Terbit *online* pada laman : https://ejournal.seminar-id.com/index.php/bees

**BEES: Bulletin of Electrical and Electronics Engineering**

ISSN 2722-6522 (Media Online), Vol 2, No 1, July 2021, pp 35-39

# Implementasi Algoritma RSA Untuk Keamanan Data Kredit di PT Bank Perkreditan Rakyat Solider Pematangsiantar

**Ferdinal Rahmad Gea[1,*], Sumarno[1], Zulaini Masruro Nasution[2], Dedy Hartama[1], Jalaluddin[2]**

[1] STIKOM Tunas Bangsa, Pematangsiantar, Indonesia
[2] AMIK Tunas Bangsa, Pematangsiantar, Indonesia
Email: [1,*]ferdinalrahmat11@gmail.com, [2]sumarno@gmail.com, [3]zulaini@amiktunasbangsa.ac.id, [4]dedyhartama@amiktunasbangsa.ac.id, [5]jalaluddin@amiktunasbangsa.ac.id

INFORMASI ARTIKEL

Article History
Received : Jul 13, 2021
Accepted : Jul 26, 2021
Published : Jul 27, 2021

KORESPONDENSI

Email: ferdinalrahmat11@gmail.com

**A B S T R A K**

Bank adalah sebuah badan usaha yang menghimpun dana dari masyarakat dalam bentuk simpanan dan menyalurkannya kepada masyarakat dalam bentuk kredit. PT.Bank Perkreditan Rakyat Solider memiliki sistem data yang hanya boleh diketahui pihak tertentu saja. Keamanan data adalah salah satu hal yang paling perlu diperhatikan dalam menjaga kerahasiaan informasi kumpulan data yang penting, dibutuhkan suatu teknik pengamanan tambahan dengan tujuan untuk menjaga kerahasiaan informasi penting tersebut. Tanpa adanya teknik tambahan untuk menjaga kerahasiaan data, maka banyak pihak yang tidak berhak dapat melakukan serangan, salah satunya adalah pencurian data. Algoritma *RSA* merupakan teknik pengamanan yang tepat karena menggunakan sepasang kunci dengan tingkat kesulitan yang tinggi dalam memfaktorkan bilangan menjadi faktor-faktor prima. Dengan metode Algoritma *RSA* data kredit nasabah di PT. Bank Perkreditan Rakyat Solider terjaga kerahasiaanya.

**Kata Kunci:** Keamanan Data Kredit; Enkripsi; Dekripsi *RSA*

**A B S T R A C T**

Bank is a business entity that collects funds from the public in the form of savings and distributes them to the public in the form of credit. PT. Bank Perkreditan Rakyat Solider has a data system that can only be known by certain parties. Data security is one of the most important things to consider in maintaining the confidentiality of important data collection information, an additional security technique is needed with the aim of maintaining the confidentiality of this important information. Without additional techniques to maintain data confidentiality, many unauthorized parties can carry out attacks, one of which is data theft. The RSA algorithm is an appropriate security technique because it uses a pair of keys with a high level of difficulty in factoring numbers into prime factors. With the RSA Algorithm method, customer credit data at PT. Solider People's Credit Bank is kept confidential.

**Keywords:** Credit Data Security; Encryption; RSA Decryption.

## 1. PENDAHULUAN

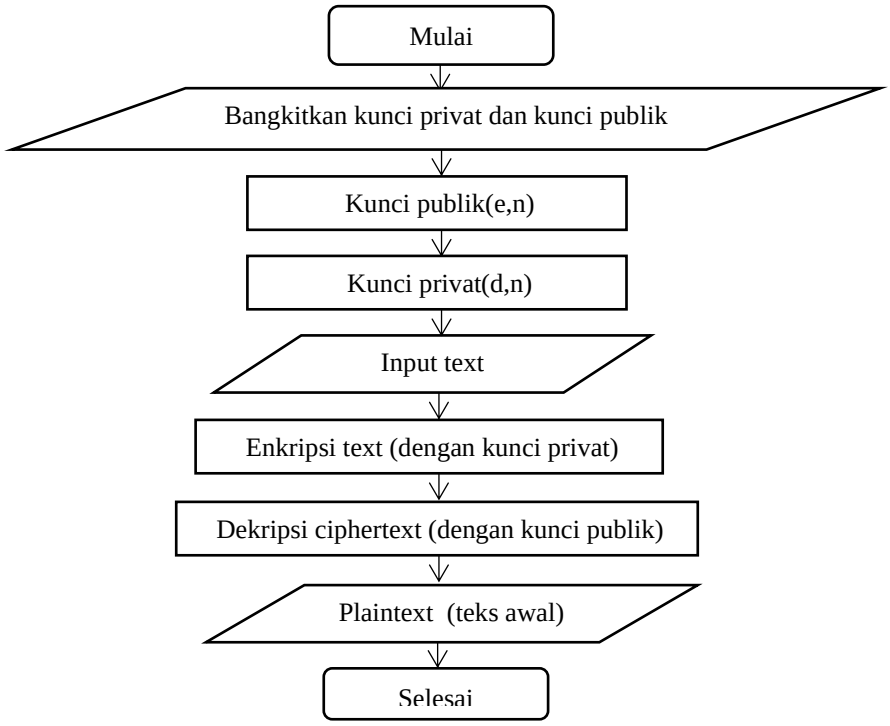
Data merupakan sesuatu yang amat penting dan berharga pada abad teknologi pada saat ini karena sangat penting maka harus di jaga kerahasiaanya[1]. Bank adalah badan usaha yang menghimpun dana dari masyarakat dalam bentuk giro, tabungan, deposito, dan menyalurkannya kepada masyarakat dalam bentuk kredit. PT.Bank Perkreditan Rakyat Solider Pematangsiantar menggunakan sistem simpan pinjam untuk anggotanya sendiri dan data hanya boleh diketahui pihak perusahaan dan nasabah. [2]Dari tuntutan kerahasiaan data tersebut maka sangat dibutuhkan suatu sistem pengamanan tambahan untuk menjaga keamanan data dan kerahasiaan data.

Permasalahan PT.Bank Perkreditan Rakyat Solider Pematangsiantar adalah keamanan data kredit. Dengan tidak adanya sistem pengamanan tambahan, data kredit rentan terhadap manipulasi ataupun pencurian dan kerusakan, maka penulis menggunakan algoritma kriptografi[3] *RSA* [4]untuk proses enkripsi data.

## 2. METODOLOGI PENELITIAN

### 2.1 Rancangan Penelitian

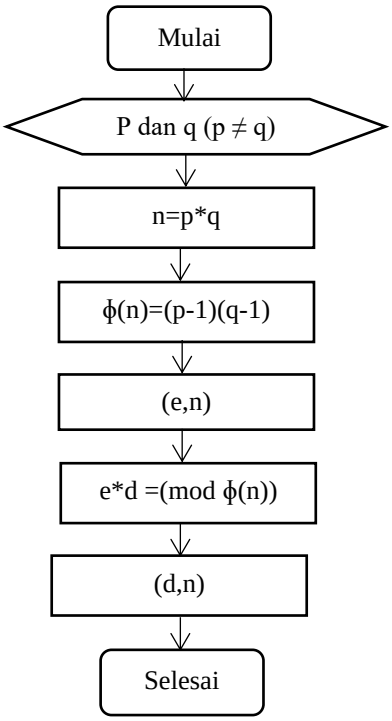
a. Berikut tahap *Flowchart* penelitian ditunjukan pada gambar 1.




**Gambar 1.** *Flowchart* penelitian

b. *Flowchart* Proses Pembangkitan Kunci

Untuk membangkitkan kunci publik dan kunci privat, tentukan dua buah bilangan prrima , p dan q. kemudian hitung modulus (n) dengan cara mengalikan kedua bilangan tersebut (n=p.q). lalu hitunglah faktor prima dari n(ϕ(n)) dengan rumus ϕ(n) =(p-1)(q-1). Tentukan kunci publik dari hasil pemfaktoran bilangan primanya. Untuk mencari kunci privat digunakan persamaan (e * d = (mod ϕ(n)), persamaan ini equivalen dengan (e * d =1 + k ϕ(n)) sehingga d dapat dapat dihitung dengan $d = \frac{1+k\phi(n)}{e}$ hasilnya adalah kunci privat. Pada gambar 2. di tunjukkan proses pembangkitan kunci kriptografi RSA.




**Gambar 2.** *Flowchart* Pembangkitan Kunci

c. Proses Enkripsi

Dalam mengenkripsi pesan(*plaintext*), masukkan kunci publik. Proses enkripsi digambarkan dengan rumus (c = $m^e$ mod n), dimana c (*cipherteks*), m (pesan), e (kunci publik) dan n (modulus). Dengan rumus tersebut pesan

dibagi menjadi blok-blok $m_1,m_2,\ldots m_i$ sehingga setiap blok merepresentasikan nilai didalam selang [n - 1]. Setiap blok $m_i$ di enkripsi menjadi blok $c_i$ dengan rumus ($c_i = m_i^{\,e} \bmod n$).Hasilnya berupa pesan yang telah dienkripsi (*cipherteks*).

### 2.2 Algoritma RSA

Algoritma *RSA* adalah yang paling populer dari banyaknya kriptografi[5] kunci public yang pernah dibuat. Algoritma *RSA* [6]dibuat oleh tiga orang peneliti dari *MIT (Massachussets Institute of Technology)* pada tahun 1976, yaitu: *Ron(R)ivest, Adi(S)hamir, dan leonardo(A)dleman*. [7]Keamanan algoritma *RSA*[8] terletak pada sulitnya memfaktorkan bilangan yang besar menjadi faktor-faktor prima. Pemfaktoran dilakukan untuk memperoleh kunci privat. Kunci privat dibangun dari beberapa buah bilangan prima bersama-sama dengan kunci enkripsi. Untuk menemukan kunci dekripsi orang harus memfaktorkan suatu bilangan non prima menjadi faktor prima. Semakin besar bilangan non primanya tentu semakin sulit pula pemfaktorannya. Semakin sulit pemfaktorannya semakin kuat pula algoritma *RSA*, maka selama itu pula keamanan algoritma *RSA* tetap terjamin[9].

Tujuan dalam metode penelitian ini adalah untuk meningkatkan keamanan dan menjaga kerahasiaan data kredit di PT. Bank Perkreditan Rakyat Solider menggunakan metode algoritma *RSA*.
Pembangkitan kunci dalam algoritma RSA dijelaskan sebagai berikut:

1. Pilih dua bilangan prima
2. Hitung n dengan persamaan:
   $n = p\,q.\ (p \neq q)$
3. Hitung $\phi$ dengan persamaan:
   $\phi = (p-1)(q-1)$
4. Dipilih bilangan bulat (integer) antara satu dan $\phi$ ($1 < e < \phi$) yang merupakan bilangan pasangan dari $\phi$
5. Hitung d dengan persamaan:
   $de = 1 \pmod{\phi}$

Hasil dari algoritma ini;
Kunci publik : pasangan (e,n)
Kunci privat : pasangan (d,n)

Enkripsi yang digunakan dalam algoritma RSA di jelaskan sebagai berikut:
1.Susun pesan menjadi blok-blok plaintext: $m_1,m_2,m_3\ldots m_n$
2.Hitung blok ciphertext $c_i$ untuk plaintext $m_i$ dengan rumus :
$c_i = m_i^{\,e} \bmod n$. Yang di dalam hal ini ,e adalah kunci publik

Dekripsi yang digunakan dala algoritma RSA di jelaskan sebaga berikut :
1.Gunakan kunci privat untuk melindungi $m_i = c_i^{\,d} \bmod n$
2.Carilah nilai m dengan rumus: $m_i = c_i^{\,d} \bmod n$

Pemodelan dari metode algoritma kriptografi *RSA* pada penelitian ini ialah Algoritma *RSA* mengenkripsi *plaintext*(teks asli) kedalam bentuk kode ,agar tidak mudah dimengerti selain orang yang berhak mengetahuinya, lalu mendekripsikan kembali data tersebur seperti semula(data awal)

## 3. HASIL DAN PEMBAHASAN

### 3.1 Penerapan Algoritma RSA

Didalam merancang suatu sistem keamanan ke dalam suatu program aplikasi membutuhkan metode algoritma yaitu dengan menggunakan langkah enkripsi dan dekripsi untuk mengamakan data-data yang bersifat rahasia. Contoh perhitungan enkripsi dan dekripsi algoritma *RSA* dalam penelitian ini disimulasikan manual dengan *plaintext* "0000000001".

Pertama mengenkripsi *plaintext* menggunakan algoritma RSA dengan langkan awal dilakukan terlebihdahulu adalah mengubah *plaintext* dan kedalam bentuk heksadesimal. Konversi *plaintext* kedalam bentuk heksadesimal dalam pengkodean tabel *ASCII* .

Dibawah ini langkah-langkan enkripsi dengan menggunakan algoritma RSA:

1. Pililah bilangan prima misalnya p = 3 dan q =17
2. Di hasilkan n = p * q = 3 * 17 = 51
3. Hitunglah m (3-1) * (17-1) = (2*16) = 32
4. Pilih nilai e yang relative prima terhadap m = 96
   Dengan ketentuan e > 1 dan e < m, maka dalam hal ini e = 3. Karena 3 relative prima terhadap 96 sebab pembagi bersama terbesarnya adalah 1
5. Tentukan d dimana dengan persamaan e * d = 1 (mod $\phi$ (n)

$$d = \frac{1 + (k * m)}{e}$$

$$d = \frac{1+(1*32)}{e} = \frac{33}{3} = 11$$

Diperoleh nilai bulat .11 maka d =11

6. Public key (e,n) = (3,51)
7. Private key (d,n) = (11,51)
8. Proses enkripsi dengan menggunakan persamaan $c_i = pl_i^{\ e} \bmod n$
   Dengan *plaintext* dikonversi ke tabel ASCII
   Diketahui: e = 3

   n = 51
   *plaintext* = 0000000001

   pengkodean *ASCII* adalah:
   48484848484848484849
   Pecahlah *plaintext* menjadi 10 blok dengan 2 digit dengan menyatakan *plaintext* kedalam blok $pl_i$

   $pl_1 = 0 = 48$ $pl_6 = 0 = 48$
   $pl_2 = 0 = 48$ $pl_7 = 0 = 48$
   $pl_3 = 0 = 48$ $pl_8 = 0 = 48$
   $pl_4 = 0 = 48$ $pl_9 = 0 = 48$
   $pl_5 = 0 = 48$ $pl_{10} = 1 = 49$

   Enkripsi setiap blok (pl) menjadi $c_i$ sebagai berikut:

   $c_1 = 48^3 \bmod 51 = 24$ $c_6 = 48^3 \bmod 51 = 24$
   $c_2 = 48^3 \bmod 51 = 24$ $c_7 = 48^3 \bmod 51 = 24$
   $c_3 = 48^3 \bmod 51 = 24$ $c_8 = 48^3 \bmod 51 = 24$
   $c_4 = 48^3 \bmod 51 = 24$ $c_9 = 48^3 \bmod 51 = 24$
   $c_5 = 48^3 \bmod 51 = 24$ $c_{10} = 49^3 \bmod 51 = 43$

   *ciphertext* yang di hasilkan adalah:
   *c* = 24 24 24 24 24 24 24 24 24 43
9. Proses dekripsi dengan menggunakan persamaan: $m = c^{\ d} \bmod n$
   Diketahui:
   d = 11
   n = 51
   *ciphertext* = 24 24 24 24 24 24 24 24 24 43
   Setiap blok *ciphertext* $c_i$ didekripsikan kembali menjadi blok $pl_i$

   $pl_1 = 24^{11} \bmod 51 = 48$ $pl_6 = 24^{11} \bmod 51 = 48$
   $pl_2 = 24^{11} \bmod 51 = 48$ $pl_7 = 24^{11} \bmod 51 = 48$
   $pl_3 = 24^{11} \bmod 51 = 48$ $pl_8 = 24^{11} \bmod 51 = 48$
   $pl_4 = 24^{11} \bmod 51 = 48$ $pl_9 = 24^{11} \bmod 51 = 48$
   $pl_5 = 24^{11} \bmod 51 = 48$ $pl_{10} = 43^{11} \bmod 51 = 49$

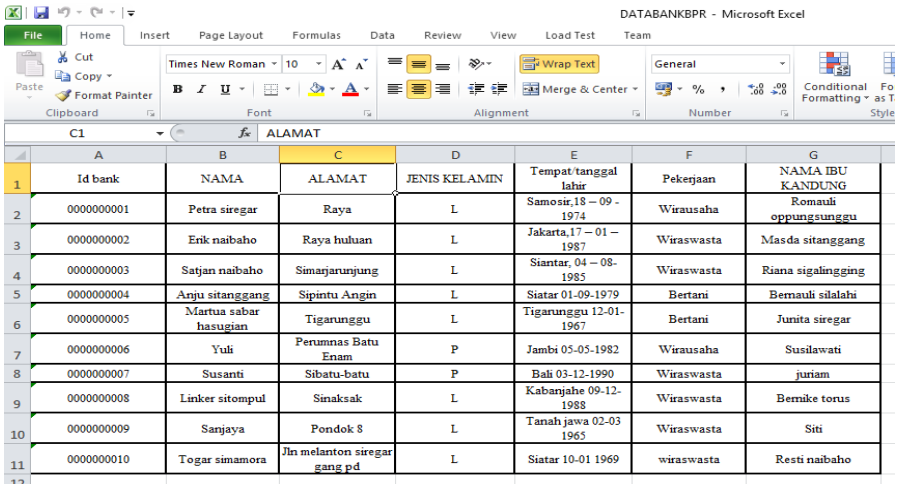
   Dekripsi yang di hasilkan adalah : 48 48 48 48 48 48 48 48 48 49

Sehingga :

Dekripsi 48484848484848484849 yang dalam sistem pengkodean ASCII adalah:
plaintext: 0000000001

### 3.2 Implementasi Program

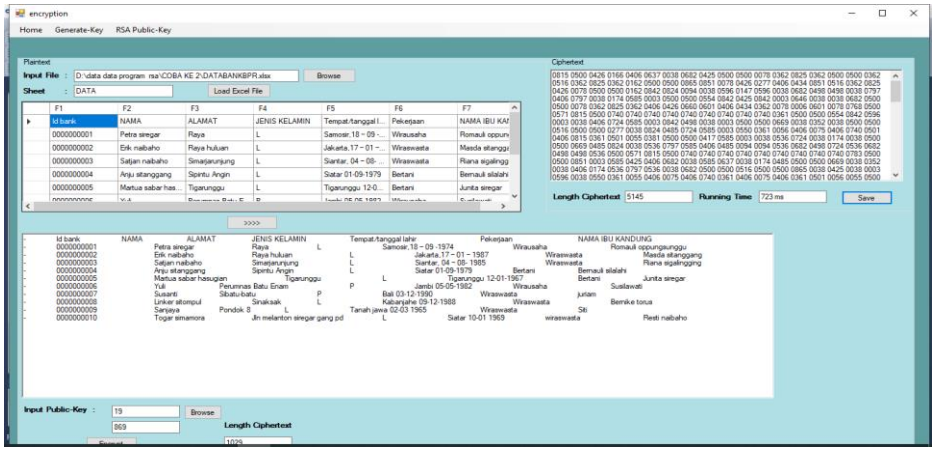
Berikut merupakan tampilan yang sebenarnya di tunjukkan pada gambar 3 dalam bentuk *Microsoft Excel.*




| | A | B | C | D | E | F | G |
|---|---|---|---|---|---|---|---|
| 1 | Id bank | NAMA | ALAMAT | JENIS KELAMIN | Tempat/tanggal lahir | Pekerjaan | NAMA IBU KANDUNG |
| 2 | 0000000001 | Petra siregar | Raya | L | Samosir,18 – 09 - 1974 | Wirausaha | Romauli oppungsunggu |
| 3 | 0000000002 | Erik naibaho | Raya huluan | L | Jakarta,17 – 01 – 1987 | Wiraswasta | Masda sitanggang |
| 4 | 0000000003 | Satjan naibaho | Simarjarunjung | L | Siantar, 04 – 08-1985 | Wiraswasta | Riana sigalingging |
| 5 | 0000000004 | Anju sitanggang | Sipintu Angin | L | Siatar 01-09-1979 | Bertani | Bernauli silalahi |
| 6 | 0000000005 | Martua sabar hasugian | Tigarunggu | L | Tigarunggu 12-01-1967 | Bertani | Junita siregar |
| 7 | 0000000006 | Yuli | Perumnas Batu Enam | P | Jambi 05-05-1982 | Wirausaha | Susilawati |
| 8 | 0000000007 | Susanti | Sibatu-batu | P | Bali 03-12-1990 | Wiraswasta | juriam |
| 9 | 0000000008 | Linker sitompul | Sinaksak | L | Kabanjahe 09-12-1988 | Wiraswasta | Bernike torus |
| 10 | 0000000009 | Sanjaya | Pondok 8 | L | Tanah jawa 02-03 1965 | Wiraswasta | Siti |
| 11 | 0000000010 | Togar simamora | Jln melanton siregar gang pd | L | Siatar 10-01 1969 | wiraswasta | Resti naibaho |

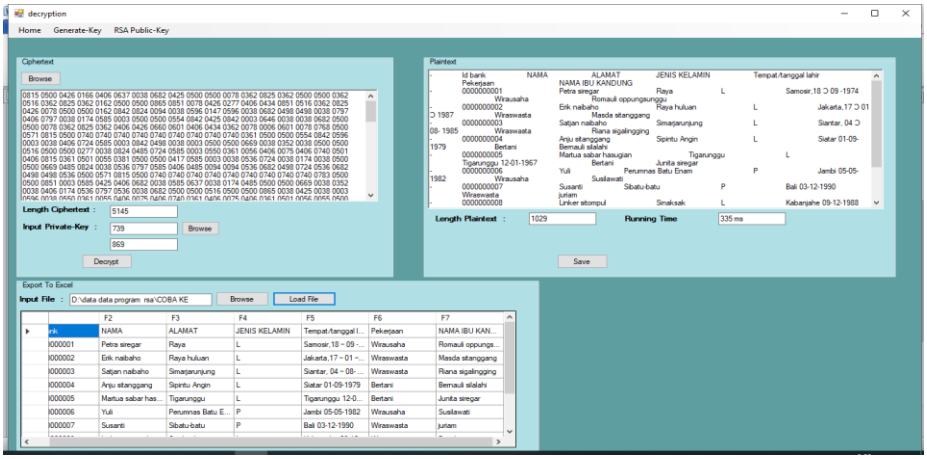
**Gambar 3.** Tampilan File Sebenarnya

Pada tahap enkripsi merupakan proses dimana *plaintext* (data yang sebenarnya) di ubah menjadi *ciphertext*(data yang telah tersanadi). Pengujian Enkripsi di tunjukkan pada gambar 4.



**Gambar 4.** Pengujian Enkripsi

Dekripsi merupakan proses dimana data *ciphertext* di ubah kembali ke data asli (*plaintext*). Pengujian dekripsi ditunjukkan pada gambar 5.



**Gambar 5.** Pengujian Deripsi

## 4. KESIMPULAN

Penggunaan teknik kriptografi algoritma RSA dapat memecahkan permasalah pengamanan data di PT. Bank Perkreditan Rakyat Solider Pematang Siantar. Skema algoritma RSA dalam mengamankan data terdiri dari : pembentukan kunci, proses enkripsi dan dekripsi.Dengan adanya algoritma dengan aplikasi yg di terapkan mampu mengurangi tingkat pencurian maupun manipulasi data.

## REFERENCES

[1] F. Zuli and A. Irawan, “Implementasi Kriptografi Dengan Algoritma Blowfish dan Riverst Shamir Adleman ( RSA ) Untuk Proteksi File,” vol. 6, pp. 27–38, 2016.
[2] B. Anwar, N. B. Nugroho, and J. Prayudha, “Implementasi Algoritma RSA Terhadap Keamanan Data Simpan Pinjam,” vol. 18, no. 1, pp. 30–34, 2019.
[3] L. Juliana, “Hybrid Cryptosystem Algoritma Rsa dan Hill Cipher dengan Kunci Fingerprint,” 2015.
[4] J. Manurung, K. Sirait, J. F. Panggabean, and D. Komputer, “PENERAPAN ALGORITMA RSA UNTUK PENGAMANAN FILE,” vol. 2, no. 2, pp. 112–116, 2018.
[5] Jamaludin, “Rancang Bangun Kombinasi Hill Cipher dan RSA Menggunakan Metode Hybrid Cryptosystem,” vol. 2, no. April 2018, 2019.
[6] P. S. Asmoro, “PENGAMANAN DATA CITRA DENGAN GABUNGAN ALGORITMA RSA DAN OTP,” pp. 1–38, 2015.
[7] M. Y. Simargolang, “IMPLEMENTASI KRIPTOGRAFI RSA DENGAN PHP,” vol. 1, pp. 1–10, 2017.
[8] Angga Aditya Permana and R. Destriani, “PENGAMANAN TEKS MENGGUNAKAN METODE ALGORITMA RSA,” vol. 7, no. 2, 2018.
[9] Suci Rahmadhiyanti and B. W. C. O. Jones, “IMPLEMENTASI KRIPTOGRAFI RSA UNTUK PENINGKATAN KEAMANAN DATABASE E-COMMERCE,” vol. 18, pp. 627–630, 2019.