TECHNOVATAR Jurnal Teknologi, Industri dan Informasi
Vol. 2, No. 4, Bulan Tahun, pp. 111 – 128
Open Access: https://journal.awatarapublisher.com/index.php/technovatar
ISSN: 3031-8874, **DOI**: 10.61434/technovatar.v2i4.247

PENERAPAN KRIPTOGRAFI RSA UNTUK MENGATASI PEMALSUAN DALAM INDUSTRI PENERBITAN BUKU

Ahmad Ngiliyun[1], Rosidin Rosidin[2], Deni Nugraha[3]
[1,2,3] Teknik Informatika, Fakultas Ilmu Komputer, Universitas Nahdlatul Ulama Cirebon, Cirebon, Indonesia

e-mail: ahmadngiliyun@gmail.com[1], rosidin@unucirebon.ac.id[2], deni.nugraha@unucirebon.ac.id[3]

INFO ARTIKEL
Sejarah Artikel:
Diterima, 14 September 2024
Direvisi, 15 September 2024
Disetujui, 20 September 2024

KEYWORDS
Book Publishing,
Information System,
RSA Cryptography,
Data Security,
Copyright

ABSTRACT
This study aims to develop a book publishing information system that can assist lecturers in publishing their academic works more efficiently and securely. The system implements the Rivest-Shamir-Adleman (RSA) cryptographic algorithm to protect book data from unauthorized access, as well as to prevent counterfeiting and copyright infringement. With the encryption applied, only authorized parties can access sensitive information. The implementation of this system has proven to increase efficiency in the book publishing process, reduce administrative obstacles, and enhance authors' confidence in the security of the system. It is expected that this system will boost academic productivity and maintain the integrity of lecturers' intellectual works.

KATA KUNCI
Penerbitan Buku,
Sistem Informasi,
Kriptografi RSA,
Keamanan Data,
Hak Cipta

ABSTRAK
Penelitian ini bertujuan untuk mengembangkan sistem informasi penerbitan buku yang dapat membantu dosen dalam menerbitkan karya ilmiah mereka dengan lebih efisien dan aman. Sistem ini menerapkan algoritma kriptografi Rivest-Shamir-Adleman (RSA) untuk melindungi data buku dari akses yang tidak sah serta mencegah pemalsuan dan pelanggaran hak cipta. Dengan enkripsi yang diterapkan, hanya pihak yang memiliki otoritas yang dapat mengakses informasi sensitif. Implementasi sistem ini terbukti meningkatkan efisiensi dalam proses penerbitan buku, mengurangi hambatan administratif, dan meningkatkan kepercayaan penulis terhadap keamanan sistem. Diharapkan, sistem ini dapat mendorong produktivitas akademik dan menjaga integritas karya intelektual para dosen.

CORRESPONDING AUTHOR
Ahmad Ngiliyun
Universitas Nahdlatul Ulama Cirebon
Cirebon
ahmadngiliyun@gmail.com

PENDAHULUAN

Dalam beberapa tahun terakhir, industri penerbitan buku menghadapi berbagai tantangan terkait pemalsuan dan pelanggaran hak cipta. Pemalsuan buku tidak hanya merugikan penerbit dan penulis dengan mengurangi pendapatan mereka, tetapi juga berdampak negatif pada konsumen yang tidak menyadari bahwa mereka membeli produk yang tidak asli [1]. Selain itu, pemalsuan buku dapat mengurangi kualitas karya yang beredar di pasaran dan merusak reputasi penerbit. Pelanggaran hak cipta, seperti pembajakan dan penggunaan karya tanpa izin, juga merusak integritas karya intelektual dan menghambat inovasi [2].

Universitas Nahdlatul Ulama Cirebon sebagai lembaga pendidikan memiliki peran penting dalam melindungi karya intelektual yang dihasilkan oleh komunitas akademiknya. Namun, hingga saat ini, belum tersedia sistem informasi penerbitan buku yang mampu menjamin keamanan hak cipta. Untuk itu, diperlukan pengembangan sistem informasi penerbitan buku dengan keamanan yang memadai guna melindungi hak cipta dan mencegah pemalsuan. Sistem ini dirancang dengan

mengambil contoh dari UPI Press, yang telah menerapkan sistem keamanan serupa dari segi tampilan, fungsional, dan hak akses [3].

Salah satu solusi yang menjanjikan untuk mengatasi masalah ini adalah penerapan teknik kriptografi, seperti Rivest-Shamir-Adleman (RSA), yang dapat melindungi informasi dan mencegah akses yang tidak sah [4]. RSA adalah sistem kriptografi asimetris yang menggunakan sepasang kunci, yaitu kunci publik dan kunci privat, untuk mengenkripsi dan mendekripsi data. Keamanan RSA terletak pada kesulitan faktorisasi bilangan prima yang sangat besar, yang menjadi dasar dari kunci tersebut [5].

Dalam konteks sistem informasi penerbitan buku di Universitas Nahdlatul Ulama Cirebon, kriptografi RSA dapat digunakan untuk mengamankan konten buku dan transmisi data, serta mengautentikasi pihak yang terlibat dalam proses penerbitan. Dengan mengenkripsi konten buku menggunakan RSA, akses terhadap konten tersebut dapat dibatasi hanya untuk pihak yang memiliki kunci yang sesuai, sehingga mencegah pembajakan dan penggunaan ilegal dari karya tersebut [6]. Penerapan ini diharapkan dapat mencegah terjadinya pemalsuan dan pelanggaran hak cipta, serta meningkatkan kepercayaan dan integritas dalam industri penerbitan buku.

Rumusan Masalah

1. Bagaimana cara merancang sistem informasi penerbitan buku menggunakan algoritma RSA?
2. Bagaimana cara mengimplementasikan sistem informasi penerbitan buku menggunakan algoritma RSA?

Tujuan Penelitian

1. Membuat rancangan sistem informasi penerbitan buku menggunakan algoritma RSA.
2. Mengimplementasikan sistem informasi penerbitan buku menggunakan algoritma RSA.

LITERATURE REVIEW

Kriptografi Rivest-Shamir-Adleman (RSA)

Kriptografi Rivest-Shamir-Adleman (RSA) merupakan salah satu algoritma kriptografi asimetris yang digunakan untuk melindungi data sensitif dalam berbagai sistem, termasuk sistem informasi penerbitan buku. Algoritma ini ditemukan oleh Ron Riv Rivestest, Adi Shamir, dan Len Adleman pada tahun 1977, dan didasarkan pada penggunaan kunci publik dan kunci privat untuk enkripsi dan dekripsi data [7].

Proses enkripsi dan dekripsi pada RSA melibatkan bilangan prima dan aritmetika modulo, di mana kunci publik digunakan untuk mengenkripsi data, sementara kunci privat digunakan untuk mendekripsinya. Keamanan algoritma ini sangat bergantung pada kesulitan dalam memfaktorkan bilangan prima yang besar, yang hingga saat ini belum ditemukan metode efisien untuk melakukannya [8].

Besaran-besaran yang digunakan pada algoritma RSA [9]:

1. p dan q bilangan prima (rahasia)
2. r = p . q (tidak rahasia)
3. Φ (r) = (p – 1)(q – 1) (rahasia)
4. PK (kunci enkripsi) (tidak rahasia)
5. SK (kunci dekripsi) (rahasia)
6. X (plainteks) (rahasia)
7. Y (cipherteks) (tidak rahasia)

Gambar 1 Proses Enkripsi dan Dekripsi

Pembangkitan kunci pada algoritma RSA dapat dijelaskan sebagai berikut [4], [6]:

1. Pilih dua bilangan prima secara acak, dimana p dan q tidak sama $(p \neq q)$
2. Hitung N dengan persamaan $N = p.q$
3. Hitung $\Phi(n)$ dengan persamaan $\Phi(n) = (p-1).(q-1)$
4. Pilih bilangan bulat (integer) antara satu dan $\Phi(1 < e < \Phi)$ yang juga merupakan coprime dari Φ
5. Hitung d dengan persamaan $de \equiv 1(mod\ \Phi)$

Hasil dari algoritma ini:
Kunci Publik : pasangan (N,e)
Kunci privat : pasangan (N,d)

Algoritma enkripsi yang digunakan pada algoritma RSA sebagai berikut [10]:

1. Susun plaintext menjadi blok-blok P1,P2, ..., Pn
2. Hitung ciphertext Ci dengan rumus $C_i = P_i^e\ mod\ N$

Algoritma dekripsi yang digunakan pada algoritma RSA sebagai berikut [7], [11]:
Gunakan kunci privat untuk pangkat nilai dari ciphertext
Carilah nilai P dengan rumus $P_i = C_i^d\ mod\ N$

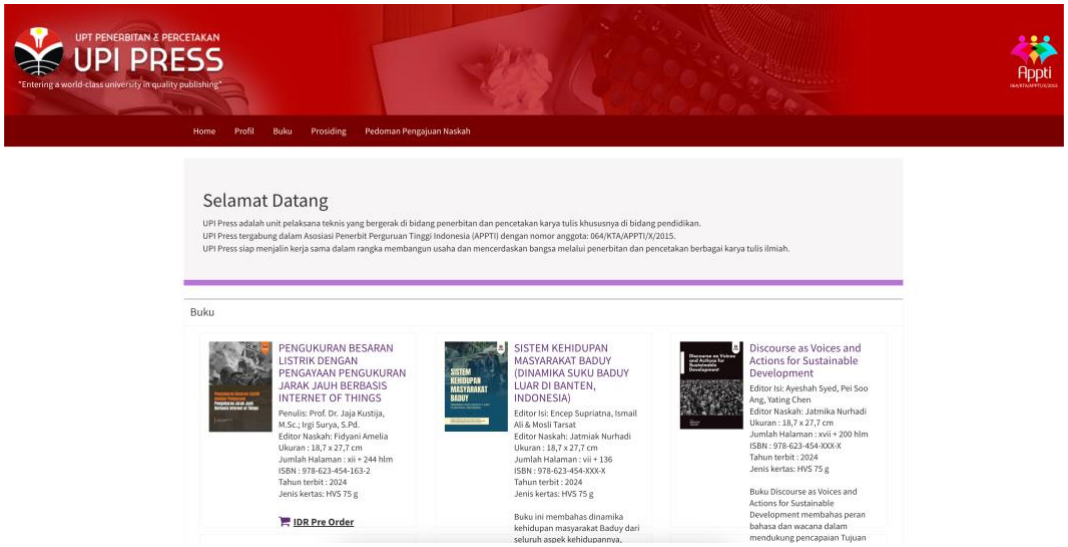
Pengertian Kriptografi

Menurut penelitian Wiliam [11] (Apdilah & Swanda, 2018), kriptografi berasal dari bahasa Yunani yang berarti 'menulis secara rahasia.' Kriptografi bertujuan untuk menciptakan komunikasi yang aman, sehingga meskipun ada pihak ketiga yang berusaha mencuri informasi, data tersebut tetap terlindungi dan tidak dapat dibaca. Algoritma RSA termasuk dalam kategori kriptografi asimetris, yang memanfaatkan dua kunci yang berbeda untuk proses enkripsi dan dekripsi. Algoritma ini dikenal karena tingkat keamanannya yang tinggi, karena menggunakan perhitungan bilangan prima yang sangat besar dan kompleks [12].

Penerapan RSA pada Sistem Informasi Penerbitan Buku

Dalam penerapan pada sistem informasi penerbitan buku, algoritma RSA dapat digunakan untuk mengamankan berbagai jenis data, seperti informasi hak cipta, data pembayaran, data identitas pengguna, dan informasi strategis penerbitan. Enkripsi data ini bertujuan untuk mencegah akses yang tidak sah dan melindungi informasi sensitif dari pihak yang tidak berwenang [11]. Sebagai contoh, informasi hak cipta mengenai buku, termasuk detail pemegang hak cipta dan tanggal penerbitan, dapat dienkripsi untuk memastikan hanya pihak berwenang yang dapat mengaksesnya.

Metode Pengembangan Sistem Informasi Penerbitan Buku



Gambar 2 Sistem UPI Press

Selain itu, sistem informasi penerbitan buku di Universitas Nahdlatul Ulama Cirebon mengadopsi pendekatan yang serupa dengan sistem yang diterapkan oleh UPI Press, dengan fokus pada tampilan, fungsionalitas, dan hak akses untuk memastikan keamanan dan kemudahan penggunaan [3]. Penggunaan metode prototipe dalam pengembangan sistem ini juga memungkinkan pengembang untuk terus mendapatkan umpan balik dari pengguna, sehingga sistem yang dihasilkan dapat lebih sesuai dengan kebutuhan dan ekspektasi pengguna [6].

METODE PENELITIAN

Gambar 3 Ilustrasi *Model Prototype*

Penelitian ini menggunakan metode prototipe dalam pengembangan sistem informasi penerbitan buku. Pendekatan prototipe dipilih untuk memastikan bahwa sistem yang dikembangkan dapat memenuhi kebutuhan pengguna melalui iterasi yang berulang, sehingga sistem dapat disesuaikan berdasarkan umpan balik yang diperoleh selama proses pengembangan. Metode ini memungkinkan pengembang untuk bekerja sama dengan pengguna dalam mengevaluasi prototipe sebelum sistem akhir diimplementasikan sepenuhnya [9].

Berikut tahapan prototype dalam pengembangan sistem [7], [11], [13]:

1. Requirements gathering and analysis

Tahapan awal model prototype dimulai dari analisis kebutuhan. Dalam tahap ini kebutuhan sistem didefinisikan dengan rinci. Dalam prosesnya, klien dan tim developer akan bertemu untuk mendiskusikan detail sistem seperti apa yang dibutuhkan oleh pengunjung.

2. Quick design
   Tahap kedua adalah pembuatan desain sederhana yang akan memberi gambaran singkat tentang sistem yang ingin dibuat. Design baru dapat dibuat jika persyaratan dari user sudah diketahui. Setelah itu, pembuatan design dapat dilakukan berdasarkan requirement gathering dan analisis pada tahap 1.
3. Build prototype
   Setelah desain quick design disetujui oleh user, tahap selanjutnya yaitu pembangunan prototype sebenarnya yang akan dijadikan rujukan tim programmer untuk pembuatan program atau aplikasi.
4. User evaluation
   Setelah prototype dibuat selanjutnya adalah tahap evaluasi oleh pengunjung. Pada tahap ini, sistem yang telah dibuat dalam bentuk prototype dipresentasikan pada klien untuk di evaluasi.
5. Refining prototype
   Tahap refining merupakan tahap perbaikan prototype berdasarkan hasil feedback klien pada tahap 4. Jika pengunjung tidak mempunyai catatan revisi dari prototype yang dibuat, maka tim bisa berlanjut pada tahapan 6 untuk implementasi produk.
6. Implement product and maintenance
   Setelah perbaikan pada tahap 5 disetujui klien, maka selanjutnya adalah tahap implement dan maintenance. Pada fase akhir ini, produk akan segera dibuat oleh para programmer berdasarkan prototype akhir.

Tahap pertama dalam metode ini adalah analisis kebutuhan, di mana fitur-fitur utama sistem dirancang berdasarkan kebutuhan penerbit, penulis, dan pengguna. Selanjutnya, dilakukan perancangan sistem dengan menggunakan diagram use case dan activity diagram untuk memvisualisasikan alur sistem dan fungsionalitasnya. Setelah itu, prototipe dikembangkan dan dievaluasi oleh pengguna untuk mendapatkan umpan balik yang berguna bagi perbaikan sistem.

Dalam implementasi, algoritma Rivest-Shamir-Adleman (RSA) diterapkan untuk mengamankan data sensitif dalam sistem. Algoritma ini digunakan untuk enkripsi dan dekripsi informasi yang berkaitan dengan hak cipta, data penulis, dan transaksi penerbitan. Pada tahap pengujian, sistem diuji untuk memastikan bahwa data yang terenkripsi hanya dapat diakses oleh pihak yang memiliki kunci yang sah, sehingga keamanan data dapat terjamin.

Dengan metode prototipe ini, proses pengembangan sistem informasi penerbitan buku dapat diselesaikan dengan lebih responsif terhadap kebutuhan pengguna, serta mampu memberikan perlindungan hak cipta yang optimal melalui penerapan teknologi kriptografi RSA.

DISKUSI DAN PEMBAHASAN

Implementasi algoritma Rivest-Shamir-Adleman (RSA) pada sistem informasi penerbitan buku di Universitas Nahdlatul Ulama Cirebon bertujuan untuk meningkatkan keamanan data dan mengatasi masalah pemalsuan serta pelanggaran hak cipta. Berdasarkan analisis sistem lama dan sistem baru yang dilakukan, proses penerbitan sebelumnya hanya bergantung pada prosedur manual melalui LPPM, sedangkan sistem baru yang dikembangkan menggunakan teknologi kriptografi RSA untuk menjamin keamanan data yang lebih optimal.

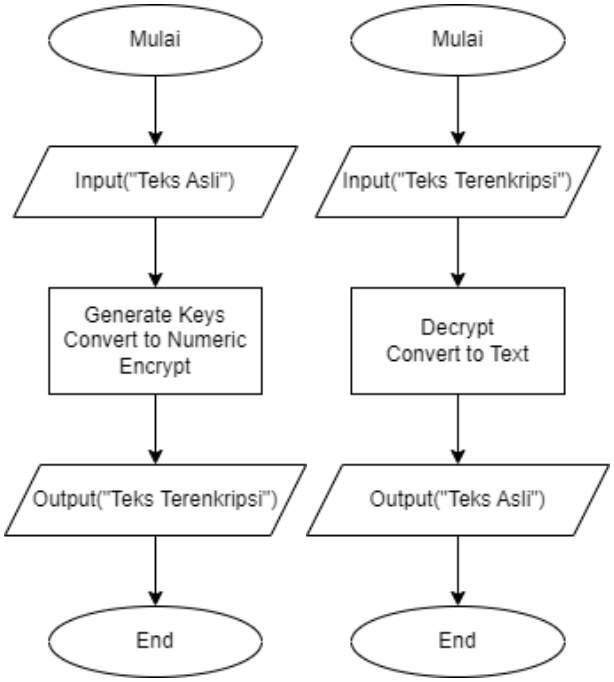
Analisis Kebutuhan Fungsional dan Non-Fungsional

Kebutuhan fungsional dari sistem ini mencakup kemampuan untuk menambahkan, mengubah, dan menghapus detail buku, serta mengunggah berkas dalam format tertentu (seperti gambar dan PDF). Pengunjung hanya diberikan akses untuk melihat dan membaca buku yang telah diterbitkan, sedangkan admin memiliki hak akses yang lebih luas untuk mengelola data penerbitan buku. Kebutuhan non-fungsional mencakup perangkat keras dan perangkat lunak yang digunakan dalam membangun sistem. Kebutuhan ini memastikan bahwa sistem dapat berjalan dengan baik dan memenuhi kriteria kinerja yang diharapkan.

1. Prosedur Penerbitan
    a. Penulis mengisi formulir pengajuan penerbitan buku dan mengirim soft file naskah.
    b. Editor UNU Cirebon Press melakukan penilaian naskah.
    c. Jika naskah tanpa perbaikan, staf bidang administrasi akan menghubungi penulis (pilihan paket penerbitan, formulir tanda terima naskah).
    d. Jika naskah perlu perbaikan, naskah akan dikembalikan kepada penulis untuk diperbaiki.
    e. UNU Cirebon Press mengirim SK Penerbitan kepada penulis.
    f. Pembuatan layout dan design serta diproses untuk dilakukan pencetakan.
    g. Penyerahan buku cetak & Sertifikat.
2. Alur Penerbitan

Gambar 4 Alur Penerbitan UNU Cirebon Press

Penggunaan RSA pada sistem ini melibatkan enkripsi dan dekripsi data penting seperti detail buku, hak cipta, dan informasi pengguna. Implementasi RSA dipilih karena kemampuannya dalam menjaga integritas data dan memberikan perlindungan terhadap akses yang tidak sah, sehingga meningkatkan keamanan dalam proses penerbitan buku.



Gambar 5 Proses Enkripsi dan Dekripsi

Dari analisis sistem lama, maka dirumuskanlah analisis sistem baru dengan membuat sistem informasi penerbitan buku yang ditambahkan pengamanan data menggunakan algoritma RSA. Hak akses pada website ini adalah admin dan pengunjung, adapun analisisnya sebagai berikut:

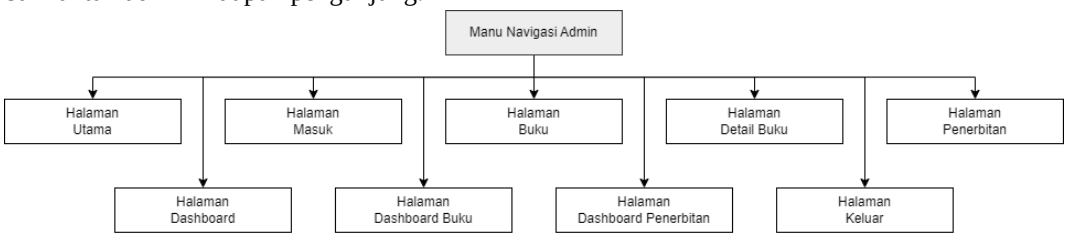
1. Admin mengakses website sistem penerbitan buku
2. Admin mengunjungi halaman masuk
3. Admin login lebih dulu menggunakan *email* dan *password* yang tersedia.
4. Admin membuka halaman *dashboard* dan mengelola data penerbitan buku.
5. Admin akan keluar jika menekan tombol logout, jika tidak admin dapat mengelola data penerbitan buku.
6. Pengunjung mengakses website.
7. Pengunjung melihat-lihat dan membaca buku.

Kebutuhan fungsional sistem baik untuk admin maupun untuk user, sebagai berikut:

1. Sistem dapat menambahkan, mengubah dan menghapus detail buku, seperti: judul, deskripsi, penulis, penerbit, tahun terbit, editor dan ISBN buku.
2. Sistem dapat mengunggah berkas berupa cover buku berupa gambar dan file buku berformat PDF.
3. Sistem dapat menampilkan buku-buku yang sudah ditambahkan dan yang telah diubah serta tidak menampilkan buku-buku yang sudah dihapus.
4. Sistem dapat mengamankan data-data dari detail buku yang akan diterbitkan.
5. Admin dapat menambahkan, mengubah, menghapus, mengunggah berkas cover dan file buku.
6. Pengunjung hanya dapat melihat dan membaca buku yang sudah diterbitkan.

Dalam sistem lama, proses penerbitan melibatkan berbagai tahapan manual, mulai dari pengajuan naskah hingga pencetakan buku. Proses ini memiliki kelemahan, terutama dalam hal pengamanan data dan efisiensi prosedur. Oleh karena itu, sistem baru dirancang untuk mengatasi

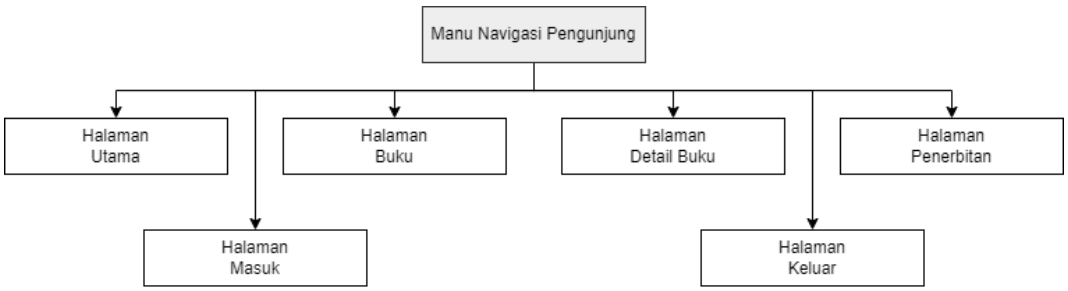
kelemahan tersebut dengan menyediakan fitur keamanan tambahan, yaitu enkripsi menggunakan RSA, serta peningkatan fungsionalitas melalui sistem informasi berbasis web. Fitur ini tidak hanya memastikan keamanan data, tetapi juga menyediakan aksesibilitas yang lebih baik bagi pengguna, baik untuk admin maupun pengunjung.



Gambar 6 Menu Navigasi Admin

Tabel 1 Penjelasan Menu Navigasi Admin

Halaman	Keterangan
Utama	Menampilkan semua buku yang telah diterbitkan
Masuk	Menyediakan form login dengan email dan password yang akan tertuju pada halaman dashboard
Buku	Menampilkan semua buku yang telah diterbitkan
Detail Buku	Menampilkan detail buku yang telah dipilih
Penerbitan	Menampilkan prosedur dan gambar alur penerbitan
Dashboard	Menampilkan jumlah buku yang telah diterbitkan
Dashboard Buku	Menampilkan semua buku yang telah diterbitkan dan dapat menambahkan, mengubah, menghapus, mengunggah cover serta file buku
Dashboard Penerbitan	Menampilkan prosedur dan gambar alur penerbitan dan dapat mengubah serta mengunggah gambar alur penerbitan
Keluar	Menghapus sesi admin dan kembali ke halamana utama



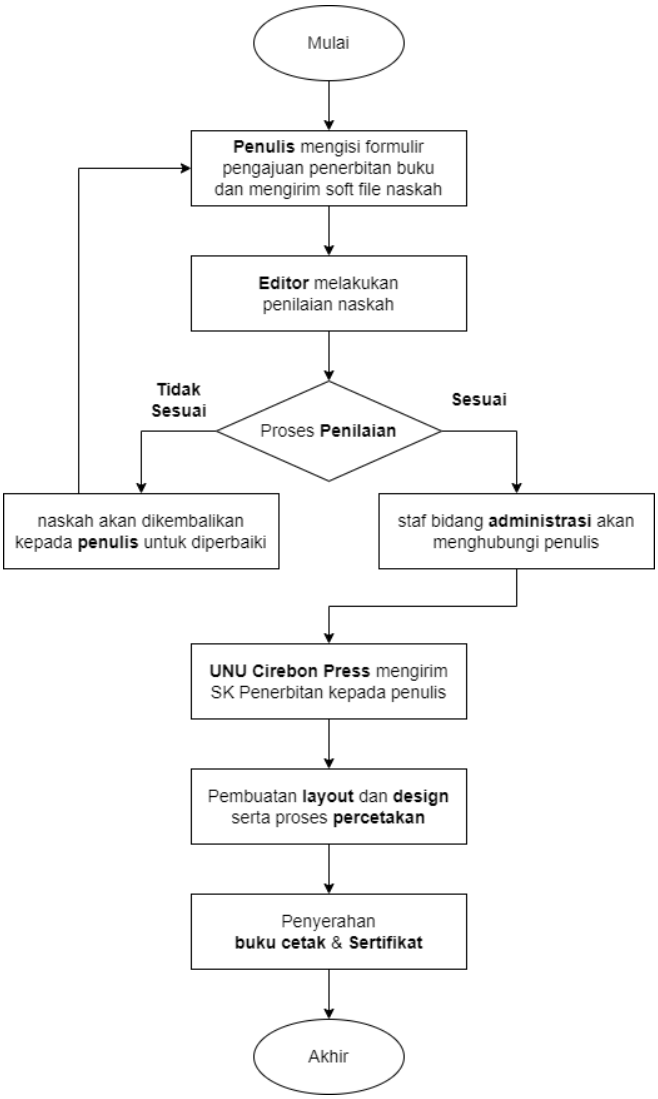
Gambar 7 Menu Navigasi Pengunjung

Tabel 2 Penjelasan Menu Navigasi Pengunjung

Halaman	Keterangan
Utama	Menampilkan semua buku yang telah diterbitkan
Masuk	Menyediakan form login dengan email dan password yang akan tertuju pada halaman utama
Buku	Menampilkan semua buku yang telah diterbitkan
Detail Buku	Menampilkan detail buku yang telah dipilih
Penerbitan	Menampilkan prosedur dan gambar alur penerbitan

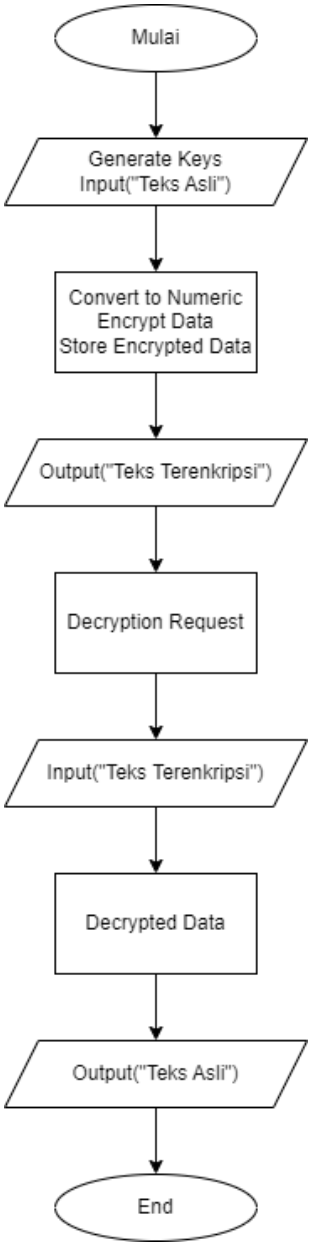
Keluar	Menghapus sesi pengunjung dan kembali ke halamana utama

Implementasi Sistem



Gambar 8 Flowchart Proses Penerbitan Buku

Implementasi sistem baru dilakukan dengan mengembangkan fitur-fitur yang dapat memenuhi kebutuhan fungsional dan non-fungsional pengguna. Untuk pengunjung, sistem menyediakan halaman utama yang menampilkan daftar buku yang tersedia, halaman masuk untuk pengguna yang telah terdaftar, serta halaman detail buku yang memungkinkan pengunjung membaca buku jika lisensinya bersifat gratis. Admin memiliki akses yang lebih luas, termasuk kemampuan untuk mengelola buku, mengubah prosedur penerbitan, dan mengunggah berbagai berkas terkait penerbitan. Pada Gambar 10 hingga Gambar 19, ditampilkan contoh tampilan halaman-halaman untuk pengunjung dan admin, yang memberikan gambaran visual tentang interaksi sistem dan bagaimana fitur-fitur tersebut diimplementasikan.

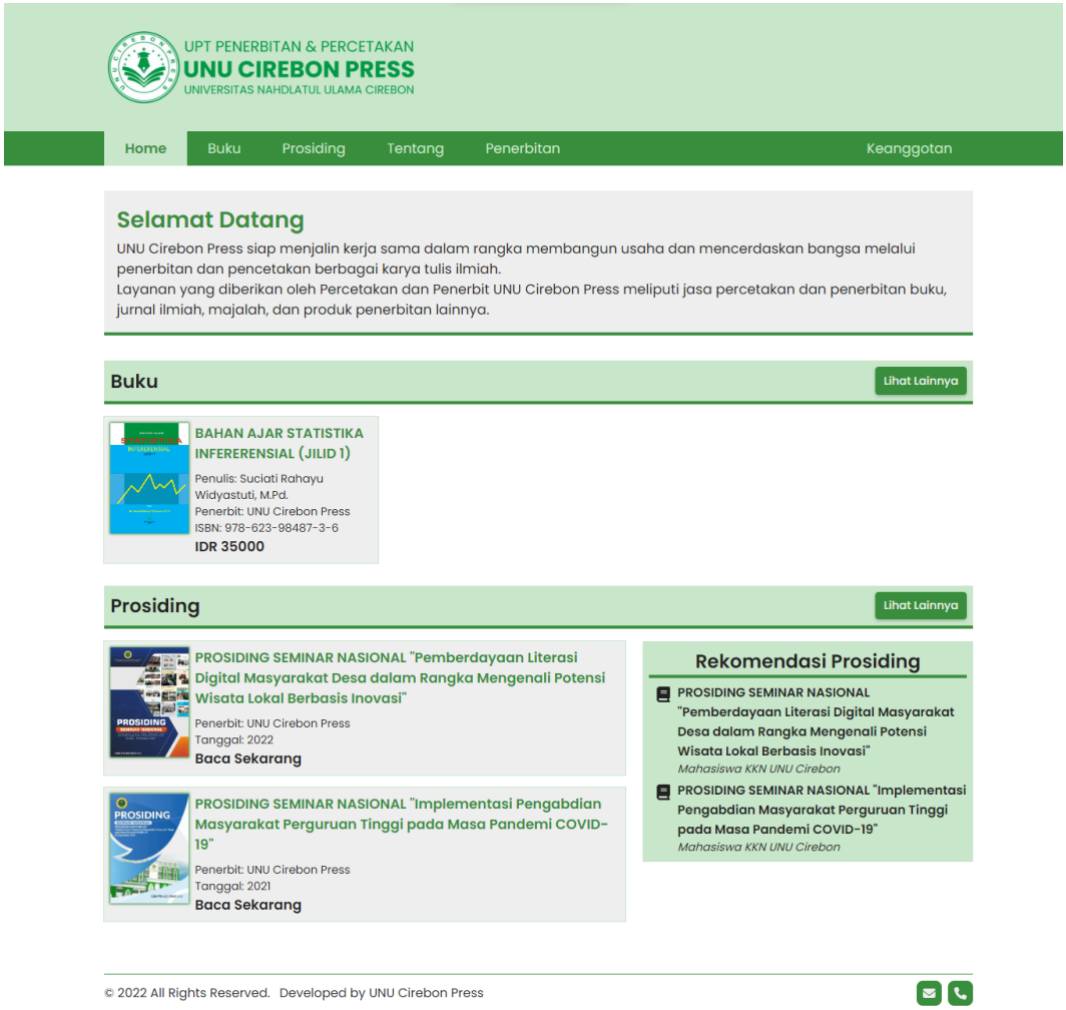


Gambar 9 Proses Implementasi Keamanan pada SI Penerbitan Buku

Flowchart Proses Implementasi Keamanan dengan Algoritma RSA pada Sistem Informasi Penerbitan Buku:

1. *Start*: Mulai proses implementasi keamanan dengan algoritma RSA pada sistem informasi penerbitan buku.
2. *Generate Keys*: Buat sepasang kunci RSA, yaitu kunci publik dan kunci privat.
3. *Input Data*: Masukkan data yang ingin dienkripsi, seperti konten buku, informasi hak cipta, data pembayaran, dan data identitas pengguna.
4. *Encrypt Data*: Lakukan proses enkripsi pada data menggunakan kunci publik.
5. *Encrypted Data*: Hasil enkripsi berupa data terenkripsi.
6. *Store Encrypted Data*: Simpan data terenkripsi ke dalam database atau sistem penyimpanan yang aman.

7. *Output Encrypted Data*: Berikan data terenkripsi kepada pihak yang berhak untuk mengaksesnya, misalnya editor, penulis, atau distributor.
8. *Decryption Request*: Terima permintaan dekripsi data dari pihak yang berhak.
9. *Decrypt Data*: Lakukan proses dekripsi pada data terenkripsi menggunakan kunci privat.
10. *Decrypted Data*: Hasil dekripsi berupa data asli.
11. *End*: Selesaikan proses implementasi keamanan dengan algoritma RSA pada SI penerbitan buku.



Gambar 10 Halaman Utama

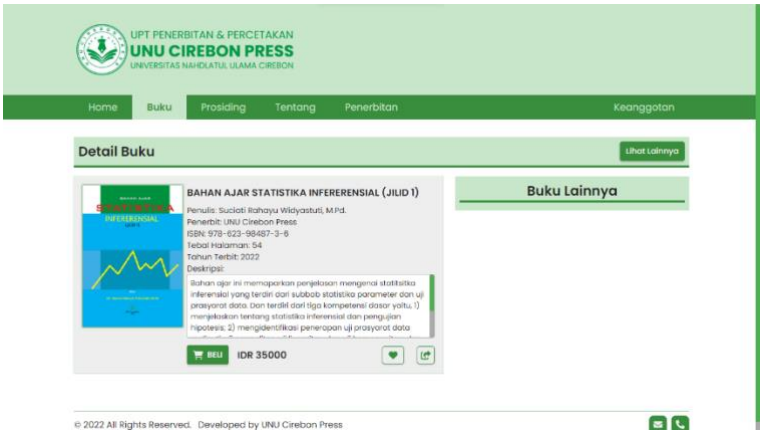
Pada halaman ini pengunjung dan admin dapat melihat buku-buku yang telah diterbitkan dan bisa membacanya jika lisensinya adalah gratis.

Gambar 11 Halaman Masuk

Pada halaman ini pengunjung bisa masuk jika sudah terdaftar sebagai anggota dari UNU Cirebon Press, dengan cara mengisi *form email* dan *password*. Setelah itu akan diarahkan ke halaman utama kembali untuk bisa melihat-lihat buku dan membacanya.

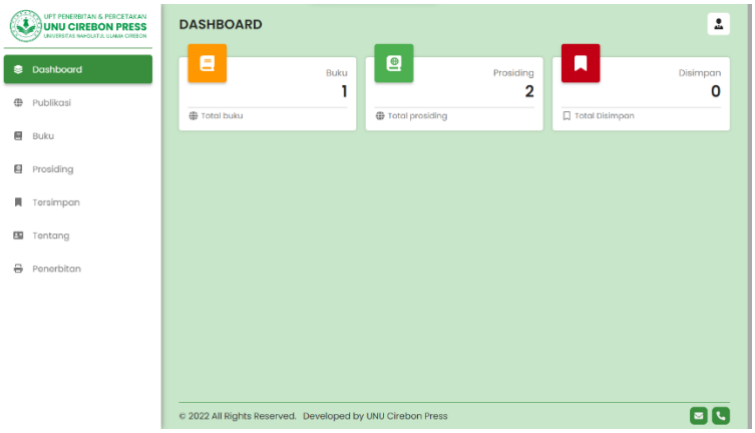
Gambar 12 Halaman Buku

Pada halaman ini akan ditampilkan semua buku yang telah diterbitkan dan pengunjung dapat melihat dan membacanya.



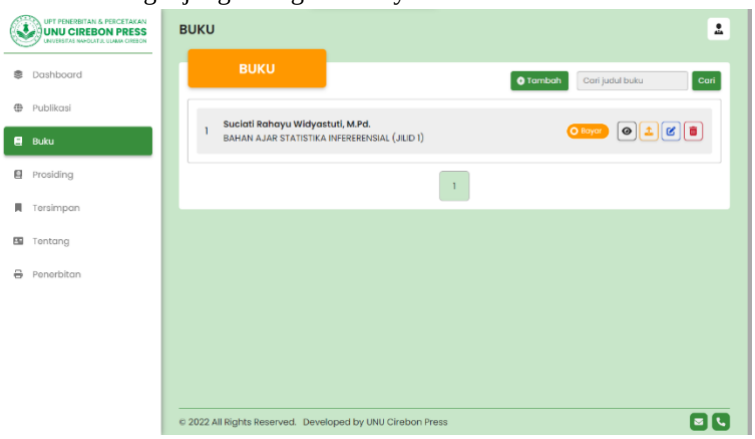
Gambar 13 Halaman Detail Buku

Pada halaman ini akan menampilkan detail buku yang telah dipilih oleh pengunjung dan dapat membacanya jika lisensi dari buku tersebut adalah gratis.



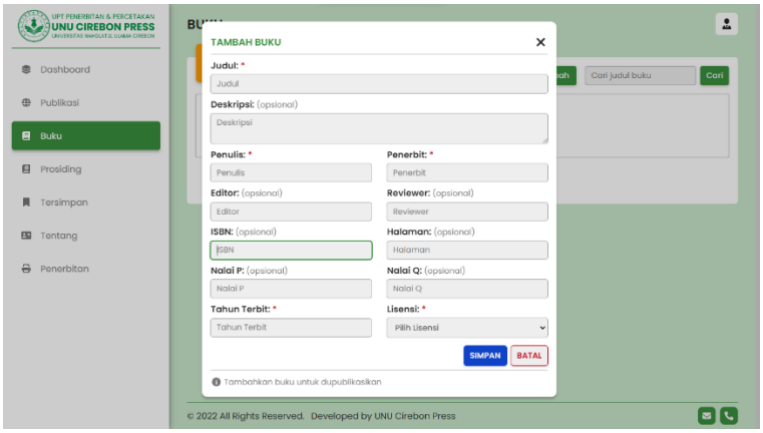
Gambar 14 Halaman Dashboard

Pada halaman ini admin dapat melihat jumlah buku yang telah diterbitkan dan yang telah admin simpan dan bisa mengunjungi navigasi lainnya.



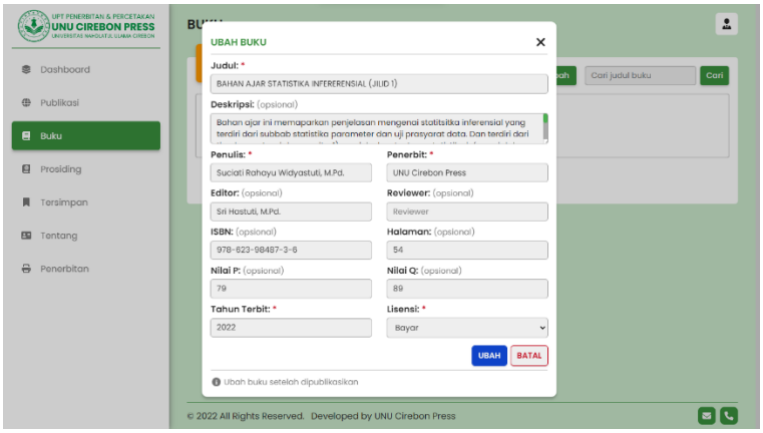
Gambar 15 Halaman Dashboard Buku

Pada halaman ini admin dapat melihat, menambahkan, mengedit, menghapus, mengunggah berkas cover dan file buku untuk diterbitkan.



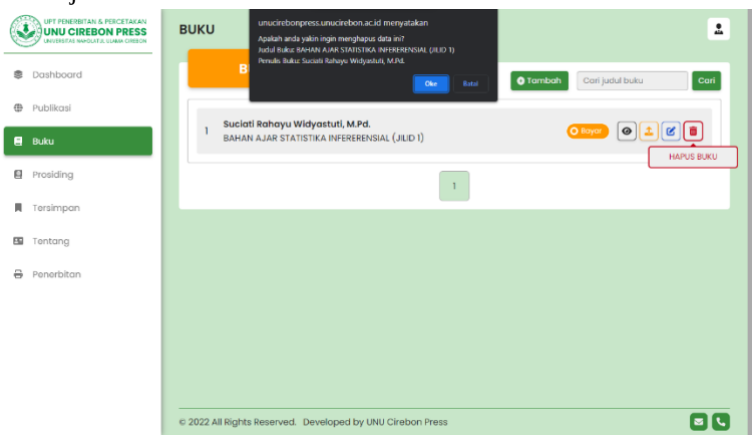
Gambar 16 Halaman Dashboard Tambah Buku

Pada halaman ini admin dapat menambahkan buku dengan cara mengisi semua form yang tersedia.



Gambar 17 Halaman Dashboard Ubah Buku

Pada halaman ini admin dapat mengubah buku sesuai yang admin inginkan dan akan langsung diterbitkan jika sudah menekan tombol ubah.



Gambar 18 Halaman Dashboard Hapus Buku

Pada halaman ini admin dapat menghapus buku dengan menekan tombol hapus dan mengkonfirmasi penghapusan buku.

Gambar 19 Halaman Dashboard Unggah Buku

Pada halaman ini admin dapat mengunggah berkas cover dalam bentuk gambar (jpg, png, jpeg) dan file dalam bentuk dokumen (pdf)

Pengujian Sistem

Pengujian sistem dilakukan untuk memastikan bahwa setiap fungsi yang ada dapat berjalan dengan baik dan sesuai dengan yang direncanakan. Pengujian ini mencakup berbagai halaman sistem, mulai dari halaman utama, halaman buku, halaman detail buku, hingga halaman dashboard untuk admin. Hasil pengujian yang ditampilkan pada Tabel 3 menunjukkan bahwa seluruh fungsionalitas sistem telah diuji dan dinyatakan valid, termasuk navigasi, pencarian buku, penambahan dan penghapusan data, serta pengunggahan berkas. Setiap fitur berhasil diuji tanpa terdapat kesalahan atau error yang signifikan.

Tabel 3 Pengujian Sistem

Halaman	Pengujian	Hasil
Halaman Utama	Navigasi dan tampilan	Valid
	Mengujikan navigasi dan tampilan halaman utama	Valid
	Memastikan tautan dan menu berfungsi dengan baik	Valid
Halaman Buku	Menampilan daftar buku	Valid
	Navigasi ke halaman Detail Buku	Valid
	Pencarian buku berdasarkan judul	Valid
Halaman Detail Buku	Menampilkan informasi buku	Valid
	Memastikan tombol baca berfungsi	Valid
Halaman Penerbitan	Menampilan daftar prosedur penerbitan	Valid
	Menampilan gambar alur penerbitan	Valid
Halaman Masuk	Mengujikan kemampuan masuk menggunakan akun yang sudah terdaftar	Valid
	Memastikan pesan error ditampilkan saat akun yang salah dimasukkan	Valid
Halaman Registrasi	Mengujikan kemampuan untuk membuat akun baru	Valid
	Memastikan pesan error ditampilkan saat informasi yang tidak valid dimasukkan	Valid
Halaman Dashboard	Mengujikan tampilan dan fungsionalitas dashboard	Valid
	Memastikan data yang ditampilkan sesuai dengan hak akses pengguna	Valid
Halaman Dashboard Buku	Tampilan daftar buku	Valid
	Penambahan, pengubahan, dan penghapusan buku	Valid
	Memastikan pesan error ditampilkan saat informasi yang tidak lengkap dimasukkan	Valid
	Mengujikan tombol unggah berfungsi	Valid
	Mengujikan tombol perhapusan hasil unggahan	Valid
Halaman Dashboard Penerbitan	Menampilan daftar prosedur penerbitan	Valid
	Mengujikan kemampuan untuk mengubah informasi penerbitan	Valid
	Memastikan pesan error ditampilkan saat informasi yang tidak valid dimasukkan	Valid
	Mengujikan tombol unggah berfungsi	Valid
	Mengujikan tombol perhapusan hasil unggahan	Valid
Halaman Keluar	Klik pada menu logout	Valid
	Memastikan bahwa pengguna berhasil logout dan tidak dapat mengakses halaman dashboard setelah logout	Valid

Keamanan dan Integritas Data

Penerapan algoritma RSA pada sistem ini berfungsi untuk mengamankan data sensitif, seperti informasi hak cipta, data pembayaran, dan identitas pengguna. Algoritma RSA menggunakan kunci publik dan kunci privat untuk proses enkripsi dan dekripsi, sehingga hanya pihak yang memiliki kunci dekripsi yang dapat mengakses informasi tersebut. Hal ini sangat penting dalam konteks penerbitan buku, karena memastikan bahwa data tidak dapat diakses oleh pihak yang tidak berwenang. Pengujian yang dilakukan menunjukkan bahwa proses enkripsi dan dekripsi dengan RSA berjalan dengan baik, meskipun membutuhkan waktu pemrosesan yang lebih lama dibandingkan dengan algoritma simetris lainnya. Namun, tingkat keamanan yang diberikan sebanding dengan waktu pemrosesan yang dibutuhkan.

Algoritma RSA adalah salah satu algoritma kriptografi asimetris yang paling populer dan banyak digunakan. Berikut adalah langkah-langkah dasar dalam perhitungan algoritma RSA:

1. Pemilihan Bilangan Prima:
   Pilih dua bilangan prima yang berbeda, p dan q.
   Misalnya, p = 61 dan q = 53.
2. Menghitung Modulus (n):
   Hitung nilai n dengan mengalikan p dan q, yaitu n = p * q.
   Contoh: n = 61 * 53 = 3233.
3. Menghitung Totient Euler (φ): φ(n) = (p-1)(q-1).
   Contoh: φ(3233) = (61-1)(53-1) = 60 * 52 = 3120.
4. Pemilihan Kunci Publik (e):
   Pilih bilangan bulat e (1 < e < φ(n)), yang relatif prima terhadap φ(n). Dalam contoh ini, kita bisa memilih e = 17, karena gcd(17, 3120) = 1.
5. Menghitung Kunci Privat (d):
   Hitung d sehingga (d * e) % φ(n) = 1. Dalam kata lain, d adalah invers modular dari e modulo φ(n).
   Dalam contoh ini, d = 2753 karena (17 * 2753) % 3120 = 1.
   Sekarang kita memiliki kunci publik (e, n) = (17, 3233) dan kunci privat (d, n) = (2753, 3233).
6. Enkripsi:
   Untuk mengenkripsi pesan M (dalam bentuk angka), gunakan kunci publik (e, n) dan hitung pesan terenkripsi C sebagai berikut:
   C ≡ M ^ e (mod n)
   Contoh: Misalkan M = 123, maka C = 123^17 (mod 3233) = 855.
7. Dekripsi:
   Untuk mendekripsi pesan yang terenkripsi C, gunakan kunci privat (d, n) dan hitung pesan asli M sebagai berikut:
   M ≡ C ^ d (mod n)
   Contoh: M = 855^2753 (mod 3233) = 123.

Kelebihan dan Kekurangan Sistem Baru

Sistem baru yang dikembangkan memiliki beberapa kelebihan dibandingkan dengan sistem lama. Salah satu kelebihannya adalah peningkatan keamanan melalui penggunaan algoritma kriptografi RSA, yang memberikan perlindungan terhadap data sensitif dan mencegah akses tidak sah. Selain itu, sistem ini menyediakan fitur yang lebih lengkap untuk admin, seperti kemampuan

untuk menambahkan, mengubah, dan menghapus data buku, serta mengunggah berkas terkait penerbitan. Namun, ada beberapa tantangan yang dihadapi dalam implementasi sistem ini, terutama terkait waktu pemrosesan enkripsi yang lebih lama dan kebutuhan sumber daya komputasi yang lebih besar. Kendala ini merupakan konsekuensi dari penggunaan algoritma RSA, tetapi manfaat yang diperoleh dalam hal keamanan data jauh lebih besar dibandingkan dengan kendala tersebut.

Umpan Balik Pengguna

Pendekatan prototipe yang digunakan dalam pengembangan sistem ini memungkinkan pengembang untuk terus mendapatkan umpan balik dari pengguna selama proses iterasi. Hal ini membantu memastikan bahwa sistem yang dikembangkan dapat memenuhi kebutuhan pengguna, baik dari segi fungsionalitas maupun keamanan. Umpan balik yang diterima dari pengguna, terutama admin, sangat positif, dengan penekanan pada kemudahan penggunaan sistem dan peningkatan keamanan data. Pengguna merasa lebih nyaman menggunakan sistem ini, karena mereka yakin bahwa data yang mereka kelola terlindungi dengan baik.

KESIMPULAN

Hasil penelitian menunjukkan bahwa sistem informasi penerbitan buku yang dikembangkan mampu memfasilitasi dosen dalam menerbitkan buku dengan lebih efisien. Sistem ini memberikan kemudahan dalam pengelolaan setiap tahapan penerbitan, mulai dari pengajuan naskah hingga publikasi, yang pada akhirnya mengurangi hambatan administratif. Peningkatan efisiensi ini memungkinkan dosen untuk lebih fokus pada peningkatan kualitas isi buku, sehingga dapat meningkatkan produktivitas dan kualitas karya akademik.

Selain itu, implementasi algoritma Rivest-Shamir-Adleman (RSA) dalam sistem ini berhasil meningkatkan keamanan data buku, melindungi informasi hak cipta, detail penulis, dan berkas buku dari akses tidak sah. Penggunaan algoritma RSA memastikan integritas dan kerahasiaan data, serta mencegah pemalsuan dan pelanggaran hak cipta, yang memberikan perlindungan yang lebih baik bagi penulis dan penerbit. Secara keseluruhan, sistem ini menawarkan efisiensi dan keamanan yang lebih baik, sehingga diharapkan dapat meningkatkan kepercayaan dan partisipasi dosen dalam proses penerbitan buku di lingkungan akademik.

REFERENSI

[1] D. P. R. RI dan P. RI, *Hak Cipta*, vol. 20. 2018. Diakses: 18 Juli 2023. [Daring]. Tersedia pada: http://peraturan.bpk.go.id/Details/38690

[2] R. S. Brahmandari, "Pelanggaran Hak Cipta di Indonesia dan Sanksinya," Blog Justika - Situs Konsultasi Hukum via Online. Diakses: 18 Juli 2023. [Daring]. Tersedia pada: https://blog.justika.com/dokumen-bisnis/pelanggaran-hak-cipta/

[3] U. Press, "UPI Press." Diakses: 27 Juli 2023. [Daring]. Tersedia pada: https://upipress.upi.edu/

[4] A. Fin, "Implementasi QR Code Menggunakan Algoritma RSA," *Kumpul. Karya Ilm. Mhs. Fak. Sains Dan Tekhnologi*, vol. 1, no. 1, Art. no. 1, Jun 2021, Diakses: 14 Juli 2023. [Daring]. Tersedia pada: https://jurnal.pancabudi.ac.id/index.php/fastek/article/view/3026

[5] M. Y. Simargolang, "Implementasi Kriptografi RSA Dengan PHP," *J. Teknol. Inf.*, vol. 1, no. 1, hlm. 1, Jun 2017, doi: 10.36294/jurti.v1i1.1.

[6] D. H. Prasetyo dan D. Priharsari, "Pengembangan Sistem Informasi Distribusi Buku Berbasis Web (Studi Kasus: Penerbit Aryoko Indonesia)," *J. Pengemb. Teknol. Inf. Dan Ilmu Komput.*, vol. 4, no. 10, Art. no. 10, Okt 2020, Diakses: 17 Juli 2023. [Daring]. Tersedia pada: https://j-ptiik.ub.ac.id/index.php/j-ptiik/article/view/8076

[7] A. Ginting, R. R. Isnanto, dan I. P. Windasari, "IMPLEMENTASI ALGORITMA KRIPTOGRAFI RSA UNTUK ENKRIPSI DAN DEKRIPSI EMAIL," *J. Teknol. Dan Sist. Komput.*, vol. 3, no. 2, hlm. 253–258, Apr 2015, doi: 10.14710/jtsiskom.3.2.2015.253-258.

[8] Y. Anshori, A. Y. E. Dodu, dan D. M. P. Wedananta, "IMPLEMENTASI ALGORITMA KRIPTOGRAFI RIVEST SHAMIR ADLEMAN (RSA) PADA TANDA TANGAN DIGITAL," *Techno.Com*, vol. 18, no. 2, Art. no. 2, Mei 2019, doi: 10.33633/tc.v18i2.2166.

[9] A. Khamsyar dan Muh. Basri, "Aplikasi Enkripsi Gambar Menggunakan Metode (Rivest Shamir Adleman) RSA," *J. Sintaks Log.*, vol. 2, no. 3, Art. no. 3, Okt 2022, doi: 10.31850/jsilog.v2i3.1850.

[10] B. Setiaji, "ANALISIS DAN IMPLEMENTASI ALGORITMA KRIPTOGRAFI KUNCI PUBLIK RSA DAN LUC UNTUK PENYANDIAN DATA," *Data Manaj. Dan Teknol. Inf. DASI*, vol. 16, no. 3, Art. no. 3, Sep 2015, Diakses: 14 Juli 2023. [Daring]. Tersedia pada: https://ojs.amikom.ac.id/index.php/dasi/article/view/247

[11] D. Apdilah dan H. Swanda, "Penerapan Kriptografi RSA dalam Mengamankan File Teks Berbasis PHP," *J. Teknol. Inf.*, vol. 2, no. 1, hlm. 45–52, Jun 2018, Diakses: 17 Juli 2023. [Daring]. Tersedia pada: https://www.neliti.com/id/publications/281917/

[12] I. Meidina, Y. Siradj, dan E. Insanudin, "Pembangunan Web Administrator Pada Aplikasi Media Informasi Dan Perdagangan Untuk Petani Sayur Di Nagari Alahan Panjang Kabupaten Solok," *EProceedings Appl. Sci.*, vol. 6, no. 2, Art. no. 2, Agu 2020, Diakses: 17 Juli 2023. [Daring]. Tersedia pada: https://openlibrarypublications.telkomuniversity.ac.id/index.php/appliedscience/article/view/12914

[13] D. Ariani dan D. A. Punkastyo, "Implentasi Algoritma RSA Untuk Aplikasi Enkripsi Dan Dekripsi Citra Dua Dimensi Berbasis Web (Studi Kasus: PT. Intigarmindo Persada)," *OKTAL J. Ilmu Komput. Dan Sains*, vol. 2, no. 03, Art. no. 03, Mar 2023, Diakses: 14 Juli 2023. [Daring]. Tersedia pada: https://journal.mediapublikasi.id/index.php/oktal/article/view/971