LEMBAR PENGESAHAN

Skripsi yang berjudul " **IMPLEMENTASI KRIPTOGRAFI DENGAN ALGORITMA RSA (RIVEST-SHAMIR-ADLEMAN) DALAM PENYANDIAN PESAN TEKS DAN DOKUMEN** "

Oleh

Septi Rahmita Sari
NIM. 412418005
Program Studi Matematika
Fakultas Matematika dan Ilmu Pengetahuan Alam

Telah dipertahankan di depan dewan penguji

Hari, tanggal : **Kamis, 5 Januari 2023**
Waktu : **10.01-11.30 WITA**
Tempat : **Ruang Sidang Jurusan Matematika Lt.3 FMIPA**

	Pembimbing	**Tanda Tangan**
Pembimbing 1	**Resmawan, S.Pd., M.Si**	
	NIP. 198804132014041001	(1. .....)
Pembimbing 2	**Nisky Imansyah Yahya, S.Pd., M.Si**	
	NIP. 199107302020121008	(2. .....)
	Penguji	**Tanda Tangan**
Penguji 1	**Djihad Wungguli, S.Pd., M.Si**	
	NIP. 198906122019031018	(1. .....)
Penguji 2	**Agusyarif Rezka Nuha, S.Pd., M.Si**	
	NIP. 199308102019031009	(2. .....)
Penguji 3	**Asriadi, S.Pd., M.Si**	
	NIP. 198910282020121015	(3. .....)

Mengetahui,
Dekan Fakultas Matematika dan IPA

Prof. Dr. Astin Lukum, M.Si
NIP.196303271988032002

LEMBAR PERSETUJUAN PEMBIMBING

Skripsi yang berjudul " **IMPLEMENTASI KRIPTOGRAFI DENGAN ALGORITMA RSA (RIVEST-SHAMIR-ADLEMAN) DALAM PENYANDIAN PESAN TEKS DAN DOKUMEN**"

Oleh

Septi Rahmita Sari
NIM. 412418005

Telah diperiksa dan disetujui untuk diuji

Pembimbing I	Pembimbing II,
Resmawan, S.Pd., M.Si	**Nisky Imansyah Yahya, S.Pd., M.Si**
NIP. 198804132014041001	NIP. 199107302020121008

Mengetahui,
Ketua Program Studi Matematika

Resmawan, S.Pd., M.Si
NIP. 198804132014041001

ABSTRAK

Septi Rahmita Sari, 2 0 2 3. *IMPLEMENTASI KRIPTOGRAFI DENGAN ALGORITMA RSA (RIVEST-SHAMIR-ADLEMAN) DALAM PENYANDIAN PESAN TEKS DAN DOKUMEN*. **Skripsi.** Gorontalo. Program Studi Matematika. Jurusan Matematika. Fakultas Matematika dan Ilmu Pengetahuan Alam. Universitas Negeri Gorontalo.
Pembimbing : **(1) Resmawan, S.Pd., M.Si(2) Nisky Imansyah Yahya, S.Pd., M.Si**

Kriptografi dapat digunakan dalam mencegah penyalahgunaan data, dikarenakan untuk keamanan dan kerahasian data merupakan hal penting. Diperlukan tindakan pencegahan untuk mengamankan isi pesan dengan cara penyandian pesan sebelum dikirim ke pihak yang bersangkutan. Kriptografi merupakan studi tentang penyandian pesan atau cara perlindungan data. Dalam penyandian isi pesan terdapat algoritma yang popular digunakan sampai saat ini yaitu algoritma RSA(Rivest-Shamir-Adleman). Algoritma RSA ialah metode yang mempunyai dua kunci yang berbeda untuk setiap proses enkripsi dan dekripsinya tetapi saling berkaitan sehingga lebih terjaga dalam proses keamanan data. Kemudian dalam proses pencarian kunci algoritma RSA memanfaatkan kaidah bilangan prima. Semakin besar bilangan prima yang dipakai sebagi kunci, semakin susah ditemukan angka besar sebagi faktornya. Dalam hal ini akan dibahas proses enkripsi pesan teks dan isi dokumen menggunakan algoritma RSA, yang kemudian akan dijelaskan proses dekripsi dan proses pembangkitan kunci. Dengan mengubah *plaintext* menjadi *ciphertext* menggunakan kode ASCII yang panjangnya 256 serta menggunakan PKCS dalam melakukan proses enkrispi pada algoritma RSA. Kemudian pengimplementasian algoritma RSA pada pesan teks dan dokumen menggunakan Bahasa pemrograman Python. Pada penelitian selanjutnya, disarankan untuk menggunakan algoritma atau Bahasa pemprograman lain dalam proses pengamanan pesan.

Kata Kunci: *Algoritma RSA, Teks, Enkripsi, Dekripsi.*

ABSTRACT

Septi Rahmita Sari, 2023. *IMPLEMENTATION OF CRYPTOGRAPHY WITH RSA (RIVEST-SHAMIR-ADLEMAN) ALGORITHM IN ENCODING TEXT MESSAGES AND DOCUMENTS*. **Undergraduate Thesis**. Gorontalo. Study Program of Mathematics, Department of Mathematics, Faculty of Mathematics and Natural Sciences. Universitas Negeri Gorontalo.
The supervisors: **(1) Resmawan, S.Pd., M.Si., (2) Nisky Imansyah Yahya, S.Pd., M.Si.**

Cryptography can be used to prevent data misuse and secure confidential data. To protect the data, it needs precautions to secure the content of the message by encoding it before it is sent to the concerned party. Cryptography is the study of encoding messages or ways of data protection. In encoding the content of messages, there is an algorithm conventionally used nowadays, the RSA (Rivest-Shamir-Adleman) algorithm. The RSA algorithm is a method that has two different keys for each encryption and decryption process but is still interrelated to maintain security in processing the data. In finding the key, the RSA algorithm utilizes the rule of prime number. The larger the prime number used as a key, the harder it is to find a large number as a factor. This research describes the process of encrypting text messages, the content of documents using the RSA algorithm, and the key generation process. Those processes are done by converting plaintext into ciphertext using ASCII code, which is 256 long, and using PKCS (Public Key Cryptography Standards) in the encryption process on the RSA algorithm. This study uses Python programming language to implement the RSA algorithm on text messages and documents. As a recommendation to the subsequent studies, it is proper to use algorithms or other programming languages to secure messages.

Keywords: *RSA Algorithm, Text, Encryption, Description.*