Jurnal Ilmiah Teknik Informatika dan Komunikasi
Volume 5. Nomor. 3 November 2025
E-ISSN: 2827-7945 ; P-ISSN: 2827-8127, Hal 647-659
DOI: https://doi.org/10.55606/juitik.v5i3.1711
Tersedia: https://journal.sinov.id/index.php/juitik

Implementasi Algoritma Kriptografi RSA dalam Proses Enkripsi dan Dekripsi untuk Mengamankan Pesan Singkat pada Aplikasi Chatting Berbasis Web

Nurul Maulida Surbakti[1], Dinda Kartika[2*], Alya Dwi Lestari[3], Maysi Puspita[4], Petra Putri Sarinah Pandiangan[5], Riamonda Singarimbun[6], Windi Suryani[7]
[1-6] Program Studi Matematika, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Negeri Medan, Indonesia
[*]*Penulis korespondensi: dindakartika@unimed.ac.id[1]*

Abstract. *The rapid development of information technology, especially in online communication, raises concerns about the security and privacy of transmitted messages. Cryptography serves as a primary alternative to protect information from unauthorized access. This study aims to implement the RSA (Rivest Shamir Adleman) cryptographic algorithm to secure short messages in a web-based chat application. The research method used was a mixed method, combining literature study and application development trials. The designed application uses the Flask framework for the backend, while HTML, CSS, and JavaScript are used for the user interface. The implementation results show that the RSA algorithm successfully converted plaintext messages (e.g., "Haii") into ciphertext (such as [7347,3641,4742,4742]) using a public key and accurately restored them to the original message using a private key, without any loss of information. This application offers an interactive and visual interface, making it easier for users to understand the RSA encryption and decryption process. Testing confirmed a consistency between manual calculations and the application's functions, proving that the system works stably and accurately. It is concluded that the RSA algorithm can be used effectively to protect short messages on web-based chat platforms, serving not only as a secure communication tool but also as an effective learning medium for asymmetric cryptography concepts. For future development, it is recommended to use larger prime numbers to enhance security, as well as to add features such as file sharing and group chats.*

Keywords: *Chat Application; Cryptography; Data Security; Encryption-Decryption; RSA Algorithm*

Abstrak. Pesatnya perkembangan teknologi informasi, terutama dalam komunikasi online, menimbulkan kecemasan mengenai keamanan dan privasi pesan yang ditransmisikan. Kriptografi menjadi alternatif utama untuk melindungi informasi dari akses yang tidak sah. Penelitian ini bertujuan untuk menerapkan algoritma kriptografi RSA (Rivest Shamir Adleman) dalam mengamankan pesan singkat di aplikasi chatting yang berbasis web. Metode penelitian yang dipakai adalah metode campuran, yang menggabungkan studi literatur dan uji coba pembuatan aplikasi. Aplikasi yang dirancang menggunakan framework Flask di sisi backend, sementara HTML, CSS, dan JavaScript digunakan untuk antarmuka pengguna. Hasil dari implementasi menunjukkan bahwa algoritma RSA berhasil mengubah pesan plaintext (misalnya "Haii") menjadi ciphertext (seperti [7347,3641,4742,4742]) dengan menggunakan kunci publik dan berhasil mengembalikannya ke pesan asli dengan tepat melalui kunci privat, tanpa kehilangan informasi. Aplikasi ini menawarkan antarmuka yang interaktif dan visual, sehingga memudahkan pengguna untuk memahami proses enkripsi dan dekripsi RSA. Pengujian telah memastikan adanya kesesuaian antara perhitungan secara manual dan fungsi pada aplikasi, membuktikan bahwa sistem ini berfungsi dengan baik dan tepat. Disimpulkan bahwa algoritma RSA dapat digunakan secara efektif untuk melindungi pesan singkat di platform chatting berbasis web, berperan tidak hanya sebagai sarana komunikasi yang aman tetapi juga sebagai sarana pembelajaran yang efektif tentang konsep kriptografi asimetris. Untuk pengembangan selanjutnya, disarankan untuk menggunakan bilangan prima yang lebih besar demi peningkatan keamanan, serta menambah fitur seperti berbagi file dan obrolan grup.

Kata kunci: Algoritma RSA; Aplikasi Chat; Enkripsi-Dekripsi; Keamanan Data; Kriptografi

1. LATAR BELAKANG

Perubahan zaman dan kemajuan teknologi informasi yang pesat memungkinkan manusia untuk melaksanakan berbagai aktivitas yang berkaitan dengan media elektronik dengan lebih mudah. Semua perusahaan teknologi bersaing untuk menghadirkan inovasi yang

Naskah Masuk: 03 Oktober 2025; Revisi: 21 Oktober 2025; Diterima: 05 November 2025;
Terbit: 10 November 2025

lebih mutakhir, efisien, dan praktis dibandingkan dengan produk sebelumnya. Meskipun penerapan teknologi ini dapat memberikan manfaat yang baik, juga ada sisi negatif dalam kehidupan manusia. Melalui aplikasi chat, seseorang dapat dengan mudah mengirim pesan kepada orang lain dengan cepat, baik dalam bentuk teks, suara, gambar, maupun video (Gusti, A.2021).

Teknologi Informasi merupakan kategori sumber daya yang mendukung proses pembuatan, analisis, penyebaran, penyimpanan, dan penghapusan data serta informasi. Beberapa dimensi atau indikator dari Teknologi Informasi diantaranya adalah perangkat keras, perangkat lunak, basis data, pengguna, jaringan lokal, dan jaringan luas atau internet (Nurul et al., 2022)

Informasi merupakan data yang telah diubah menjadi bentuk yang memiliki makna untuk penerimanya dan berguna dalam membuat keputusan saat ini atau di masa depan. Perkembangan teknologi informasi yang berlandaskan komputer mempermudah organisasi atau perusahaan dalam mengakses informasi dari mana saja dan kapan saja (Informasi et al., 2023).

Secara etimologis, istilah Kriptografi berakar dari bahasa Yunani yang berarti tersembunyi dan tulisan. Awalnya, kriptografi dipahami sebagai ilmu yang berkaitan dengan penyembunyian pesan; namun, seiring dengan perkembangan zaman, sekarang telah menjadi ilmu yang menggunakan teknik matematika untuk mengatasi masalah keamanan, termasuk privasi dan otentikasi. Teks pesan yang dikirimkan oleh pengirim dapat dengan mudah diakses oleh pihak yang ingin mengetahui isi percakapan karena tidak melalui proses enkripsi sepanjang perjalanannya. Masalah terkait keamanan dan kerahasiaan informasi merupakan salah satu aspek krusial dalam komunikasi berbasis komputer, di mana komputer yang terhubung dengan jaringan menghadapi ancaman keamanan yang lebih serius (Studi Teknik Informa & Korespondensi, 2022).

Kriptografi memiliki asal kata dari bahasa Yunani, yaitu Kryptos yang berarti tersembunyi atau rahasia, dan Graphein yang berarti menulis. Dengan demikian, arti dari kriptografi secara harfiah adalah menulis dengan cara yang tidak terlihat untuk menyampaikan pesan-pesan yang perlu dijaga kerahasiaannya. Selain itu, kriptografi juga berkaitan dengan bidang ilmu yang mempelajari metode-metode matematika yang berkaitan dengan keamanan informasi dan perlindungan pesan, yang terdiri dari dua proses utama yaitu enkripsi dan dekripsi. Enkripsi adalah proses menyembunyikan isi pesan dengan mengubah plaintext (pesan yang dapat dibaca) menjadi ciphertext (pesan acak yang tidak dapat dibaca). Sedangkan Deskripsi adalah proses yang berlawanan dengan enkripsi, yaitu mengembalikan bentuk yang

tersamar ke informasi aslinya (Nanda et al., 2023).

Penerapan metode kriptografi RSA dalam proses enkripsi dan dekripsi informasi memanfaatkan kunci publik dan kunci pribadi. Kunci-kunci ini dihasilkan melalui proses pemfaktoran angka-angka prima yang telah ditetapkan sebelumnya (Dairi et al., 2022)

Kriptografi mempelajari metode metode matematis yang terkait dengan keamanan informasi, termasuk perlindungan data, validitas data, keutuhan data, serta verifikasi identitas data. Algoritma kriptografi merupakan prosedur-prosedur yang logis untuk menyembunyikan informasi dari individu yang tidak berwenang untuk mengaksesnya (M. Arief & Ikhsan, 2015).

2. TINJAUAN PUSTAKA

Aplikasi perpesanan adalah sebuah layanan pesan instan yang ada dalam teknologi jaringan komputer, memungkinkan penggunanya untuk mengirim pesan kepada orang lain yang terhubung dalam jaringan komputer atau internet. Selain itu, aplikasi perpesanan juga menyediakan fitur tambahan yang memungkinkan pengguna untuk berbagi data kepada semua pengguna yang ada, yang bisa diakses oleh banyak orang. Fitur ini berfungsi sebagai sarana komunikasi antara klien dan server, sehingga klien bisa mendapatkan akses untuk melihat dan mengunggah file dalam aplikasi perpesanan tersebut (Sulaksono et al., 2021).

Kriptografi merupakan bidang yang mempelajari metode-metode matematis terkait dengan pengamanan informasi, termasuk kerahasiaan, keaslian, integritas, dan autentikasi data. Namun, tidak semua aspek pengamanan informasi dapat ditangani melalui kriptografi. Dengan menggunakan kunci dekripsi, informasi asli dapat dipulihkan. Berbagai teknik diterapkan untuk melindungi data atau informasi yang signifikan. Kriptografi berperan dalam mengubah pesan menjadi bentuk yang tersandikan (Hidayat et al., 2023).

Kriptografi dibuat untuk memastikan bahwa informasi yang bersifat pribadi dan dikirim melalui jaringan, seperti LAN atau internet, tidak dapat diakses dan digunakan oleh pihak-pihak tidak berwenang. RSA merupakan algoritma kriptografi yang memanfaatkan kunci public yang sering disebut sebagai kunci asimetrik (kunci untuk enkripsi dan deskripsi berbeda), sehingga tidak memerlukan saluran aman untuk mendistribusikan kunci (A. Arief & Saputra, 2016).

Algoritma kriptografi RSA merupakan cara yang bergantung pada pemfaktoran bilangan bilangan sangat besar, sehingga dianggap sulit untuk dipecahkan. Algoritma ini diciptakan oleh tiga peneliti dari MIT (Massachusetts Institute of Technology) pada tahun 1976, yaitu Ron Rivest, Adi Shamir, serta Leonard Adleman. Kekuatan algoritma RSA terletak pada kompleksitas memfaktorkan bilangan besar menjadi bilangan prima, sehingga

penggunaan bilangan prima yang lebih besar meningkatkan tingkat keamanannya. Dalam penerapan algoritma RSA pada kriptografi terdapat tiga langkah, yaitu pembuatan kunci publik dan kunci privat, langkah enkripsi, dan langkah dekripsi. Dua bilangan prima besar yang acak dipilih untuk menghasilkan kedua kunci tersebut (Dairi et al., 2022).

Setiap jenis algoritma kriptografi memiliki variasi dalam tingkat keamanannya, serta perbedaan dalam proses enkripsi dan dekripsinya dibandingkan algoritma lain. Di antara berbagai metode perlindungan data, RSA (Rivest Shamir Adleman) adalah salah satu yang paling umum digunakan, dan merupakan salah satu algoritma kunci publik yang sangat terkenal hingga sekarang (Siregar et al., 2023)

Algoritma RSA adalah jenis blok cipher yang mengubah semua data menjadi sebuah bilangan bulat. RSA terdiri dari dua jenis kunci, yaitu kunci publik yang dapat diakses oleh siapa saja, dan kunci privat yang hanya diketahui oleh pemilik data tersebut. Untuk enkripsi, digunakan kunci publik, sementara dekripsi dilakukan dengan kunci privat milik pemilik data (Dairi et al., 2022)

Berikut adalah tahapan dalam algoritma kriptografi RSA ;

Pembangkitan Kunci Pada RSA

Penggunaan RSA dalam pengkodean memerlukan sepasang kunci yang berbeda untuk enkripsi dan dekripsi. Angka yang dipilih sebagai kunci merupakan bilangan prima besar, dan memfaktorkan hasil kali dari dua bilangan prima besar menjadi dua bilangan prima yang tepat sangatlah sulit. Untuk menghasilkan kunci, digunakan algoritma berikut ini;

a. Pilih sepasang bilangan prima acak yang besar, yaitu p dan q. Nilai dari p dan q sebaikny a tetap disembunyikan
b. Hitung n dengan rumus $n\ p\ x\ q$. Besaran n tidak perlu dirahasiakan dan sebaiknya p tida k sama dengan q. Jika p sama dengan q, maka n akan menjadi p^2 , sehingga p dapat dite mukan dengan mengambil akar kuadrat dari n.
c. Hitung n dengan rumus $n = (p - 1)(q - 1)$
d. Pilih suatu bilangan bulat untuk kunci publik yang dikenal sebagai e, yang memiliki sifat relatif prima terhadap n. Relatif prima terhadap n berarti satu-satunya faktor pembagi yang dimiliki oleh keduanya adalah 1, secara matematis dinyatakan dengan $gcd\ (e, n) = 1$.
e. Hitung kunci untuk dekripsi (d) menggunakan persamaan $e.\ d\ mod\ n = 1$.

Hasil dari algoritma diatas yaitu ;

a. Kunci publik adalah pasangan (e, n)

b. Kunci privat adalah pasangan (d, n)

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

Proses Enskripsi pada Algoritma RSA ;

Enkripsi merupakan proses untuk mengubah pesan yang terdengar jelas (plaintext) menjadi pesan yang tersembunyi (ciphertext). Dalam tahap ini, pesan yang jelas terlebih dahulu diubah menjadi format desimal, lalu pesan yang telah berformat desimal akan dibagi menjadi beberapa kelompok desimal dengan cara yang teratur. Setiap kelompok desimal harus memiliki nilai yang lebih kecil dari nilai n yang disebut P. Berikut adalah langkah-langkah yang diterapkan dalam melakukan proses enkripsi pada algoritma RSA.Menggunakan public key (e, n).

a. PlaintextM dinyatakan menjadi blok-blok $P1, P2, P3, \ldots$

b. Setiap blok M_i di enkripsi menjadi C_i, dengan rumus $C_i = P_i^e \ mod \ n$

Proses Deskripsi pada Algoritma RSA ;

Proses dekripsi pada algoritma RSA mirip dengan proses enkripsinya, hanya saja kunci yang digunakan dalam proses dekripsi adalah kunci privat d. Adapun langkah-langkah yang digunakan untuk melakukan proses dekripsi pada algorimta RSA adalah sebagai berikut ;

a. Menggunakan private key(d, n)

b. Pilih ciphertext C

c. Setiap blok C_i di dekripsi menjadi blok P_i, dengan rumus $P_i = C_i^d \ mod \ n$

RSA merupakan metode kriptografi asimetrik yang memanfaatkan dua kunci, yaitu kunci publik yang digunakan untuk enkripsi dan kunci privat yang digunakan untuk dekripsi. Keamanan RSA terletak pada kesulitan manusia untuk memfaktorkan angka besar dengan efektif. Prosedur awal dalam algoritma RSA melibatkan pembuatan kunci publik dan kunci privat. Pengguna dapat menentukan panjang kunci dengan menggunakan parameter yang telah ditentukan. Data yang akan dienkripsi pertama-tama akan dikodekan, kemudian dienkripsi menggunakan kunci publik. Implementasi pengamanan data RSA dilakukan dengan menggunakan pustaka rsa dan bahasa pemrograman Python (Fajrin et al., 2024).

Keamanan adalah hal yang sangat krusial. Memelihara kerahasiaan informasi dalam dunia bisnis memerlukan tingkat perlindungan yang tinggi. Agar hal ini dapat tercapai, kolaborasi antara pemerintah dan lembaga keuangan sangat diperlukan. Data sensitif memiliki nilai yang sangat penting. Metode tertentu digunakan untuk menyimpan dan mengirim informasi agar memastikan bahwa hanya pihak yang berwenang yang dapat mengakses atau

mengubah data tersebut. Informasi ini disimpan pada komputer atau dalam basis data email. Untuk menjamin bahwa data terlindungi dengan baik, perlu diterapkan sistem keamanan yang efektif yang tidak bisa diakses oleh individu yang tidak berhak, dengan mempertimbangkan baik aspek keamanan fisik maupun sistemnya (Sari et al., 2022).

Mengamankan informasi dapat dilakukan dengan berbagai metode, salah satunya adalah melalui penerapan kriptografi yang berfungsi untuk melindungi pesan atau data saat ditransmisikan dari satu lokasi ke lokasi lainnya. Prinsip yang diterapkan melibatkan teknik enkripsi atau dekripsi. Pada akhirnya, informasi atau data ini akan mulai sebagai plainText, kemudian diubah melalui proses yang dikenal sebagai enkripsi menggunakan kunci tertentu. Hasil dari proses enkripsi ini bersifat acak dan setelah enkripsi, hasil tersebut dikenal dengan sebutan cipherText. Untuk mengembalikan cipherText ke bentuk plainText, kita melakukan proses yang disebut dekripsi. Proses ini bertujuan untuk mengubah kembali cipherText menjadi plainText agar penerima dapat memahami pesan yang diterima, tentu saja dengan kunci yang telah disiapkan (Ramadhan et al., 2023).

Salah satu cara untuk melindungi data adalah dengan menerapkan kriptografi. Algoritma kriptografi yang umum digunakan dalam pelindungan data adalah algoritma RSA. Algoritma RSA merupakan algoritma yang gampang untuk diterapkan dan dipahami (Sulaiman & Vebu, 2018).

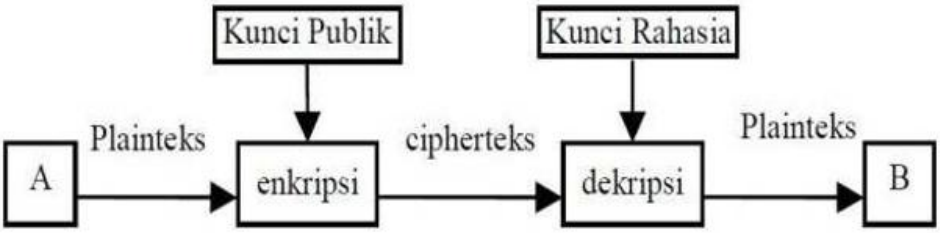
3. METODE PENELITIAN

Penelitian ini menerapkan metode campuran yang mengintegrasikan tinjauan pustaka dan eksperimen pembuatan aplikasi. Metode ini dipilih untuk memperoleh dasar teori yang kokoh sambil menguji penerapan langsung algoritma RSA dalam pengamanan pesan singkat pada aplikasi chat berbasis web.

Metode penelitian ini mengintegrasikan tinjauan pustaka dan eksperimen untuk memperoleh wawasan yang menyeluruh tentang penerapan kriptografi RSA dalam pemrograman. Melalui tinjauan pustaka, peneliti menganalisis langkah-langkah enkripsi dan dekripsi serta penerapan algoritma RSA. Di sisi lain, dengan studi pustaka, peneliti mengumpulkan informasi teoretis tentang dasar-dasar Kriptografi, algoritma RSA, dan konsep-konsep dalam bahasa pemrograman python. Kedua pendekatan ini menghasilkan pemahaman yang lengkap dan mendalam mengenai penerapan kriptografi RSA.

4. HASIL DAN PEMBAHASAN

Keamanan dari sistem sandi RSA berasal dari kompleksitas dalam memfaktorkan angka-angka besar. Hingga sekarang, RSA masih diandalkan dan banyak digunakan di dunia maya



Gambar 1. Skema Kunci Kriptografi.

Rangkaian algoritma kunci publik RSA terdiri dari tiga tahap utama, yaitu pembuatan kunci, proses enkripsi, dan proses dekripsi. Sebelum itu, akan dijelaskan beberapa konsep matematis yang mendasari RSA (Iii et al., 2019).

Pada gambar 4. 1 terlihat suatu proses yang dimulai saat Pengirim (Pihak A) ingin mengirimkan pesan asli (plainteks) kepada Penerima (Pihak B) secara aman. Untuk menjaga keamanan pesan tersebut, A memanfaatkan kunci publik milik B yang tersedia secara umum untuk melakukan enkripsi. Proses enkripsi ini mengubah plainteks menjadi cipherteks, yaitu bentuk pesan yang telah terenkripsi dan tidak dapat dimengerti tanpa kunci yang benar. Cipherteks kemudian dikirim melalui saluran komunikasi, yang meskipun bisa saja disadap, tidak akan mengungkapkan isi pesan karena hanya bisa dibuka dengan kunci rahasia yang sesuai.

Setelah teks terenkripsi sampai di tempat tujuan, Penerima (B) memanfaatkan kunci rahasia yang hanya dia miliki untuk melakukan proses dekripsi. Proses ini mengubah teks terenkripsi kembali menjadi bentuk pesan semula (plainteks), sehingga B bisa memahami isi yang dikirimkan oleh A. Keamanan dari sistem ini berpijak pada sepasang kunci asimetris: kunci publik berfungsi untuk mengamankan (enkripsi) pesan, sementara kunci rahasia yang bersangkutan digunakan untuk mengakses (dekripsi) pesan tersebut. Metode ini menjamin kerahasiaan dan integritas informasi, serta sering digunakan dalam teknologi seperti SSL/TLS, email yang aman, dan tanda tangan elektronik.

Implementasi Tampilan Antarmuka

Gambar 2. Tampilan Antarmuka Web Chat RSA.

Aplikasi percakapan yang menggunakan enkripsi RSA kini telah berhasil diluncurkan dan dapat diakses online melalui tautan: https://squashier-dorthey-shakily.ngrok-free.dev . Untuk pengembangan aplikasi ini, digunakan framework Flask pada sisi backend, sementara antarmukanya dibuat dengan kombinasi HTML, CSS, dan JavaScript. Situs ini dilengkapi fitur untuk memasukkan nama pengguna, menyimpan identitas, memilih pengguna lain, serta menghapus riwayat obrolan. Selain itu, hadir juga kolom untuk memasukkan pesan dan tombol Kirim yang berfungsi untuk memulai interaksi. Desain tampilan sederhana dengan kombinasi gradasi warna biru dan merah muda menjadikannya terlihat bersih, modern, dan mudah untuk digunakan. Di bagian utama terdapat ruang obrolan yang menampilkan pesan dalam bentuk terenkripsi dan hasil dekripsinya. Antarmuka aplikasi terlihat pada gambar 4. 2, menampilkan desain website yang sederhana namun tetap efisien dan menarik, sehingga memudahkan pengguna memahami proses enkripsi dan dekripsi RSA.

Uji Coba Aplikasi

Gambar 3. Hasil Uji Coba Aplikasi Berbasis Web Chat RSA.

Gambar 3 menunjukkan antarmuka aplikasi PROJECT MATEMATIKA DISKRIT yang dirancang sebagai alat pembelajaran interaktif untuk memahami mekanisme enkripsi pesan dengan menggunakan algoritma RSA. Dalam antarmuka ini, pengguna dapat mengisi nama, menyimpan data identitas, memilih penerima pesan (pengguna target), dan menghapus pencatatan percakapan sebelumnya. Selain itu, terdapat area untuk memasukkan pesan dan tombol Kirim yang digunakan untuk memulai proses komunikasi antar pengguna.

Dalam proses pengujian ini, terdapat pengguna yang bernama Maysi mengirimkan pesan teks *"Haii"* kepada Alya yang merupakan client**.** Sebelum pesan dikirim, sistem melakukan proses enkripsi dengan menggunakan kunci publik RSA. Hasil enkripsi tersebut berupa deretan angka atau *ciphertext* seperti berikut ; 7347,3641,4742,4742.

Proses Pembangkit Kunci

Pilih Prima ;

$$p = 101,\ q = 103$$

Hitung modulus ;

$$\begin{aligned} n &= p \times q \\ &= 101 \times 103 \\ &= 10403 \end{aligned}$$

Hitung totien Euler ;

$$\varphi(n) = (p-1)(q-1)$$

$$(p-1) = (101-1) = 100$$

$$(q-1) = (103-1) = 102$$

$$Maka, (p-1)(q-1) = 100 \times 102 = 10200$$

$$\varphi(n) = 10200$$

Hitung dan Pilih e ;

Ambil $e = 65537$

Sekarang $cek\ gcd(65537, 10200)$ menggunakan Algoritma Euclid :

- $65537 \div 10200 = 6$

Sisa: $65537 - (10200 \times 6) = 65537 - 61200 = 4337$

- $10200 \div 4337 = 2$

Sisa: $10200 - (4337 \times 2) = 10200 - 8674 = 1526$

- $4337 \div 1526 = 2$

Sisa: $4337 - (1526 \times 2) = 4337 - 3052 = 1285$

- $1526 \div 1285 = 1$

Sisa: $1526 - (1285 \times 1) = 1526 - 1285 = 241$

- $1285 \div 241 = 5$

Sisa: $1285 - (241 \times 5) = 1285 - 1205 = 80$

- $241 \div 80 = 3$

Sisa: $241 - (80 \times 3) = 241 - 240 = 1$

- $80 \div 1 = 80$

Sisa: $80 - (1 \times 80) = 0 \rightarrow$ Berhenti karena sisanya adalah 0.

Hitung d ;

$$d = \frac{1 + k\varphi(n)}{e}$$

$$k = 6020.0988\ldots\ Maka\ ;\ d = \frac{1 + 6020.0988\ldots x\ 10200}{65537}$$

$$= \frac{61405009}{65537}$$

$$= 937$$

Maka Hasilnya ;

Public key ; $(e, n) = (65537, 10403)$

Private key ; $(d, n) = (937, 10403)$

Proses Enkripsi	**Proses Deskripsi**
Rumus RSA Enkripsi: $c = m^e mod\ n$	Rumus RSA Deskripsi: $m = c^d mod\ n$
Plainteks: " Haii"	Ciphertext: [7347,3641,4742,4742]
Konversi ke kode ASCII	Konversi ke kode ASCII
$m = [72,97,105,105]$	$c = [7347,3641,4742,4742]$
$Blok\ 1: "H" \rightarrow 72 \rightarrow 7347$	$Blok\ 1: "7347" \rightarrow 72 \rightarrow H$
$Blok\ 2: "a" \rightarrow 97 \rightarrow 3641$	$Blok\ 2: "3641" \rightarrow 97 \rightarrow a$
$Blok\ 3: "i" \rightarrow 105 \rightarrow 4742$	$Blok\ 3: "4742" \rightarrow 105 \rightarrow i$
$Blok\ 4: "i" \rightarrow 105 \rightarrow 4742$	$Blok\ 4: "4742" \rightarrow 105 \rightarrow i$
Maka: $c = [7347,3641,4742,4742]$	Maka: $m =$ "Haii"

Deretan teks yang terenskripsi ini bertujuan untuk melindungi rahasia isi pesan agar tidak dapat diakses oleh orang lain tanpa kunci yang tepat. Setelah proses pengubahan menjadi kode selesai, pesan yang telah diubah ke dalam bentuk ciphertext kemudian dapat dipulihkan

kembali ke keadaan asalnya melalui langkah dekripsi dengan memanfaatkan kunci privat RSA. Hasil dari dekripsi itu kemudian ditampilkan dengan label ; [DECRYPTED] Haii

Berdasarkan hasil percobaan tersebut, dapat disimpulkan bahwa algoritma RSA telah diterapkan dengan baik dalam aplikasi web. Proses enkripsi dan dekripsi berjalan dengan baik, di mana pesan yang dikirim dapat diubah menjadi ciphertext dan dikembalikan lagi menjadi plaintext tanpa mengalami perubahan maupun kehilangan informasi. Aplikasi ini juga dirancang agar pengguna dapat memulihkan pesan asli (plaintext) hanya dengan satu klik, sehingga memudahkan dalam memahami alur konversi data dari teks menjadi ciphertext dan sebaliknya. Selain itu, tampilan antarmuka dilengkapi dengan penanda visual seperti panah dan keterangan di setiap tahap proses, yang membantu pengguna memahami mekanisme kerja algoritma RSA secara interaktif dan mudah dipahami.

Hasil Akhir Yang Diperoleh

Pesan Asli ; Haii

Hasil Enkripsi ; [7347,3641,4742,4742]

Hasil Deskripsi ; Haii

Dari penjelasan ini, terlihat bahwa terdapat kesamaan dalam hasil yang didapat, baik melalui perhitungan manual maupun menggunakan aplikasi web, hal ini menunjukkan bahwa sistem beroperasi dengan tepat dan stabil.

5. KESIMPULAN DAN SARAN

Berdasarkan hasil penelitian yang telah dilakukan, dapat disimpulkan bahwa penerapan algoritma kriptografi RSA mampu dilakukan secara efektif dalam melindungi pesan singkat dalam aplikasi chat berbasis web. Aplikasi yang dikembangkan menggunakan framework Flask, HTML, CSS, dan JavaScript ini dapat melakukan enkripsi dan dekripsi dengan baik, mengubah pesan plaintext (contohnya "Haii") menjadi ciphertext (seperti [7347,3641,4742,4 742]) dan mengembalikan pesan tersebut ke format aslinya tanpa kehilangan atau perubahan data. Sistem keamanan ini bergantung pada kesulitan pemfaktoran bilangan prima yang besar, di mana kunci publik (e, n) berfungsi untuk enkripsi dan kunci privat (d, n) untuk dekripsi. Uji coba menunjukkan adanya konsistensi antara perhitungan manual dan fungsi aplikasi, membuktikan bahwa sistem ini beroperasi dengan stabil dan akurat. Dengan tampilan yang interaktif dan menarik, aplikasi ini tidak hanya berperan sebagai sarana komunikasi yang aman, tetapi juga sebagai alat pembelajaran yang efektif untuk memahami konsep dasar kriptografi asimetris seperti RSA.

Untuk pengembangan selanjutnya, disarankan agar riset ini ditingkatkan dengan memakai bilangan prima yang lebih besar guna memperkuat tingkat keamanan, mengingat kekuatan RSA sangat bergantung pada kompleksitas dalam memfaktorkan bilangan tersebut. Selain itu, perlu dilakukan evaluasi keamanan yang lebih menyeluruh, seperti pengujian serangan brute-force, untuk menilai ketahanan sistem. Dari sisi fungsi, penambahan fitur-fitur seperti pengiriman file, obrolan grup, dan mekanisme pertukaran kunci yang lebih fleksibel akan menjadikan aplikasi ini lebih menarik dan sebanding dengan aplikasi chatting lainnya. Di samping itu, pengembangan aplikasi versi mobile dan penggabungan dengan metode kriptografi hibrida (yang mencampurkan algoritma simetris dan asimetris) bisa menjadi langkah inovasi berikutnya untuk meningkatkan kinerja dan keamanan secara keseluruhan.

DAFTAR REFERENSI

Arief, A., & Saputra, R. (2016). Implementasi kriptografi kunci publik dengan algoritma RSA-CRT pada aplikasi instant messaging. *Scientific Journal of Informatics, 3*(1), 46–54. https://doi.org/10.15294/sji.v3i1.6115

Arief, M., & Ikhsan, N. (2015). Kriptografi RSA pada aplikasi file transfer client-server based. *Jurnal Ilmiah Teknologi Informasi Terapan, 1*(3), 3–7.

Dairi, M. S., Setiani Asih, M., & (author correspondent). (2022). Implementasi algoritma kriptografi RSA dalam aplikasi sistem informasi perpustakaan. *Jurnal Ilmiah Riset Sistem Informasi, 2023*(2), 98–107. https://jurnal.unity-academy.sch.id/index.php/jirsi/index

Fajrin, A. M., Kelvin, C., Owen, B., & Aji, B. (2024). Perbandingan performa dari algoritma AES dan RSA dalam keamanan transaksi. *KESATRIA: Jurnal Penerapan Sistem Informasi, 5*(2), 696–705.

Hidayat, M., Tahir, M., Sukriyadi, A., Sulton, A., A. C. A. S., & F. S. A. (2023). Penerapan kriptografi Caesar cipher dalam pengamanan data. *Jurnal Ilmiah Multidisiplin, 2*(03), 35–41. https://doi.org/10.56127/jukim.v2i03.619

Iii, B. A. B., Penelitian, M., Westerdal, M., Rights, A., Copyright, I., Alam, H., Pasaribu, K. M., Saragi, D. R., Gultom, J. M., ..., & Febrianto, A. (2019). Perbandingan efisiensi algoritma RSA dan RSA-CRT. *Jurnal Informatika, 1*(2), 1689–1699. http://e-jurnal.pelitanusantara.ac.id/index.php/mantik/article/view/253

Informasi, S., Pamulang, U., Raya, J., Serpong, P., & Tangerang, N. (2023). Untuk pesan rahasia berbasis web. *Jurnal Sistem Informasi*, *6*(03), 50–54.

Nanda, N. A., Silalahi, S. M. S., Nasution, D. F., Sari, M., & Gunawan, I. (2023). Kriptografi dan penerapannya dalam sistem keamanan data. *Jurnal Media Informatika, 4*(2), 90–93. https://doi.org/10.55338/jumin.v4i2.428

Nurul, S., Anggrainy, S., & Aprelyani, S. (2022). Faktor-faktor yang mempengaruhi keamanan sistem informasi: Keamanan informasi, teknologi informasi, dan network (literature review SIM). *Jurnal Ekonomi Manajemen Sistem Informasi, 3*(5), 564–573. https://doi.org/10.31933/jemsi.v3i5.992

Ramadhan, A. A. I., Rivanti, E. Z., & Zulva, R. S. (2023). Implementasi kriptografi AES menggunakan bahasa Java programming: Meningkatkan keamanan data melalui enkripsi & dekripsi yang kuat. *Jurnal Pendidikan Teknologi Informasi*, 20–26. https://jurnal.umj.ac.id/index.php/TripleA/article/view/17513

Sari, M., Purnomo, H. D., & Sembiring, I. (2022). Review: Algoritma kriptografi sistem keamanan SMS di Android. *Journal of Information Technology, 2*(1), 11–15. https://doi.org/10.46229/jifotech.v2i1.292

Siregar, S. J., Nugroho, N. B., & Sigalingging, H. (2023). Implementasi algoritma kriptografi RSA (Rivest Shamir Adleman) dalam pengamanan data gaji karyawan di kantor BSPJI. *SAINTIKOM: Jurnal Sains Manajemen Informatika dan Komputer, 22*(2), 528. https://doi.org/10.53513/jis.v22i2.9409

Studi Teknik Informatika, P., & Korespondensi, P. (2022). Penerapan kriptografi menggunakan algoritma DES (Data Encryption Standard). *Jurnal Sintaks Logika, 2*(2), 9–19. https://jurnal.umpar.ac.id/index.php/sylog

Sulaiman, R., & Vebu, M. (2018). Peningkatan keamanan pesan berbasis Android menggunakan algoritma kriptografi RSA. *Jurnal Sisfokom (Sistem Informasi dan Komputer), 7*(2), 116–120. https://doi.org/10.32736/sisfokom.v7i2.574

Sulaksono, D. H., Prabiantissa, C. N., Yuliastuti, G. E., Taqwa, A. R., Informatika, T., Elektro, T., Informasi, T., Adhi, T., & Surabaya, T. (2021). Implementasi kriptografi dengan metode Elliptic Curve Cryptography (ECC) untuk aplikasi chatting berbasis Android. *Prosiding Teknologi Informasi*, 570.