

## Implementasi Metode Rivest Shamir Adleman untuk Enkripsi dan Dekripsi Text

Fatonah<sup>1</sup>, Dadang Iskandar Mulyana<sup>2</sup>, Anissa Pramudyah Heryani<sup>3</sup>, Virginia Khoirunnisa<sup>4</sup>  
<sup>1,2,3,4</sup>Sistem Informasi, Sekolah Tinggi Ilmu Komputer Cipta Karya Informatika

<sup>1</sup>fatolahapril4@gmail.com \*, <sup>2</sup>mahvin2012@gmail.com, <sup>3</sup>anissaph1810@gmail.com, <sup>4</sup>ginnyvirginia67@gmail.com

### Abstract

*Until now information technology is developing rapidly, resulting in a lot of information that is easily stolen because of increasingly sophisticated technology. For this reason, a program is needed to secure the confidentiality of information so that it is not easily read. Cryptography is one of the solutions developed to maintain the confidentiality of the information. In cryptography, there is a process where the information sent will be encoded which can be called encryption, then returned to the original information called decryption. Many techniques are owned by cryptography, one of which is a technique that has security that is difficult to solve, namely the RSA algorithm. In its application, the RSA cryptography method will create a program that can encrypt and decrypt text, and it is necessary to pay attention to the selection of prime numbers and the key generation process so that there is no attack on the RSA cryptography algorithm. The purpose of this is to ensure that the information sent reaches the recipient safely. Other people will find it difficult to read the information sent because it uses a code that is difficult to crack.*

*Keywords: RSA, Cryptography, Encryption, Decryption, Text*

### Abstrak

Sampai saat ini teknologi informasi berkembang dengan pesat, mengakibatkan banyak sekali informasi yang mudah dicuri karena semakin canggihnya teknologi. Untuk itu dibutuhkan suatu program untuk mengamankan kerahasiaan suatu informasi agar tidak mudah terbaca. Kriptografi adalah salah satu solusi yang dikembangkan untuk menjaga kerahasiaan informasi tersebut. Pada kriptografi, terdapat proses dimana informasi yang dikirimkan akan disandikan bisa disebut dengan enkripsi, lalu dikembalikan lagi ke informasi semula di sebut dekripsi. Banyak teknik yang di miliki kriptografi, salah satunya yaitu teknik yang memiliki keamanan sulit untuk di pecahkan yaitu algoritma RSA. Dalam penerapannya, kriptografi metode RSA ini akan dibuat suatu program yang dapat mengenkripsi dan mendekripsi teks, dan perlu diperhatikan dalam pemilihan bilangan prima dan proses pembangkitan kunci agar tidak terjadi serangan terhadap algoritma kriptografi RSA. Tujuan ini yaitu untuk memastikan agar informasi yang dikirim sampai kepada penerima dengan aman. Orang lain akan sulit membaca informasi yang dikirim karena menggunakan kode yang susah dipecahkan.

Kata kunci: RSA, Kriptografi, Enkripsi, Dekripsi, Teks

### 1. Pendahuluan

Masalah keamanan yaitu salah satu hal yang sangat penting dari sebuah sistem informasi. Membahas tentang keamanan, keamanan merupakan kondisi atau keadaan bebas dari suatu bahaya. Disetiap harinya kebutuhan pertukaran data semakin besar, diharapkan setiap transaksinya memiliki keamanan agar data tersebut tetap terjaga kerahasiannya. Untuk itu kemudian dikembangkanlah sistem keamanan pada sebuah jaringan komputer. Salah satu sistem keamanan yang banyak digunakan ialah kriptografi.

Didalam kriptografi, terdapat suatu proses dimana data atau informasi yang dikirimkan akan disandikan (enkripsi dan dekripsi). Enkripsi ini dilakukan saat informasi akan dikirimkan dengan disandikan sehingga informasi tersebut akan sulit terbaca. Dekripsi dilakukan saat penerimaan informasi dengan cara mengubah kembali menjadi bentuk aslinya. Proses Dekripsi tersebut hanya bisa dilakukan oleh penerima dengan menggunakan kunci rahasia yang telah disepakati bersama sebelumnya.

Umumnya kriptografi bisa diartikan dengan suatu proses penyampaian informasi atau pesan secara tersembunyi

dan rahasia. Akan tetapi jika dikaitkan dengan penerapan teknologi digital, kriptografi merupakan teknik yang mempelajari tentang cara mengenkripsikan suatu informasi asli (plaintext) yang di susun dengan acak menggunakan kunci enkripsi sehingga sangat sulit untuk di baca (ciphertext) oleh penerima yang tidak mempunyai kunci dekripsinya. Tujuan dari kriptografi ini sendiri ialah untuk mengamankan layanan suatu informasi yang memiliki aspek kerahasiaan yang ditujukan untuk menjaga agar informasi tersebut tidak dapat dibaca oleh pihak-pihak yang tidak berwenang.

Kriptografi ialah ilmu yang mempelajari teknik matematika yang memiliki kaitan dengan aspek keamanan data dan informasi seperti validitas data, otentikasi data serta integritas data. Sistem kriptografi merupakan sebuah fasilitas untuk mengubah pesan teks asli (plainteks) menjadi pesan terenkripsi (cipherteks). Proses konversi ini disebut enkripsi (encryption). Di sisi lain, mengubah ciphertext menjadi plaintext disebut dekripsi (decryption). Proses enkripsi juga dekripsi dapat menggunakan satu atau beberapa kunci kriptografi [1]. Sistem kriptografi ini sangat bagus karena berada dalam kerahasiaan kunci, bukan ada pada kerahasiaan algoritma yang digunakan [2].

Berdasarkan waktu kemunculannya, kriptografi dibagi dalam dua bidang, yakni kriptografi klasik dan modern. Di kriptografi klasik, proses enkripsinya menggunakan perhitungan sederhana dan dapat dilakukan secara manual. Berbeda dengan kriptografi modern, proses enkripsi membutuhkan bantuan komputer karena proses enkripsi kompleks dan membutuhkan jumlah bilangan yang banyak [3].

Berdasarkan kuncinya, algoritma kriptografi ini dibagi menjadi tiga jenis, yakni kriptografi simetris, asimetris dan hybrid. Algoritma kriptografi simetris menggunakan kunci yang sama disebut kunci privat, dan dapat dilakukan dengan cara berikut: Advanced Encryption Standard (AES), One Time Pad (OTP), Data Encryption Standard (DES), Riverst Cipher 4 (RC4), Blowfish dan lainnya. Ini akan dikonfigurasi. Lalu kriptografi asimetris menggunakan kunci publik dan privat untuk melindungi data, contohnya algoritma RSA (Rivest Shamir Adleman), Diffie Hellman, Elliptic Curve, Hill Cipher, Diffie Hellman, El Gamal dan lainnya. Enkripsi hibrida menggunakan dua lapisan kunci: kunci rahasia (simetris) untuk enkripsi data (juga dikenal sebagai kunci sesi) dan pasangan kunci publik rahasia untuk melindungi kunci simetris [4].

Kemudian berdasarkan dari kunci untuk enkripsi dekripsi, kriptografi dibagi kedalam dua kunci yang termasuk kriptografi modern, yaitu kriptografi kunci simetri dan kriptografi kunci nirsimetri [5]

Sangat banyak data-data yang harus diamankan dari pihak ketiga, sebab data itu adalah data privasi atau rahasia yang penting. Data-data sangat mudah diketahui apabila dalam bentuk fisik. Data-data bisa jaga

keamanannya dengan melakukan enkripsi lalu bisa buka kembali dengan melakukan dekripsi. Pengamanan data teks dengan menggunakan teknik kriptografi ini telah banyak dilakukan dalam berbagai penelitian.

Metode RSA merupakan algoritma yang paling umum digunakan, dan algoritma RSA sangat aman karena memfaktorkan bilangan yang besar. Algoritma RSA mulai dikembangkan pada tahun 1976 oleh Ron Rivest, Adi Shamir dan Leonard Adleman. Mengenkripsi dan mendekripsi pesan menggunakan kunci privat dan publik. Salah satu kelebihan dari algoritma RSA adalah sulitnya memfaktorkan bilangan yang besar menjadi faktor prima [6]. Sejauh ini algoritma RSA memiliki tingkat keamanan yang cukup tinggi karena belum ditemukan mesin/ metode lain yang dapat dengan cepat mendekripsi data terenkripsi dari algoritma enkripsi tersebut. Panjang kunci dapat menentukan kerumitan dan kesulitan dalam penguraian sandinya. Semakin panjang bit, semakin sulit untuk diselesaikan, karena sulit untuk memfaktorkan dua bilangan prima acak yang dipilih untuk menghasilkan kunci.

Mekanisme operasi RSA sangat mudah dipahami dan sederhana, tetapi kuat. Sejauh ini, satu-satunya cara untuk memecahkannya yaitu dengan mencoba setiap kombinasi kunci yang mungkin atau yang biasa dikenal dengan serangan brute force. Lalu panjang (ukuran kunci) kata sandi yang menentukan tingkat keamanan kata sandi berdasarkan kemungkinannya untuk diretas. Kombinasi kunci yang mungkin ada akan semakin banyak jika kodenya semakin panjang [7].

Dalam penelitian ini dilakukan suatu implementasi metode RSA dari sistem kriptografi berbasis komputer dengan membuat suatu aplikasi yang dimana hasil implementasi adalah dapat merahasiakan sebuah teks kedalam bentuk sandi, pengkodean atau teks acak yang dienkripsi terlebih dahulu, sehingga dalam proses pengiriman informasi tersebut, teks sebenarnya tidak dapat dibaca. Kemudian Informasi tersebut akan terbaca jika melalui proses yang namanya dekripsi.

Dari latar yang telah di jabarkan diatas, penulis telah mengumpulkan dan menyimak dari beberapa referensi jurnal yang berkaitan dengan penelitian ini. Untuk itu penulis bermaksud mengajukan judul penelitian yang berjudul "Implementasi Metode Rivest Shamir Adleman untuk Enkripsi dan Dekripsi Text". Selanjutnya, Adapun tujuan dari penelitian ini akan diuraikan dalam pokok-pokok sebagai berikut:

- a. Mengetahui apa itu kriptografi.
- b. Mengetahui proses enkripsi dan dekripsi dengan menggunakan Metode Rivest Shamir Adleman (RSA).
- c. Dapat merancang dan menggunakan sebuah program pengamanan data teks yang berbentuk aplikasi dengan metode RSA.

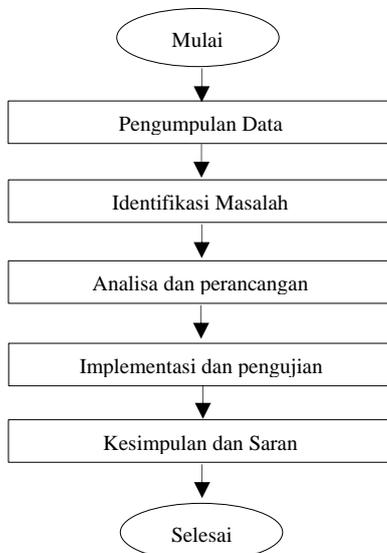
Harapan yang ingin dicapai dari penelitian ini yaitu bisa dijadikan sebagai bahan referensi mengenai cara pengamanan informasi menggunakan Metode Rivest Shamir Adleman (RSA) dan dapat menghasilkan sebuah perangkat lunak atau aplikasi yang dapat membantu mengamankan suatu teks rahasia.

## 2. Metode Penelitian

Keamanan data adalah hal yang sangat dibutuhkan dan amat penting dalam organisasi apapun, upaya untuk menjaga kerahasiaan data dari orang lain. Metode kriptografi RSA merupakan solusi yang banyak digunakan dalam penanganannya.

### 2.1. Tahapan Penelitian

Tahapan penelitian merupakan tahapan, langkah atau gambaran yang akan digunakan untuk membuat alur pembuatan penelitian ini, mulai dari mengidentifikasi masalah hingga implementasi sampai dengan selesai. Prosedur penelitian ini digambarkan pada diagram dibawah ini:



Gambar 1. Skema tahapan penelitian

Gambar 1 adalah gambar skema tahapan penelitian yang akan dilakukan oleh penulis pada penelitian ini. Tahapan penelitian memiliki tujuan untuk memberikan gambaran atau uraian seluruh kegiatan yang dilaksanakan selama kegiatan penelitian berlangsung.

Gambaran dari program aplikasi yang akan dirancang nantinya akan memiliki prosedur kerja sebagai berikut, yang pertama dilakukan yaitu pembangkitan sepasang kunci, kemudian melakukan proses enkripsi dan langkah terakhir yaitu melakukan proses dekripsi. Jadi ada tiga tahapan yang akan dilakukan penulis untuk menyelesaikan kasus pada penelitian ini yang meliputi: identifikasi masalah, pengumpulan data, analisa dan perancangan, implementasi dan pengujian, selanjutnya adalah kesimpulan dan saran.

### 2.2. Identifikasi Masalah

Identifikasi masalah merupakan tahapan atau langkah awal yang penting dalam melakukan proses penelitian. Proses identifikasi masalah yaitu dengan survey literatur dimana metode ini akan dilakukan dengan melakukan pengumpulan bahan literatur dan informasi berkaitan dengan judul penelitian. Kemudian mengembangkan ide-ide melalui diskusi, dan yang terakhir menyusun ulang masalah penelitian. Identifikasi masalah dapat memperjelas masalah sehingga memudahkan dalam menyelesaikan penelitiannya [8].

Dalam penelitian ini masalah yang dibahas adalah berkaitan dengan pengamanan data teks. Banyak sekali terjadinya pencurian data, baik itu data yang bernilai pribadi atau data penting lainnya, yang mana tindakan itu bisa menimbulkan kerugian dari sisi pemilik data. Penyebab terjadinya hal ini yaitu tidak adanya pengamanan pada data yang disimpan. Akibatnya, orang yang tidak bertanggung jawab dapat dengan mudah mencuri atau merusak data. Untuk mencegah hal-hal yang tidak diinginkan, maka program keamananlah yang sangat dibutuhkan untuk menjaga kerahasiaan setiap datanya.

Berdasarkan permasalahan tersebut, maka solusi yang di ambil untuk menjaga keamanan data text diatas yaitu dibuatlah program aplikasi metode kriptografi RSA, yang memiliki fungsi untuk menjaga data text tetap aman dan juga agar tidak ada pihak luar yang mengetahui isi text tersebut.

### 2.3. Pengumpulan Data

Pengumpulan data merupakan suatu aktivitas yang dilakukan untuk mencari informasi yang diperlukan dalam rangka mencapai tujuan penelitian. Penelitian dilakukan dengan menggunakan beberapa metode yakni mempelajari beberapa referensi buku dan situs internet yang berkaitan dengan topik yang dibahas. Selanjutnya, akan didiskusikan hasil analisis data yang diperoleh dari hasil pencarian literatur dengan dosen pembimbing untuk memecahkan masalah yang sulit. Informasi data yang sangat dibutuhkan pada penelitian ini antara lain teori-teori yang berkaitan dengan pengamanan data menggunakan metode kriptografi RSA.

Metode pengumpulan data yang digunakan untuk memperoleh data yaitu dengan cara studi literatur. Studi literatur merupakan kegiatan yang dilakukan oleh peneliti untuk mengumpulkan data dengan cara membaca, mencatat dan mengelolanya. Studi literatur memiliki tujuan untuk mengumpulkan dan mengelola data untuk penelitian dari referensi-referensi yang diperlukan. Biasanya referensi di dapat dari jurnal, artiket, buku-buku, dan dari internet.

### 2.4. Analisa dan Perancangan

Dalam tahap analisa dan perancangan ini akan digunakan untuk mengelola data dari hasil studi literatur

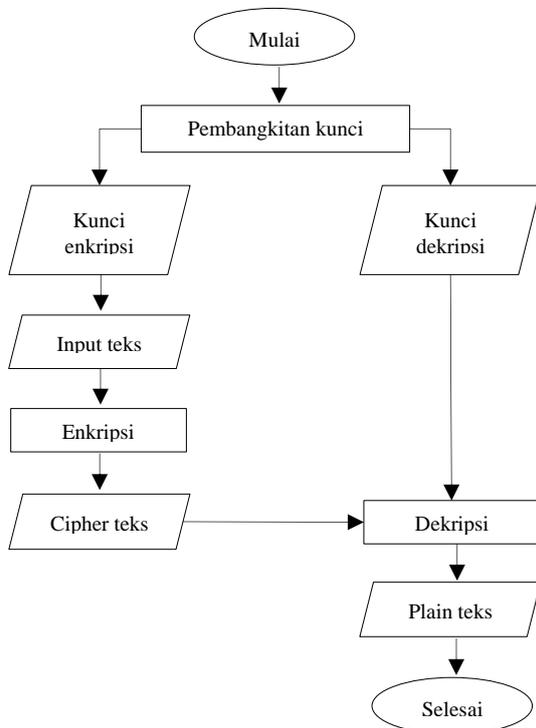
lanjut untuk melakukan analisis sehingga menjadi suatu informasi. Tahap ini mencakup pembuatan algoritma program, flowchart program, perancangan program aplikasi, serta pembuatan program aplikasi. Program yang di analisa ini memiliki tujuan agar teks yang akan di rahasiakan tidak dapat terbaca oleh orang yang tidak berwenang.

Metode RSA memiliki tiga proses: pembangkitan kunci, lalu proses enkripsi, dan terakhir proses dekripsi. Kesulitan dengan metode ini adalah menemukan dua elemen prima yang besar untuk digunakan sebagai kunci privat dan kunci publik.  $p$  dan  $q$  adalah dua bilangan prima besarnya, dimana  $p \neq q$  [9].

Keamanan algoritma RSA terletak pada sulitnya memfaktorkan nilai non prima yang akan menjadi faktor prima, dalam hal ini  $n = p \times q$ , ketika  $n$  difaktorkan menjadi  $p$  dan  $q$ , kita dapat menghitung  $\phi(n) = (p - 1) (q - 1)$ . Juga, kunci enkripsi  $e$  bersifat publik (bukan rahasia), sehingga kunci dekripsi  $d$  dapat dihitung dari persamaan berikut [10]:

$$m_i = c_i^d \text{ mod } n$$

Program yang akan dianalisis dan dirancang secara garis besar akan berjalan seperti:



Gambar 2. Flowchart alur algoritma RSA

### 2.5. Implementasi dan Pengujian

Pengembangan dari tahap perancangan sistem merupakan implementasi sistem. prosedur ini adalah yang paling penting sebab membutuhkan implementasi dari sistem yang dirancang [11]. Setelah perancangan sistem dan desain kemudian di bangun aplikasi yang merupakan perwujudan dari rancangan tersebut, untuk

melakukan pengujian aplikasi tersebut berjalan sesuai rancangan atau tidaknya, maka dilakukan percobaan. Dengan melakukan pembangkitan kunci, langkah selanjutnya melakukan enkripsi dan langkah terakhir melakukan proses dekripsi.

### 3. Hasil dan Pembahasan

Di era teknologi informasi saat ini, data menjadi pertimbangan penting bagi pengolah data informasi agar tidak disalahgunakan oleh pihak-pihak tertentu yang tidak bertanggung jawab. Untuk itu, dibutuhkan suatu sistem untuk mengamankan data - data penting dan rahasia. Pengamanan data tersebut akan dilakukan menggunakan metode RSA. Beberapa analisa kebutuhan sistem yaitu sebagai berikut:

- Program yang dirancang dan dibuat ini memiliki fungsi untuk menjaga kerahasiaan teks
- Program ini dapat memberikan layanan proses enkripsi yaitu pengacakan isi teks
- Program ini dapat memberikan layanan proses dekripsi yaitu mengubah isi teks seperti semula

Metode Rivest Shamir Adleman merupakan metode yang mempunyai di kunci yang berbeda (kunci enkripsi dan dekripsi). Metode RSA ini dikenal sebagai salah satu metode kriptografi yang menggunakan konsep kriptografi kunci publik. Terdapat beberapa properti dalam metode RSA yaitu:

Tabel 1. Properti metode RSA

Properti yang ada pada metode RSA	
$p$ dan $q$ bilangan prima	rahasia
$n = p \times q$	tidak rahasia
$\phi(n) = (p-1) \times (q-1)$	rahasia
$e$ (kunci enkripsi)	tidak rahasia
$d$ (kunci dekripsi)	rahasia
$m$ (plainteks)	rahasia
$c$ (cipherteks)	tidak rahasia

Algoritma RSA terdiri dari 3 proses, yaitu [12]:

#### a. Pembangkit Kunci

Proses pembangkitan kunci algoritma RSA yaitu :

- Pilih dua bilangan prima,  $p$  dan  $q$
- Hitung  $n = p * q$  (sebaiknya  $p \neq q$ )
- Hitung  $\phi(n) = (p - 1) (q - 1)$
- Pilih kunci publik  $e$ , yang relatif prima terhadap  $\phi(n)$
- Bangkitkan kunci dekripsi  $d$ , dengan menggunakan persamaan  $ed \equiv 1 \pmod{\phi(n)}$

Terdapat bilangan bulat  $k$  yang memberikan bilangan bulat  $d$ . Hasil dari algoritme di atas: Kunci publik adalah pasangan  $(e, n)$ , Kunci privat adalah pasangan  $(d, n)$ .

b. Enkripsi

Langkah-langkah dalam mengenkripsi teks

1. Ambil kunci publik penerima pesan, e, dan modulus n.
2. Nyatakan plainteks m menjadi blok-blok  $m_1, m_2, m_3, \dots$ , (syarat:  $0 < m_i < n - 1$ )
3. Setiap blok  $m_i$  dienkripsi menjadi blok  $c_i$  dengan rumus:  

$$c_i = m_i^e \text{ mod } n$$

c. Dekripsi

Setiap blok ciphertext  $c_i$  didekripsi kembali menjadi blok  $m_i$  dengan rumus:

$$m_i = c_i^d \text{ mod } n$$

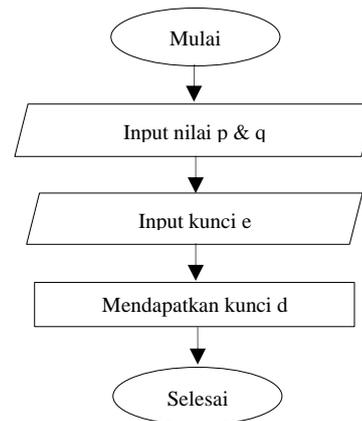
3.1. Perancangan Sistem

Perancangan sistem merupakan aktivitas untuk merancang dan mendesain rincian sistem yang sudah dianalisis. Pada perancangan sistem ini akan dilakukan analisa sistem dan analisa desain tampilan sistem. Tujuan dari perancangan sistem yaitu untuk menggambarkan bagaimana aplikasi yang dirancang akan berjalan. Berdasarkan hasil analisis diatas maka akan dibuat sebuah program dengan menggunakan metode kriptografi RSA. Pada metode RSA ini terdapat tiga tahapan atau proses yaitu, tahap pertama adalah pembangkitan sepasang kunci, kemudian tahap kedua yaitu proses enkripsi dan tahap ketiga atau terakhir yaitu proses dekripsi.

3.1.1. Pembangkitan Kunci

Pembangkitan kunci merupakan proses tahap awal dalam metode kriptografi RSA (Rivest Shamir Adleman). Metode kriptografi RSA menggunakan kunci asimetris, pada proses enkripsi menggunakan kunci publik sedangkan pada proses dekripsi menggunakan kunci privat. Proses pembangkitan kunci adalah tahap pertama yang dilakukan, dengan cara masukan nilai p, masukan nilai q dan masukan kunci enkripsi dengan bentuk bilangan prima yang akan di hitung kuncinya. Dimana nilai dari p dan q ini akan menjadi sebuah nilai dari nilai n dan  $\phi(n)$ , lalu nilai dari kunci enkripsi akan berfungsi sebagai nilai publik.

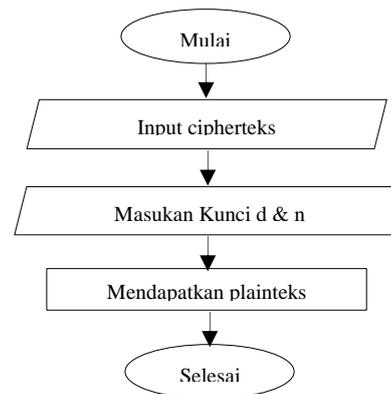
Pembangkitan kunci dilakukan dengan menggunakan bilangan prima. Bilangan prima ialah bilangan yang memiliki dua faktor untuk membaginya antara lain angka satu dan bilangan itu sendiri, bilangan ini lebih besar dari angka satu. Contoh dari bilangan prima yaitu: 2, 3, 5, 7, 11, 13, 17, 19 dan lainnya. Berikut alur kerja dari pembangkitan kunci :



Gambar 3. Flowchart pembangkitan kunci

3.1.2. Proses Enkripsi

Proses enkripsi merupakan proses dimana suatu data teks akan disandikan agar tidak terbaca dengan cara diacak. Enkripsi dilakukan setelah dilakukannya pembangkitan kunci yang akan mendapatkan kunci privat (kunci yang tidak boleh diberitahukan pada orang lain) dan kunci publik (kunci yang boleh diberitahukan pada orang lain). Lalu dilakukanlah pertukaran kunci antara penerima dan pengirim pesan teks, setelah itu maka dilakukan enkripsi teks. Pesan yang akan dienkripsi berupa teks. Bisa dilihat pada gambar 4 dibawah, itu adalah alur kerja dari proses enkripsi.

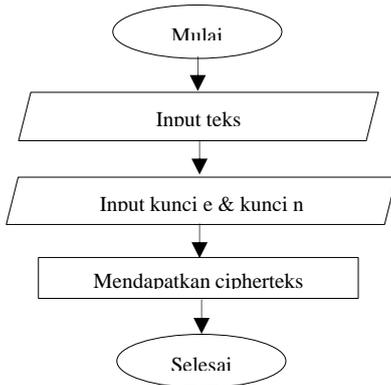


Gambar 4. Flowchart proses enkripsi

3.1.2. Proses Dekripsi

Sebelum melakukan proses dekripsi, penerima pesan harus ingat sebelumnya kunci yang telah di tentukan antara pengirim dan penerima pesan. Proses dekripsi dilakukan untuk mengubah pesan teks yang telah di acak tersebut sehingga kembali ke bentuk teks semula, agar bisa di baca oleh si penerima. Dalam proses dekripsi ini, apabila kunci yang di masukan salah maka proses dekripsi tidak akan berhasil dilakukan.

Berikut gambar dari alur kerja proses dekripsi:

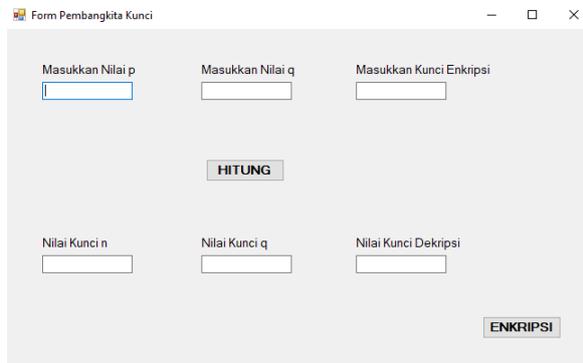


Gambar 5. Flowchart proses dekripsi

### 3.2. Implementasi dan Pengujian Sistem

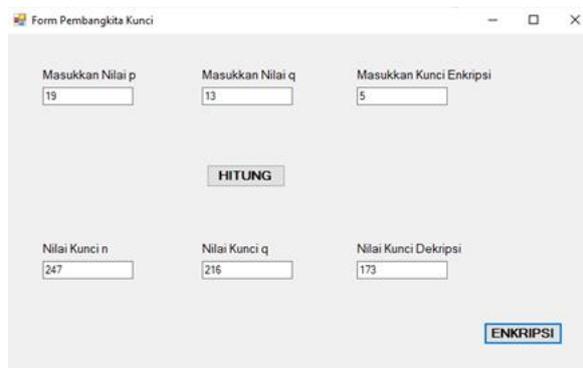
Sistem ini berjalan pada laptop dengan sistem operasi Windows 10. Proses implementasi sistem yang terjadi di dalam aplikasi yang dirancang dibagi menjadi tiga, yaitu: proses pembangkitan kunci, proses enkripsi dan langkah terakhir yaitu melakukan proses dekripsi.

#### a. Tampilan proses pembangkitan sepasang kunci



Gambar 6. Tampilan proses pembangkitan kunci

Pada Gambar 6 merupakan gambar tampilan dari pembangkitan kunci, dari tampilan tersebut terdapat beberapa nilai yang harus diisi dengan bilangan prima. Yang harus diisi adalah nilai p, q, dan kunci enkripsi, dimana nilai  $p > q >$  kunci e.



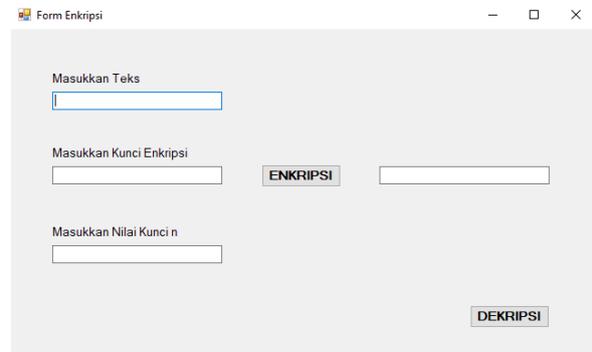
Gambar 7. Tampilan uji coba pembangkitan kunci

Kemudian dilakukan pengujian seperti pada Gambar 7 pengujian yang dilakukan yaitu dengan mengisi nilai

$p = 19$ , nilai  $q = 13$  dan nilai kunci enkripsi = 5, kemudian jika di klik button HITUNG maka akan menghasilkan nilai kunci  $n = 247$ , nilai kunci  $q = 216$  dan nilai kunci dekripsi = 173.

Setelah selesai melakukan pembangkitan kunci selanjutnya melakukan proses enkripsi dengan cara mengklik button ENKRIPSI yang ada di kanan bawah aplikasi. Setelah itu akan di arahkan ke tampilan untuk enkripsi seperti pada gambar dibawah.

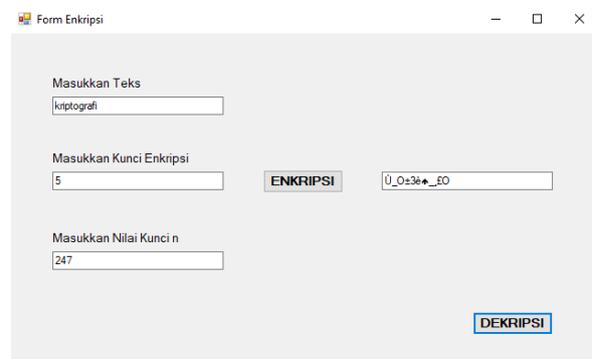
#### b. Tampilan proses enkripsi



Gambar 8. Tampilan proses enkripsi

Setelah dilakukan proses pembangkitan kunci maka akan mendapatkan kunci publik dan kunci privat guna melanjutkan ke proses enkripsi dan dekripsi. Sebaiknya harus di hafalkan nilai kunci yang telah di buat di pembangkitan kunci agar tidak terjadi kesalahan pada proses enkripsi dan dekripsinya. Setelah mengklik button ENKRIPSI maka akan muncul tampilan pada Gambar 8.

Proses enkripsi data adalah langkah pertama dari proses melindungi file dalam aplikasi ini. Metode enkripsi ini menggunakan algoritma yang ditentukan untuk mengacak data asli . Untuk memprosesnya anda harus mengisikan teks yang akan di enkripsikan, isikan kunci enkripsi dan nilai kunci n. Nilai kunci enkripsi dan nilai kunci n harus diisi sesuai dengan nilai pada saat melakukan pembangkitan kunci.



Gambar 9. Tampilan uji coba proses enkripsi

Dilakukan uji coba (silahkan lihat pada Gambar 9) di sini penulis akan mengisikan teks = kriptografi, kunci enkripsi = 5, nilai kunci n = 247. Setelah semua data terisi silahkan klik button ENKRIPSI maka akan



- [7] Android,” *J. CKI SPOT*, vol. 9, no. 2, pp. 105–114, 2016.  
H. N. Octafiani and A. Rosita, “MENGUNAKAN METODE RIVEST SHAMIR,” vol. 8, no. 1, pp. 72–77, [11] 2021.
- [8] A. Azizah, F. Fauziah, and N. Hayati, “uSocial Realtime Berbasis Android Menggunakan Volley dan Algoritma BruteForce,” *STRING (Satuan Tulisan Ris. dan Inov. Teknol.*, vol. 5, no. 2, p. 171, 2020, doi: 10.30998/string.v5i2.7751.
- [9] L. Benny, “Analisis Dan Perancangan Aplikasi Kriptografi Keamanan File Berbasis Teks Dengan Menggunakan Metode Rsa,” *Ris. dan E-Jurnal Manaj. Inform. Komput.*, vol. 1, no. April P-ISSN : 2541-1322, pp. 15–23, 2017, [Online]. Available: <http://jurnal.polgan.ac.id/index.php/remik/article/view/10116>.
- [10] A. Rahim, “Implementasi Algoritma Rsa Pada Sistem Pendukung Keputusan Pengalokasian Dana Bantuan Langsung Masyarakat Dengan Metode Weighted Product (Studi Kasus Desa Beka Kecamatan Marawola Kabupaten Sigi),” *J. Ilmu Komput.*, vol. 12, no. 1, p. 16, 2019, doi: 10.24843/jik.2019.v12.i01.p01.
- S. Sutejo, “Implementasi Algoritma Kriptografi Rsa (RiSutejo, S. (2021). Implementasi Algoritma Kriptografi Rsa (Rivest Shamir Adleman) Untuk Keamanan Data Rekam Medis Pasien. INTECOMS: Journal of Information Technology and Computer Science, 4(1), 104–114. <https://doi.org/10.31539/intecom.v4i1.2437>.” *INTECOMS J. Inf. Technol. Comput. Sci.*, vol. 4, no. 1, pp. 104–114, 2021, doi: 10.31539/intecom.v4i1.2437.
- S. I. Febriani, S. Juanita, and M. Hardjianto, “Implementasi Kriptografi Teks pada SMS Menggunakan Algoritme Multiple Encryption dengan Metode RSA dan 3DES,” *J. Telemat. Inst. Teknol. Harapan Bangsa, Bandung*, vol. 15, no. 2, pp. 77–84, 2020.