

IMPLEMENTASI ALGORITMA RSA UNTUK PERANCANGAN APLIKASI BERBASIS JAVA DESKTOP PADA MTS DAARUL FALAH

Muhammad Sugiarto^{1*}, Purwanto²

^{1,2}Fakultas Teknologi Informasi, Teknik Informatika, Universitas Budi Luhur, Jakarta, Indonesia

Email: ^{1*}1811500436@student.budiluhur.ac.id, ²purwanto@budiluhur.ac.id

(* : corresponding author)

Abstrak- Hal yang sangat penting dan krusial dalam dunia informasi saat ini adalah keamanan data. Selain itu jika informasi yang disimpan dan dikirim berupa data yang penting dan sangat rahasia, dimana pihak luar yang tidak diperbolehkan mengetahui informasi rahasia tersebut. Karena bila informasi rahasia ini tersebar pada pihak yang tidak bertanggung jawab, maka akan menimbulkan kerugian yang amat fatal bagi pihak sekolah yang informasi/datanya telah dicuri. Beberapa informasi & dokumen yang bersifat sangat penting bagi sekolah yaitu seperti : data diri siswa & guru, kumpulan soal ujian, nilai siswa atau kurikulum yang digunakan sekarang, dan lainnya perlu diamankan oleh pihak sekolah MTs Daarul Falah. Dengan mengimplementasikan algoritma kriptografi Rivest Shamir Adleman (RSA), system aplikasi ini dibuat dengan bahasa pemrograman Java berbasis desktop. Metode Rivest Shamir Adleman (RSA) digunakan pada aplikasi ini untuk menyandikan (enkripsi) pesan rahasia yang berupa file (dokumen) agar kerahasiaan data tersebut semakin kuat dan aman dari pencurian data. Berdasarkan implementasi dan uji coba, program aplikasi enkripsi dan dekripsi yang menggunakan algoritma Rivest Shamir Adleman (RSA) tersebut mampu mengamankan file (dokumen) dengan baik. Hasil dari penelitian ini menunjukkan bahwa algoritma RSA dapat diterapkan dalam mengenkripsi dan mendekripsi file pada Madrasah Tsanawiyah Daarul Falah, dengan kecepatan proses enkripsi file 0,16 detik ekstensi doc, 0,034 detik ekstensi xls, dan 0,004 detik ekstensi txt. Untuk proses dekripsi dengan kecepatan 3,811 detik ekstensi doc, 1,411 detik ekstensi xls, dan 0,041 detik ekstensi txt. Dengan adanya aplikasi kriptografi, proses penyimpanan data-data sekolah yang penting menjadi lebih aman dari orang-orang yang tidak berkepentingan.

Kata Kunci : kriptografi, enkripsi, dekripsi, rivest samir adleman (RSA)

IMPLEMENTATION OF RSA ALGORITHM FOR JAVA-BASED APPLICATION DESIGN AT MTS DAARUL FALAH

Abstract- The most important and crucial thing in today's world of information is data security. In addition, if the information stored and sent is in the form of important and very confidential data, where outside parties are not allowed to know the confidential information. Because if this confidential information is spread to irresponsible parties, it will cause very fatal losses for the school whose information/data has been stolen. exam questions, student & teacher attendance data, student grades or the current curriculum, and others need to be secured by the MTs Daarul Falah school. By implementing the Rivest Shamir Adleman (RSA) cryptographic algorithm, this application system is made with the desktop-based Java programming language. The Rivest Shamir Adleman (RSA) method is used in this application to encode (encrypt) secret messages in the form of files (documents) so that the confidentiality of the data is stronger and safer from data theft. Based on implementation and testing, the encryption and decryption application program that uses the Rivest Shamir Adleman (RSA) algorithm is able to secure files (documents) well. The results of this study indicate that the RSA algorithm can be applied to encrypt and decrypt files at Madrasah Tsanawiyah Daarul Falah, with a file encryption speed of 0.16 seconds doc extension, 0.034 seconds xls extension, and 0.004 seconds txt extension. For the decryption process with a speed of 3.811 seconds doc extension, 1.411 seconds xls extension, and 0.041 seconds txt extension. With the application of cryptography, the process of storing important school data becomes safer from unauthorized people.

Keywords : cryptography, encryption, decryption, rivest samir adleman (RSA).

1. PENDAHULUAN

Madrasah Tsanawiyah Daarul Falah merupakan sekolah Madrasah yang berlokasi di Karang Tengah - Ciledug. Di setiap sekolah pasti ada berkas - berkas untuk per semesternya. Berkas yang dimaksud yaitu berupa data diri siswa, nilai siswa atau kurikulum yang digunakan oleh sekolah. Maka sekolah tersebut dapat dipastikan mempunyai berkas-berkas yang sangat krusial dan rahasia seperti data diri siswa, nilai siswa atau kurikulum yang digunakan sekarang. Sehingga data penting tersebut tidak boleh disebarluaskan ke sembarang pihak, ditakutkan terjadi penyalahgunaan data oleh pihak yang tidak berwenang di sekolah. Berkas sekolah yang sangat krusial dan rahasia sangatlah rawan dalam pencurian data, sehingga berkas krusial dan rahasia yang semestinya

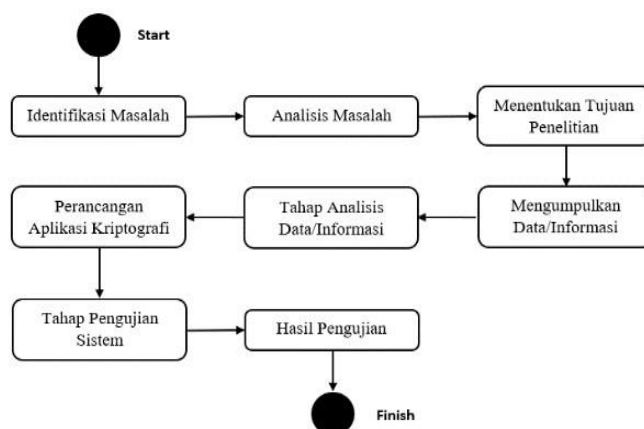
diamankan tidak boleh diketahui oleh pihak dari luar sekolah yang tidak bertanggung jawab. Karena dokumen tersebut disimpan dalam sebuah soft file tanpa keamanan yang dapat mengakibatkan kerentanan pencurian dan penyebaran data penting sekolah. Maka diperlukan sebuah sistem atau aplikasi yang berupa keamanan data guna mengantisipasi dari pencurian dan penyebaran data atau dokumen penting sekolah oleh pihak luar sekolah yang tidak berwenang.

Maka dari itu akan dibuat sistem keamanan data menggunakan metode kriptografi dengan algoritma RSA (Rivest Shamir Adleman) sebagai proses enkripsi dan dekripsi dokumen atau file untuk mengamankan data, serta untuk mengimplementasikan rancangan aplikasi pengamanan dokumen menggunakan algoritma RSA (Rivest Shamir Adleman) ini, penulis akan membuat aplikasi berbasis desktop. Karena ketika didalam sekolah lebih banyak pengguna yang merasa lebih mudah menggunakan aplikasi yang berbasis desktop dari pada web, dan aplikasi yang berbasis web juga memiliki kerentanan pencurian data yang lebih besar dari pada via desktop, Karena aplikasi yang berbasis web bisa di akses oleh siapapun dan dimanapun, sedangkan aplikasi berbasis desktop hanya dapat di gunakan oleh user yang bersangkutan dengan sekolah.

2. METODE PENELITIAN

2.1 Pengumpulan Data Penelitian

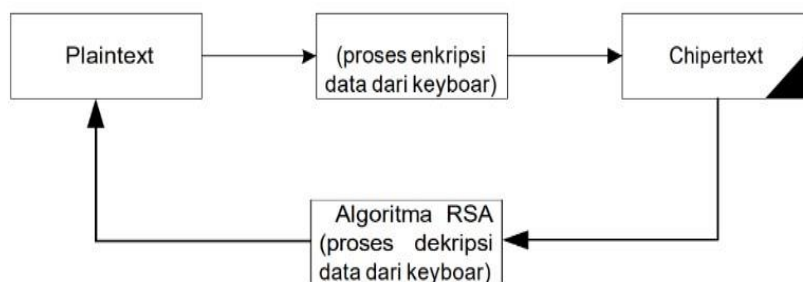
Dalam melakukan penelitian dengan menggunakan metode penelitian *private key & public key cryptography*, pengumpulan data dilakukan dengan pendekatan studi literasi, dimana dengan melakukan pencarian sumber literasi yang digunakan untuk menjadi acuan dan fakta – fakta yang telah ada pada penelitian terdahulu. Studi literasi yang dilakukan dengan menggali informasi sebanyak mungkin. Pada gambar 1 dijelaskan tahapan membangun aplikasi yang bermula dari identifikasi masalah, analisis masalah, lalu berlanjut sampai pada tahapan hasil pengujian. Berikut tahapan membangun aplikasi kriptografi yang akan dirancang.



Gambar 1. Tahapan membangun aplikasi

2.2 Metode Rivest Shamir Adleman (RSA)

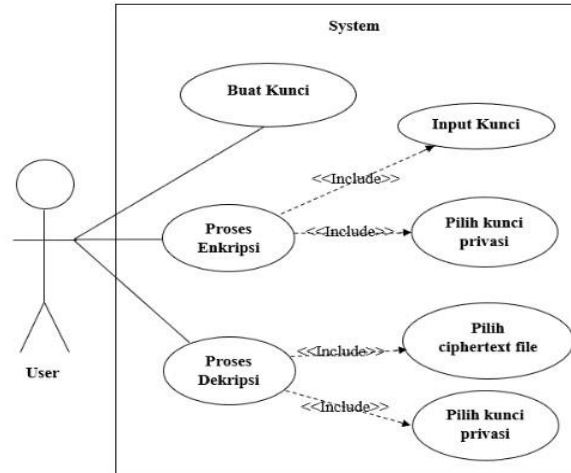
Algoritma RSA mempunyai dengan 2 kunci yang tidak sama yaitu untuk enkripsi (*plaintext*) dan dekripsi (*ciphertext*). Pada gambar 2 dijelaskan mengenai skema dari Algoritma Rivest Shamir Adleman dari awal *plaintext* di enkripsi sampai *ciphertext* di dekripsi.



Gambar 2. Skema Algoritma RSA

2.3 Use Case Diagram Aplikasi

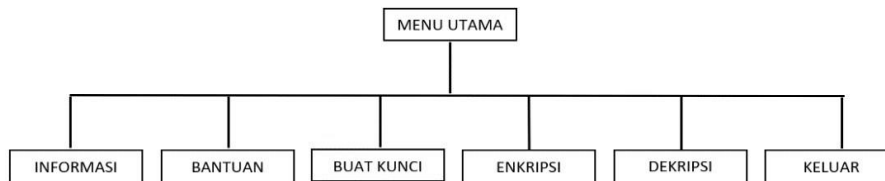
Use case diagram yaitu jenis diagram *Unified Modelling Language* (UML) yang memanifestasi hubungan antar sistem dan pengguna. Pada gambar 3 dijelaskan tentang hubungan dalam sistem aplikasi dengan pengguna, mulai dari pembuatan kunci, proses enkripsi dan dekripsi.



Gambar 3. Use Case Diagram Aplikasi

2.4 Rancangan Menu Utama

Pada gambar 4 merupakan rancangan utama dari aplikasi yang dibuat :



Gambar 4. Rancangan Menu Utama

3. HASIL DAN PEMBAHASAN

Dilakukan langkah pengujian dari rancangan sistem yang sudah dibuat. Pengujian penelitian dapat berjalan lancar dengan adanya rangkaian yang berurutan dan dirancang secara sistematis. File yang di uji coba meliputi *.doc, *.xls, dan *.txt.


3.1 Rancangan Layar Menu Buat Kunci

Pada gambar 5 berikut adalah rancangan layar menu buat kunci untuk kunci publik dan kunci privasi.

Gambar 5. Rancangan Layar Menu Buat Kunci

3.2 Rancangan Layar Menu Enkripsi

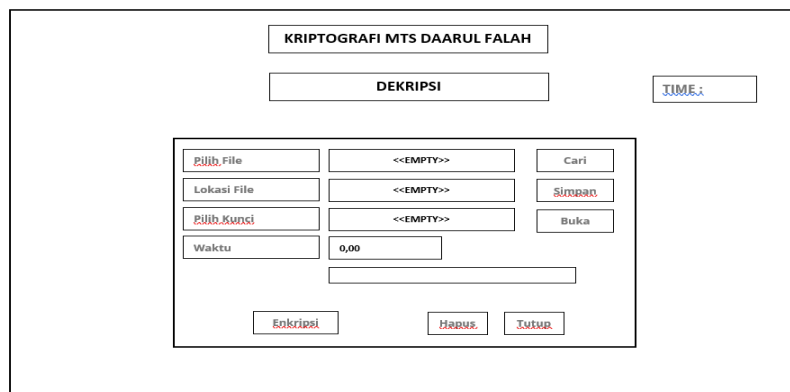
Pada gambar 6 berikut adalah rancangan layar menu enkripsi untuk mengubah plaintext menjadi ciphertext.



Gambar 6. Rancangan Layar Menu Enkripsi

3.3 Rancangan Layar Menu Dekripsi

Pada gambar 7 berikut adalah rancangan layar menu dekripsi untuk mengubah ciphertext menjadi plaintext.



Gambar 7. Rancangan Layar Menu Dekripsi

3.4 Flowchart Proses Enkripsi

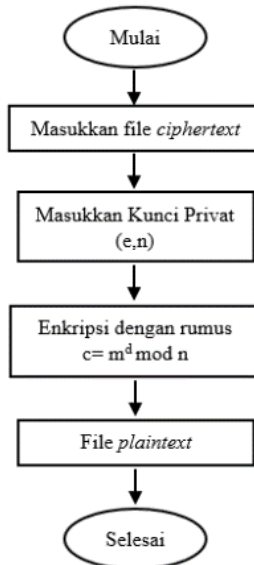
Pada gambar 8 merupakan flowchart proses enkripsi dari aplikasi yang dibuat.



Gambar 8. Flowchart proses enkripsi

3.5 Flowchart Proses Dekripsi

Pada gambar 9 merupakan flowchart proses dekripsi dari aplikasi yang dibuat.



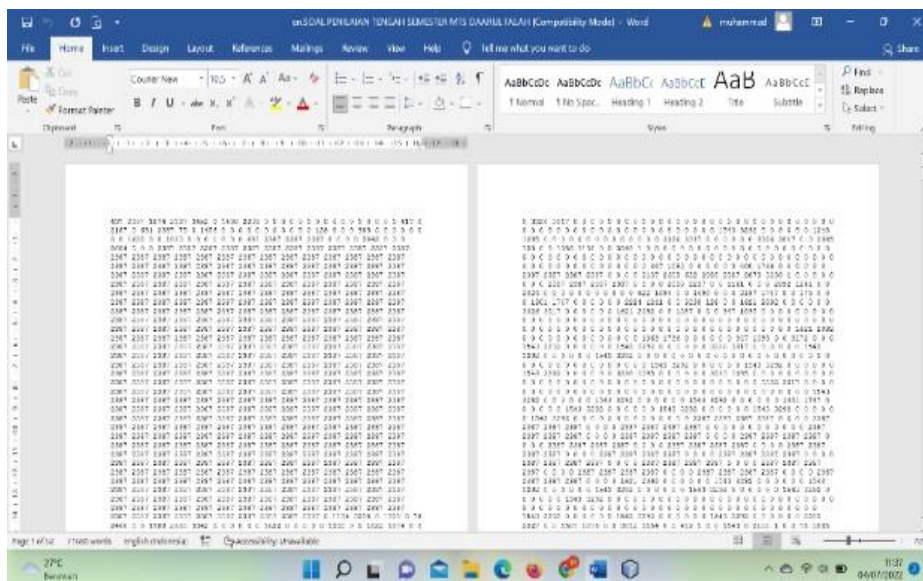
Gambar 9. Flowchart proses dekripsi

3.6 Dataset

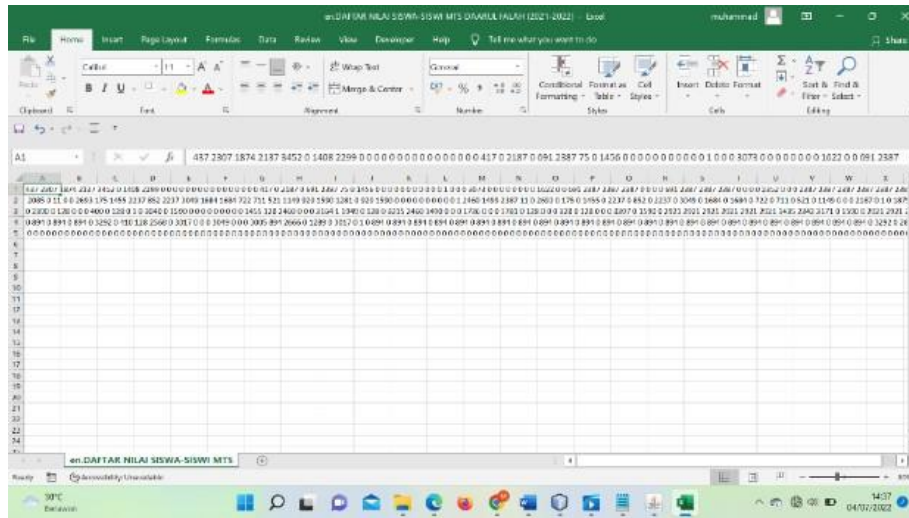
Data yang digunakan pada penelitian ini diambil dari tempat riset, yakni Madrasah Tsanawiyah Daarul Falah yang dimana data tersebut merupakan data diri siswa & guru, kumpulan soal ujian, nilai siswa dan lainnya.

3.7 Pengujian

Pada pengujian ini, akan membahas tentang perbandingan-perbandingan antara proses enkripsi dan proses dekripsi. File yang digunakan untuk pengujian yaitu *.doc, *.xls, dan *.txt. Pada gambar 10 dan 11 berikut ini adalah hasil file berekstensi doc. dan xls. sesudah di enkripsi yang dimana merupakan proses pengamanan data dari pesan asli menjadi pesan berbentuk *ciphertext*.

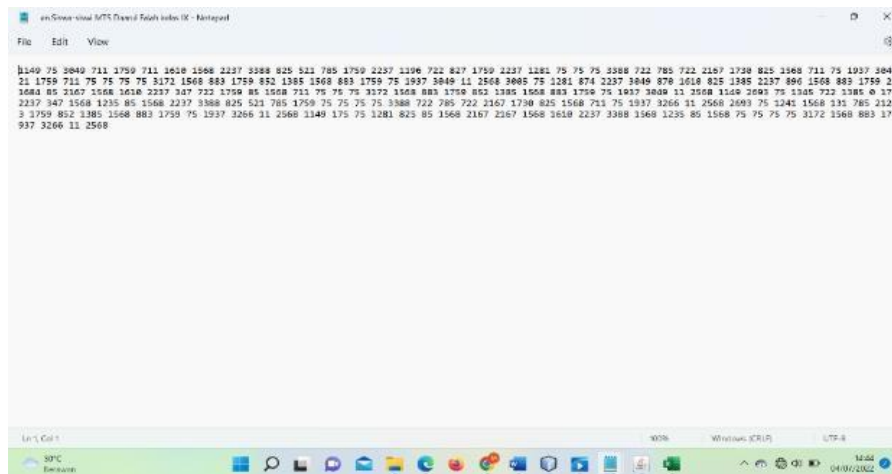


Gambar 10. File doc. setelah di enkripsi



Gambar 11. File xls. setelah di enkripsi

Pada gambar 12 berikut ini adalah hasil file berekstensi txt. sesudah di enkripsi yang dimana merupakan proses pengamanan data dari pesan asli menjadi pesan berbentuk *ciphertext*.



Gambar 12. File txt. setelah di enkripsi

3.7.1 Tabel Pengujian Proses Enkripsi

Pada Tabel 1 dijelaskan mengenai pengujian pada proses enkripsi file, mulai dari nama file, ukuran file sebelum dan sesudah di enkripsi dan waktu enkripsi.

Tabel 1. Tabel Pengujian Proses Enkripsi

Nama File Asli	Ukuran File Asli	Ukuran File Hasil Enkripsi	Waktu Enkripsi (detik)
Soal Penilaian Tengah Semester MTs Daarul Falah.doc	70,0 KB (71.680 bytes)	238 KB (244.225 bytes)	0,16
Daftar nilai siswa-siswi MTs Daarul Falah (2021-2022).xls	42,0 KB (43.008 bytes)	123 KB (126.262 bytes)	0,034
Siswa-siswi MTs Daarul Falah kelas IX.txt	1,12 KB (1.149 bytes)	4,70 KB (4.816 bytes)	0,004

3.7.2 Tabel Pengujian Proses Dekripsi

Pada Tabel 2 dijelaskan mengenai pengujian pada proses dekripsi file, mulai dari nama file, ukuran file sebelum dan sesudah di dekripsi dan waktu dekripsi.

Tabel 2. Tabel Pengujian Proses Dekripsi

Nama File Asli	Ukuran File Asli	Ukuran File Hasil Enkripsi	Waktu Enkripsi (detik)
Soal Penilaian Tengah Semester MTs Daarul Falah.doc	238 KB (244.225 bytes)	70,0 KB (71.680 bytes)	3,811
Daftar nilai siswa-siswi MTs Daarul Falah (2021-2022).xls	123 KB (126.262 bytes)	42,0 KB (43.008 bytes)	1,411
Siswa-siswi MTs Daarul Falah kelas IX.txt	4,70 KB (4.816 bytes)	1,12 KB (1.149 bytes)	0,041

4. KESIMPULAN

Dari apa yang sudah dirancang, dibuat, dan serangkaian pengujian serta analisa program dari aplikasi kriptografi ini, maka dapat ditarik kesimpulan antara lain :

- Proses penyimpanan data-data sekolah yang krusial menjadi lebih terkontrol dari oknum yang tidak berwenang.
- Waktu kecepatan proses enkripsi file 0,16 detik ekstensi doc, 0,034 detik ekstensi xls, dan 0,004 detik ekstensi txt. Untuk proses dekripsi dengan kecepatan 3,811 detik ekstensi doc, 1,411 detik ekstensi xls, dan 0,041 detik ekstensi txt.
- Proses Data yang sudah di enkripsi dapat dikembalikan seperti data awal sebelum di enkripsi tanpa merubah isi data asli tersebut.

DAFTAR PUSTAKA

- [1] M. Arief, F. Fitriyani and N. Ikhsan, "Kriptografi RSA Pada Aplikasi File Transfer Client-Server Based," *JITTER: Jurnal Ilmiah Teknologi Informasi Terapan*, pp. vol 1, no 3, pp 45-51, 2015.
- [2] Basri, "Kriptografi Simetris dan Asimetris Dalam perspektif Keamanan Data Dan Kompleksitas Komputasi," *Jurnal Ilmiah Ilmu Komputer*, vol 2 ,no 2, pp 16-23, 2016.
- [3] Hariyanto, et al, "Aplikasi Enkripsi dan Dekripsi pada Soal Ujian Menggunakan Algoritma RSA Berbasis JAVA Desktop," *Jurnal Ilmiah Komputer & Sistem Informasi*, vol 17, no 3, pp. 229-237, 2018.
- [4] F. Wanita, "Rancang Bangun Sistem Enkripsi dan Dekripsi Pengiriman Informasi Menggunakan Algoritma RSA (Rivest Shamir Adlement) Berbasis Wifi," *Inspiration: Jurnal Teknologi Informasi & Komunikasi*, vol. 5, no 1, pp. 35-43, 2015.
- [5] M. A. Zainuddin and D. I. Mulyana, "Penerapan Algoritma RSA Untuk Keamanan Pesan Instan Pada Perangkat Android," *Jurnal CKI On SPOT*, vol. 9, no. 2, pp. 105-114, 2016 .
- [6] B. S. Muchlis, M. A. Budiman and D. Rachmawati, "Teknik Pemecahan Kunci Algoritma Rivest Shamir Adleman (RSA) dengan Metode Kraitichik," *Sinkron : Jurnal & Penelitian Teknik Informatika* , vol. 2, no. 2, pp. 49-64, 2017.
- [7] R. S. Ashari Arief, "Implementasi Kriptografi Kunci Publik Dengan AlgoritmaRSA-CRT pada Aplikasi Instant Messaging," *SJI (Scientific Journal of Indormatics)*, vol. 3, no. 1, pp. 46-54, 2016.
- [8] R. Kurniawan, "Rancang Bangun Aplikasi Pengaman Isi File Dokumen Dengan Algoritma RSA," *ALGORITMA : Jurnal Ilmu Komputer Dan Informatika*, vol. 1, no.01, pp. 46-52, 2017.
- [9] F. Azmia and W. Erika, "Analisis Keamanan Data Pada Block Cipher Algoritma Kriptografi RSA," *CESS : Journal of Computer Engineering System and Science*, vol. 2, no. 1, pp. 27-29, 2017.
- [10] D. d. S. Satriya Tri Cahaya Kurniawan, Implementasi Kriptografi Algoritma Rivest Shamir Adleman Dengan Playfair Ciper Pada Pesan Teks Berbasis Android, *Jurnal Online Informatika*, vol. 2, no. 2, pp. 102-109, 2017.