ABSTRAK

Peningkatan pengguna internet pada masa pandemi *COVID-19* ternyata menyebabkan peningkatan kejahatan siber di dunia. Kasus *phising* dan *ransomware* merupakan kasus kejahatan siber yang paling banyak terjadi. Kedua kasus tersebut memiliki tujuan yang sama yaitu untuk mencuri informasi dari korbannya. Untuk meminimalisir pencurian informasi dan mengamankannya, ada dua algoritma yang bisa digunakan yaitu kriptografi dan steganografi. Tujuan penelitian ini adalah untuk memahami bagaimana cara menggabungkan algoritma *RSA* dengan steganografi teks dengan metode *LSB Matching* dan mengimplementasikannya ke dalam sebuah perangkat lunak untuk mengamankan informasi. Karena belum banyak penelitian yang menggunakan steganografi dengan *cover-object* berupa teks maka, dibuatlah penelitian ini yaitu dengan menggabungkan kriptografi asimetris *RSA* dan steganografi teks dengan metode *LSB Matching*. Metode Penelitian yang digunakan adalah metode eksperimental dengan dua tahap yaitu tahap pengumpulan data melalui observasi dan studi literatur dan tahap pengembangan perangkat lunak menggunakan *SDLC Waterfall*. Hasil dari penelitian ini berhasil dibuat sebuah perangkat lunak yang menggabungkan dua algoritma yaitu *RSA* dan *LSB Matching* yang bisa digunakan untuk mengamankan informasi berupa teks. Proses penggabungan kedua algoritma tersebut ada beberapa tahapan yaitu pembuatan kunci *RSA*, proses *encode* menggunakan *LSB Matching* dengan *cover-object* teks dan enkripsi *RSA*, proses *decode* menggunakan dekripsi *RSA* dan memanfaatkan *stego-key* untuk memperoleh informasi rahasia kembali. Pengujian pada perangkat lunak yang dibuat dilakukan menggunakan 10 *plaintext*, 10 *cover-object* dan 20 pasang *RSA key*. Hasil pengujian menunjukan bahwa algoritma *RSA* dan *LSB Matching* yang dibuat berhasil untuk mengenkripsi serta menyisipkan *plaintext* untuk diamankan tanpa adanya perubahan pada isi *stego-object* dan berhasil untuk mendekrip serta men-*decode plaintext* ke bentuk aslinya.

Kata kunci: Kriptografi, Steganografi, *RSA*, *LSB Matching*, Keamanan Informasi.

ABSTRACT

The increase in internet users during the COVID-19 pandemic has actually led to an increase in cybercrime in the world. Phishing and ransomware cases are the most common cybercrime cases. Both cases have the same goal, namely to steal information from the victim. To minimize information theft and secure it, there are two algorithms that can be used, namely cryptography and steganography. The purpose of this study is to understand how to combine the RSA algorithm with text steganography with the LSB Matching method and implement it into a software to secure information. There are not many studies that use steganography with a cover-object in the form of text, this research was made by combining RSA asymmetric cryptography and text steganography with the LSB Matching method. The research method used is an experimental method with two stages, namely the data collection stage through observation and literature study and the software development stage using SDLC Waterfall. The results of this study is a succesfully created software that combines two algorithms, namely RSA and LSB Matching which can be used to secure information in the form of text. The process of merging the two algorithms has several stages, namely RSA key generation, encode process using LSB Matching using text cover-object and RSA encryption, decode process using RSA decryption and utilizing stego-key to obtain secret information again. Tests on the software made were carried out using 10 plaintext, 10 cover-objects and 20 pairs of RSA keys. The test results show that the RSA and LSB Matching algorithms are successful in encrypting and embedding plaintext to secure it without any changes to the contents of the stego-object and succesful in decrypting and decoding the plaintext to its original form.

Keywords: Cryptography, Steganography, RSA, LSB Matching, Information Security.