak permintaan buku	Mengklik tombol ‘Decline’	Pesan ‘Request declined’	Berhasil
Membaca buku	Mengklik tombol ‘read now’	Menampilkan isi buku	Berhasil
Mengunggah buku	Mengisi *form* data buku dan mengklik ‘upload’	Mengalihkan ke laman ‘Store’ dan menampilkan buku yang baru diunggah	Berhasil
Mengunggah buku tanpa mengisi *form* lengkap	Mengisi *form* data buku dan mengklik ‘upload’	Pesan untuk mengisi *form* yang wajib diisi	Berhasil
Keluar dari akun	Mengklik tombol ‘sign	Mengalihkan ke laman	Berhasil

	out’	‘Store’ tanpa akun terdaftar	

BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil dari pengembangan sistem distribusi *e-book* berbasis kriptografi asimetris, penulis memperoleh kesimpulan sebagai berikut:

a. Seluruh fitur sistem, hingga proses enkripsi dan dekripsi *file e-book* menggunakan kriptografi jenis asimetris RSA, dapat berjalan dengan baik sesuai harapan.
b. Penerapan algoritma asimetris RSA kurang efisien jika digunakan pada *file e-book*. Hal ini disebabkan oleh *file e-book* yang tergolong besar untuk menerapkan algoritma RSA. Algoritma ini sangat bergantung pada spesifikasi sistem dan ukuran *file* karena membutuhkan daya komputasi yang tinggi. Semakin tinggi spesifikasi sistem, maka waktu yang diperlukan dalam proses enkripsi dan dekripsi semakin sedikit. Hal ini dapat menyebabkan terganggunya *user experience* untuk pengguna dengan spesifikasi sistem yang kurang memadai jika ingin membaca *e-book* dengan ukuran *file* yang cukup besar.

5.2 Saran

Berdasarkan hasil dari pengembangan sistem distribusi *e-book* berbasis kriptografi asimetris, saran yang dapat diberikan untuk penelitian selanjutnya adalah:

a. Melakukan optimasi pada sistem dengan menggunakan pendekatan *hybrid* dalam proses enkripsi dan dekripsi, yaitu menggabungkan algoritma asimetris dengan algoritma simetris. Sebagai contoh, *e-book* melalui proses enkripsi menggunakan algoritma simetris AES, kemudian kunci AES tersebut dienkripsi ulang menggunakan algoritma asimetris RSA. Dengan menggunakan pendekatan ini, waktu yang dibutuhkan dalam proses enkripsi dan dekripsi akan menjadi lebih sedikit. Selain itu, sistem keamanan juga akan meningkat dikarenakan pendekatan ini menggunakan dua jenis kriptografi berbeda.
b. Penyimpanan kunci privat diharapkan dapat lebih baik. Kunci privat pada sistem masih disimpan di dalam basis data, yang dapat menyebabkan resiko terhadap keamanan seperti kebocoran data dan penyalahgunaan oleh pihak tidak bertanggungjawab. Alternatif yang lebih aman adalah menyimpan kunci privat di perangkat keras terpisah, di direktori sistem yang aman, dan melakukan enkripsi ulang. Penerapan algoritma dan

penyimpanan kunci yang baik akan berdampak pada peningkatan keamanan sistem, sehingga upaya untuk melindungi hak cipta akan terlaksana dengan lebih baik.

c. Mengaplikasikan proses transaksi penjualan buku. Pada sistem ini, belum diterapkan proses transaksi penjualan secara khusus, seperti fitur khusus yang mendukung pemilihan opsi pembayaran. Hal ini menunjukkan bahwa sistem masih membutuhkan pengembangan lebih lanjut agar proses transaksi menjadi lebih optimal.

DAFTAR PUSTAKA

Aldisa, R., & Abdullah, M. (2022). Penerapan Agile Development Methodology dalam Sistem Penjualan Buku dengan Fitur Kategori dan Pencarian. *Building of Informatics, Technology and Science (BITS)*, 3(4), 547-553. https://doi.org/10.47065/bits.v3i4.1434

Amin, M. M. (2017). IMPLEMENTASI KRIPTOGRAFI KLASIK PADA KOMUNIKASI BERBASIS TEKS. *Pseudocode*, *3*(2), 129–136. https://doi.org/10.33369/pseudocode.3.2.129-136

Basri. (2016). Kriptografi Simetris dan Asimetris dalam Perspektif Keamanan Data dan Kompleksitas Komputasi. *Jurnal Ilmiah Ilmu Komputer*, 2(2), 17–23. Retrieved from http://ejournal.fikom-unasman.ac.id

Dairi, M. S., Asih, M. S., & Khairunnisa (2023). Implementasi Algoritma Kriptografi RSA Dalam Aplikasi Sistem Informasi Perpustakaan. *Jurnal Ilmu Komputer dan Sistem Informasi*, 2(1), 214-223.

Diarse, N. N., & Bendi, R. (2016). Penerapan Algoritma RSA pada Sistem Kriptografi File Audio MP3. *Jurnal Hoaq Teknologi Informasi*, 7(2), 567-575.

Fachri, B., & Surbakti, R. W. (2021). Perancangan Sistem Dan Desain Undangan Digital Menggunakan Metode Waterfall Berbasis Website (Studi Kasus: Asco Jaya). *Journal Of Science And Social Research*, 4(3), 263-267.

Fahrezi, A. ., Noer Salam, F. ., Mahardhika Ibrahim, G. ., Rahman Syaiful, R. ., & Saifudin, A. . (2022). Pengujian Black Box Testing pada Aplikasi Inventori Barang Berbasis Web di PT. AINO Indonesia. *LOGIC : Jurnal Ilmu Komputer Dan Pendidikan*, 1(1), 1–5. Retrieved from https://www.journal.mediapublikasi.id/index.php/logic/article/view/1262

Guswandi, C. P., Romadona, H. G., Ariani, M., & Disemadi, H. S. (2021). Pengaruh Revolusi Industri 4.0 Terhadap Perlindungan Hukum Hak Cipta Di Indonesia. In *CoMBInES-Conference on Management, Business, Innovation, Education and Social Sciences* (Vol. 1, No. 1, pp. 277-283).

Hafsari, R., Aribe, E., & Maulana, N. (2023). Perancangan Sistem Informasi Manajemen Inventori Dan Penjualan Pada Perusahaan PT. INHUTANI V. *PROSISKO: Jurnal Pengembangan Riset dan Observasi Sistem Komputer*, 10(2), 109-116.

Hermiati, R., Asnawati, A., & Kanedi, I. (2021). PEMBUATAN E-COMMERCE PADA RAJA KOMPUTER MENGGUNAKAN BAHASA PEMROGRAMAN PHP DAN DATABASE MYSQL. *JURNAL MEDIA INFOTAMA*, 17(1). https://doi.org/10.37676/jmi.v17i1.1317

Kharisma, S., & Nasution, M. I. P. (2023). Peran Database Dalam Sistem Informasi Manajemen. *Jurnal Akuntansi Keuangan Dan Bisnis*, 1(2), 54–58. Retrieved from https://jurnal.ittc.web.id/index.php/jakbs/article/view/36

Kozlowski, M. (2018). eBook piracy is on the rise in 2018. *Good E-Reader*. Retrieved from https://goodereader.com/blog/e- book-news/ebook-piracy-is- on-the-rise-in-2018

Maharani, D., Helmiah, F., & Rahmadani, N. (2021). Penyuluhan Manfaat Menggunakan Internet dan Website Pada Masa Pandemi Covid-19. *Abdiformatika: Jurnal Pengabdian Masyarakat Informatika*, 1(1), 1–7. https://doi.org/10.25008/abdiformatika.v1i1.130

Muhamad Wahyu Saputra, Anjeli Sapitri, & Mesy Aniza Putri. (2023). PENERAPAN KRIPTOSISTEM HYBRID UNTUK MENGENKRIPSI PESAN MENGGUNAKAN ALGORITMA RSA CIPHER. *JOCITIS-Journal Science Infomatica and Robotics*, 1(1), 10–21. Retrieved from https://jurnal.ittc.web.id/index.php/jct/article/view/29

Nova, C., Sanjaya, G.I., Ahmad, Z., Firjatullah, D.A., Mufid, A.A., (2021). Implementasi Cryptography Menggunakan Algoritma Caesar Cipher.

Pertama, D., Sulistiyani, H., & Rahmanto, Y. (2023). Pengembangan E-Commerce Untuk Penjualan Buku Bekas (Studi Kasus: Ramayana Pasar Bawah) Berbasis Mobile. TELEFORTECH: *Journal of Telematics and Information Technology*, 4(1), 16-23.

Purnama, B. E., Permana, M. E. (2021). Implementasi Buku Online Sebagai Solusi Digitalisasi Media. *Indonesian Journal of Networking and Security (IJNS)*, *10*(4).

Putra, W. A., Fitri, I., & Hidayatullah, D. (2022). Implementasi Waterfall dan Agile dalam Perancangan E-Commerce Alat Musik Berbasis Website. *Jurnal JTIK (Jurnal Teknologi Informasi dan Komunikasi)*, 6(1), 56-62.

Putri, G. G., Setyorini, W., & Rahayani, R. D. (2018). Analisis Kriptografi Simetris Aes Dan Kriptografi Asimetris Rsa Pada Enkripsi Citra Digital. *ETHOS: Jurnal Penelitian dan Pengabdian kepada Masyarakat*, 6(2), 197-207.

Ristic, I. (2013). Openssl cookbook: A guide to the most frequently used openssl features and commands. *Feisty Duck*.

Rizki, M., & Farida Ariyani, P. (2021). PENERAPAN KRIPTOGRAFI DENGAN MENGGUNAKAN ALGORITMA RSA UNTUK PENGAMANAN DATA BERBASIS DESKTOP PADA PT TRIAS MITRA JAYA MANUNGGAL. *SKANIKA: Sistem Komputer Dan Teknik Informatika*, 4(2), 77-82. https://doi.org/10.36080/skanika.v4i2.1991.

Ruddamayanti, R. (2019). Pemanfaatan Buku Digital dalam Meningkatkan Minat Baca. In *Prosiding Seminar Nasional Program Pascasarjana Universitas PGRI Palembang.*

Sari, R. P., & Istikoma, I. (2018). Analisis dan Perancangan Sistem Informasi Rapat Online FMIPA UNTAN menggunakan UML. *Prosiding SISFOTEK*, *2*(1), 154-165.

Sasvito, N. (2024). Pengaruh Persepsi Kemudahan dan Persepsi Manfaat terhadap Minat Pelaku Bisnis Digital Membuat Landing Page Menggunakan Content Management System. *Multidiscience : Journal of Multidisciplinary Science*, 1(2), 135–142. https://doi.org/10.59631/multidiscience.v1i2.252

Setyorini, S., & Pranoto, E. (2021). Analisis dan pengembangan sistem penjualan dan sewa buku digital (ebook) menggunakan metode unified modeling language (UML). *Jurnal Ilmiah Teknologi dan Rekayasa*, *26*(2), 139-153.

Simargolang, M. Y. (2017). Implementasi Kriptografi Rsa Dengan Php. *(JurTI) Jurnal Teknologi Informasi*, 1(1), 1-10.

Surbakti, T. B., Fauzi, A., & Khair, H. (2023). Hybrid Sistem Algoritma Rivest Shamir Adleman (RSA) dan Algoritma Blum Blum Shub (BBS) dalam Mengamankan File Database E-Absensi. *Indonesian Journal of Education And Computer Science*, 1(3), 89–97. https://doi.org/10.60076/indotech.v1i2.59

Tiawati, S., & Pura, M. H. (2021). Analisa Hukum Perlindungan Hak Cipta Terhadap Pembelian Buku Elektronik Secara Ilegal. Ajudikasi : *Jurnal Ilmu Hukum*, 4(2), 169–180. https://doi.org/10.30656/ajudikasi.v4i2.

Uyun, Q. (2023). NORMALISASI PEMBAJAKAN BUKU DI ERA TEKNOLOGI DIGITAL. *Mu'amalah: Jurnal Hukum Ekonomi Syariah*, *2*(2), 255-262. https://doi.org/10.32332/muamalah.v2i2.7881

Viega, J., Messier, M., & Chandra, P. (2002). *Network security with openSSL: cryptography for secure communications*. " O'Reilly Media, Inc.".

Zulfikar, M. I., Abdillah, G., & Komarudin, A. (2019). Kriptografi untuk Keamanan Pengiriman Email Menggunakan Blowfish dan Rivest Shamir Adleman (RSA). In *Seminar Nasional Aplikasi Teknologi Informasi (SNATi)*.

LAMPIRAN

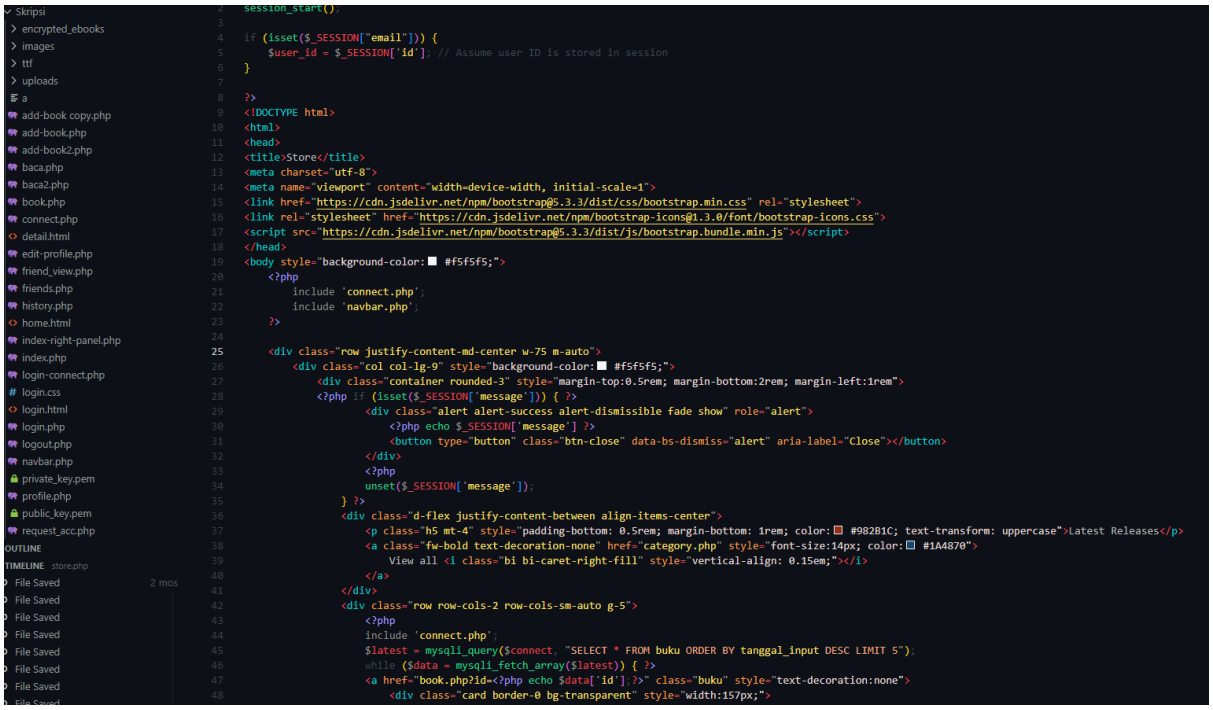
Filters

Containing the word:

	Table	Action						Rows	Type	Collation	Size
☐	buku	Browse	Structure	Search	Insert	Empty	Drop	24	InnoDB	utf8mb4_general_ci	64.0 KiB
☐	request	Browse	Structure	Search	Insert	Empty	Drop	5	InnoDB	utf8mb4_general_ci	48.0 KiB
☐	request_buku	Browse	Structure	Search	Insert	Empty	Drop	2	InnoDB	utf8mb4_general_ci	64.0 KiB
☐	teman	Browse	Structure	Search	Insert	Empty	Drop	4	InnoDB	utf8mb4_general_ci	48.0 KiB
☐	transaksi	Browse	Structure	Search	Insert	Empty	Drop	18	InnoDB	utf8mb4_general_ci	48.0 KiB
☐	user	Browse	Structure	Search	Insert	Empty	Drop	12	InnoDB	utf8mb4_general_ci	48.0 KiB
	6 tables	Sum						65	InnoDB	utf8mb4_general_ci	320.0 KiB

Check all With selected:

LAMPIRAN A



LAMPIRAN B