p-ISSN: 2301-5373
e-ISSN: 2654-5101

The Security System For Web-Based Lontar Images In JPG Format Using The Rivest Shamir Adleman Method

Winda Rianty[a1], I Ketut Gede Suhartana[a2]

[a]Informatics Department, Faculty of Math and Science, Udayana University
Bali, Indonesia
[1]windharianty4@gmail.com
[2]ikg.suhartana@unud.ac.id

Abstract

The Security System for Web-Based Lontar Images in JPG Format Using the Rivest Shamir Adleman Method is a system that is basically used to secure an image in JPG format, which after the encryption process will be converted into txt. Where the system functions to secure lontar by using an encryption process using a cryptographic technique, namely Rivest Shamir Adleman (RSA) which is expected to help the public to maintain information or documentation and evidence of important events that occurred in the past.

Keywords: *Security system, Cryptography, Rivest Shamir Adleman, Lontar, JPG.*

1. Introduction

Technological developments make it easier for users to secure data that is deemed important, therefore data security is very much needed at this time. One way that can be used to secure data is to use mathematical techniques related to aspects of information security such as confidentiality, data integrity, and authentication[1].

The study of data security methods is known as cryptography. The application of data security using cryptography requires an algorithm to complicate security so that data is safe and there is no piracy by irresponsible parties. One of the most popular cryptographic algorithms at this time is the RSA (Rivest Shamir Adleman) algorithm. RSA is a symmetric algorithm method. The step in the RSA algorithm is to create a key pair, namely the public key and the private key[2].

Current technological developments help to perform security or encryption. One of the media that can be used is through a website, by using web media, users will be facilitated by not needing to download an application. If you want to use the system, you only have to access the URL, and it can be accessed on all devices.

Many data contain important information, one of the things that must be secured is lontar data. The palm data is in the form of an image in JPG format which will be secured using an encryption process. Lontar is a past text made from tal leaves, besides that lontar is also a very important source of information for the community, because from lontar people can get information or documentation and evidence of important events that occurred in the past. [3] therefore lontar can be used as a cultural reflection for the continuation of future generations. So in this case the author wants to develop a web for further use of securing JPG data which in turn can help secure data and increase the effectiveness and efficiency of its users.

2. Reseach Methods

2.1 Lontar

Lontar (Borassus Flabellifer) is a type of palm that is multipurpose. This is because almost all parts of this plant are beneficial to mankind, among others as food, buildings, household furniture and art items, but what many people cultivate from lontar trees is sap and leaves. The sap is tapped as a drink or processed into sugar. The palm leaves are used as a roof or woven as a craft material. Lontar is dried siwalan or tal leaves and used as material for manuscripts and crafts[3].

2.2 JPG

JPG format is a compressed lossy file format. This makes it useful to save photos at a size smaller than BMP. JPG is a common choice for use on the Web because it is compressed. JPG-shaped images are most often used to display realistic photos that look fine and can still keep the file size low.

2.3 Cryptography

Cryptography comes from the Greek language by combining words from Greek, namely kryptos and graphein. Kryptos means hidden or secret, while graphein means writing. Cryptography is the science of encryption techniques where data is scrambled using an encryption key to become something that is difficult to read by someone who does not have a decryption key[4].

2.4 Rivest Shamir Adleman

RSA stands for Rivest Shamir Adleman. The RSA Algortima was described in 1977 by three people: Ron (R) ivest, Adi (S) Hamir, and Leonard (A) dleman from the Massachusetts Institute of Technology. RSA in cryptography is an algorithm for public key encryption. RSA was the first algorithm suitable for digital signatures as well as encryption, and RSA is one of the most advanced methods in the field of public key cryptography[5].

2.5 PHP

PHP is a programming language used to develop static websites, dynamic websites or web applications. PHP can be inserted between HTML language scripts and other server side language arenas, with that PHP will be executed directly on the server. Meanwhile, the browser will execute the web page through the server which will then receive a "finished result" display in HTML form, while the PHP code itself will not be visible[6[.

2.6 Database (PhpMyAdmin)

PhpMyAdmin is free software written in the PHP programming language which is used to handle MySQL administration via the World Wide Web. PhpMyAdmin is a free (opensource) application / software written in the PHP programming language which is used to handle MySQL database administration via local networks or the internet. phpMyAdmin supports various MySQL operations, including (managing databases, tables, fields, relations, indexes, users, permissions, etc.)[7].

2.7 System Design

a. Flowmap of the running system

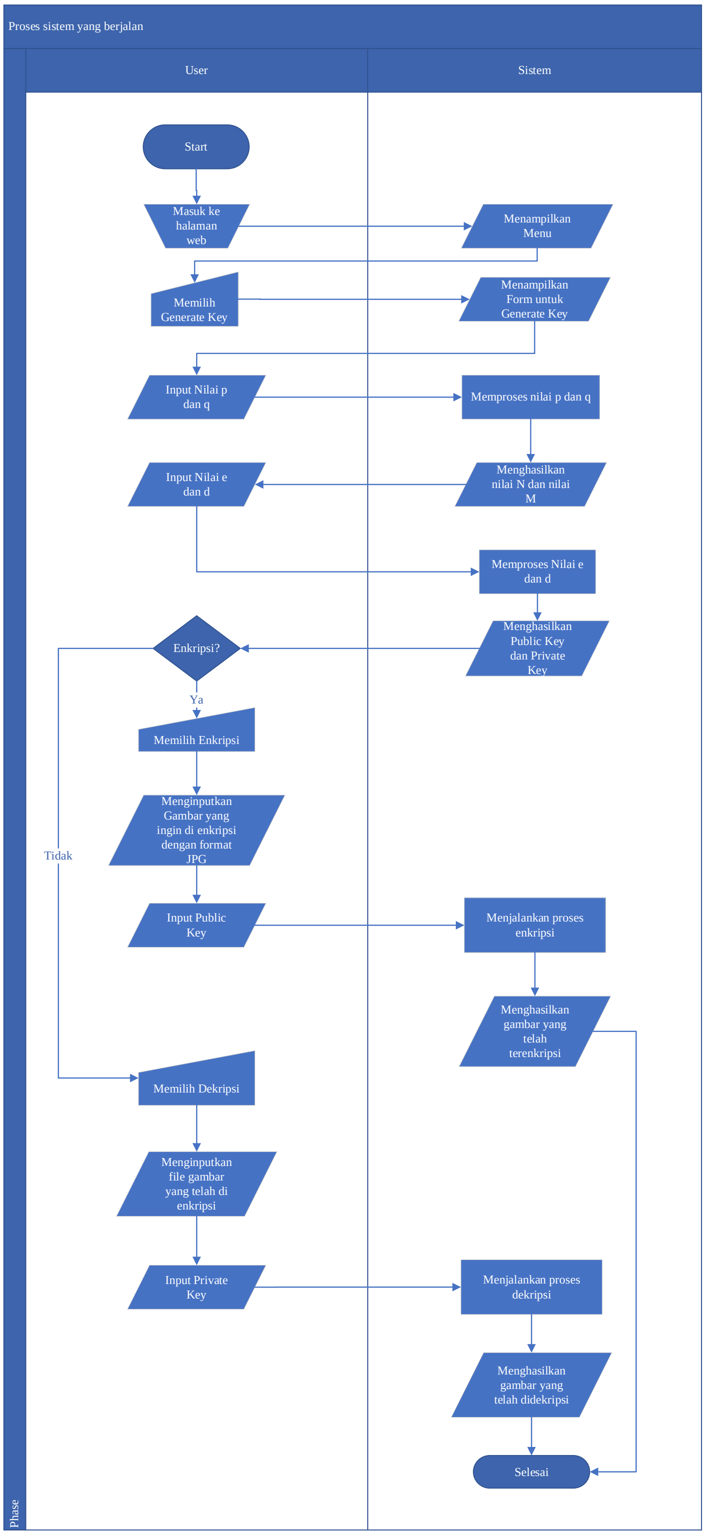

Proses sistem yang berjalan
User
Sistem
Phase
Start
Masuk ke halaman web
Menampilkan Menu
Memilih Generate Key
Menampilkan Form untuk Generate Key
Input Nilai p dan q
Memproses nilai p dan q
Input Nilai e dan d
Menghasilkan nilai N dan nilai M
Memproses Nilai e dan d
Enkripsi?
Menghasilkan Public Key dan Private Key
Ya
Memilih Enkripsi
Menginputkan Gambar yang ingin di enkripsi dengan format JPG
Tidak
Input Public Key
Menjalankan proses enkripsi
Menghasilkan gambar yang telah terenkripsi
Memilih Dekripsi
Menginputkan file gambar yang telah di enkripsi
Input Private Key
Menjalankan proses dekripsi
Menghasilkan gambar yang telah didekripsi
Selesai

Figure 1. Flowmap of The Running System

Description of the system process flowmap is running

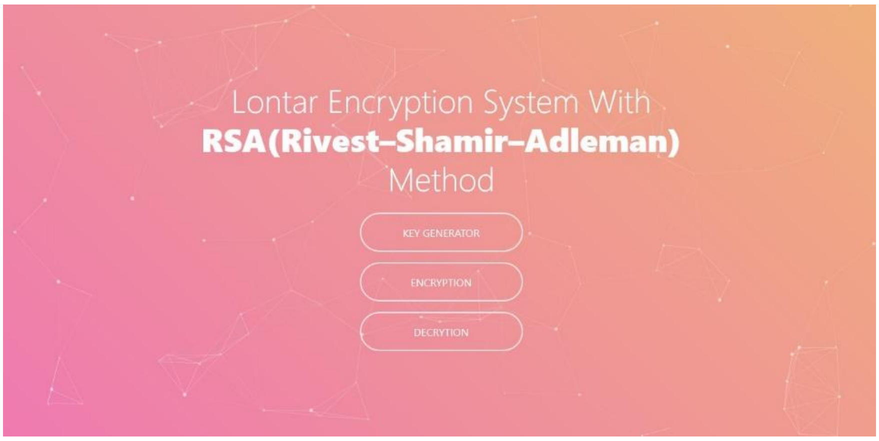
- The user enters a website page, the website user page will see several options that he can choose from.
- The user selects the Generate Key menu.
- Then the system will display a form that will be filled out by the user.
- The user will enter the values for p and q, to get the values for n and m.
- Then the user enters the values d and e, to get the public key and private key.

- After generating the key, the user will choose between the encryption or decryption process.
- If the user selects encryption, the user will provide to insert a palm-shaped image in JGP format.
- Then the user will enter the public key.
- After the user enters the public key and clicks on encryption, the system will run the encryption process and if it is successful the encryption file can be downloaded by clicking the download button.
- If the user chooses decryption, then the user will submit to enter an encrypted file with txt format.
- Then the user will enter the private key.
- After the user enters the private key and clicks on decrypt, the system will run the decryption process and if it is successful the decrypted image file can be downloaded by clicking the download button.

3. Result and Discussion

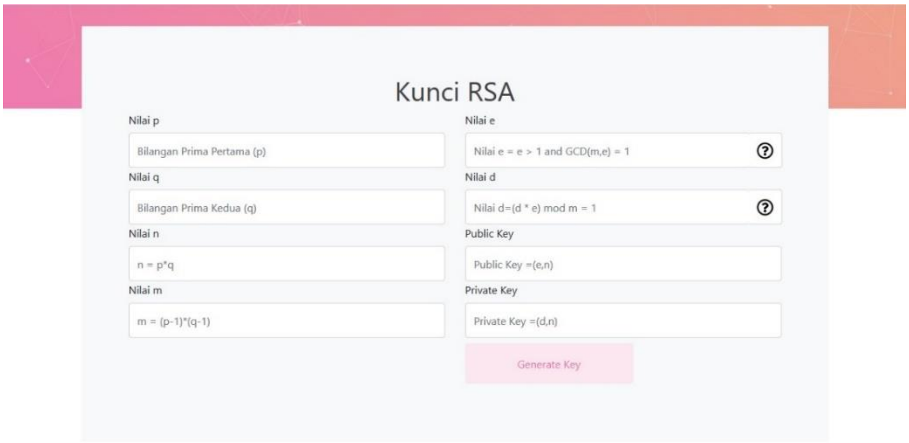
3.1. Appplication View

In the application screen that has been created, there are 4 pages, namely the first page for selecting the menu, the second page for generating the key, the third page for image encryption and the last page for decrypting an encrypted image.



Lontar Encryption System With
RSA(Rivest–Shamir–Adleman)
Method

Figure 2. Homepage



Kunci RSA

Nilai p: Bilangan Prima Pertama (p)

Nilai q: Bilangan Prima Kedua (q)

Nilai n: n = p*q

Nilai m: m = (p-1)*(q-1)

Nilai e: Nilai e = e > 1 and GCD(m,e) = 1

Nilai d: Nilai d=(d * e) mod m = 1

Public Key: Public Key =(e,n)

Private Key: Private Key =(d,n)

Figure 3. Generate Key page display

p-ISSN: 2301-5373
e-ISSN: 2654-5101

In figure 3. The display when the user will generate a key to get a public key and a private key

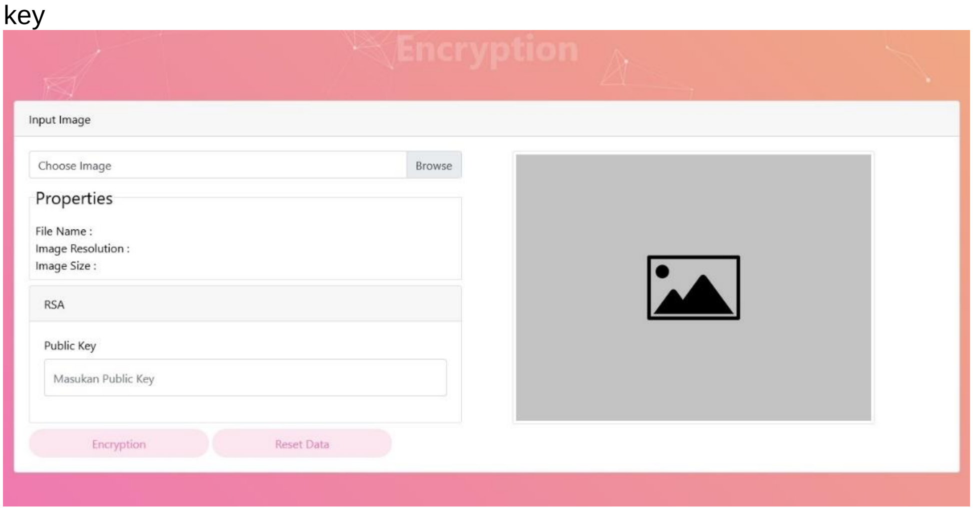


Figure 4. Encryption Page Display

In figure 4. The display when the user will do the image encryption process by entering the image and private key

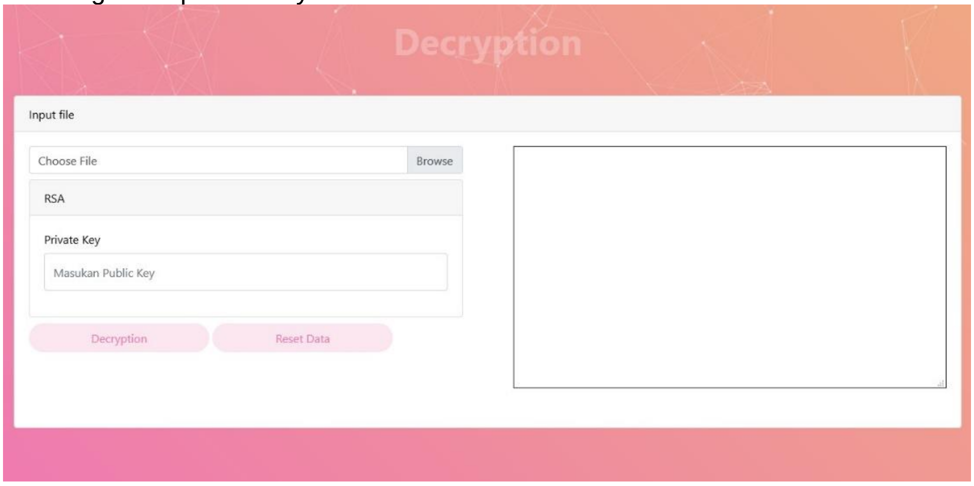


Figure 5. Decryption Page Display

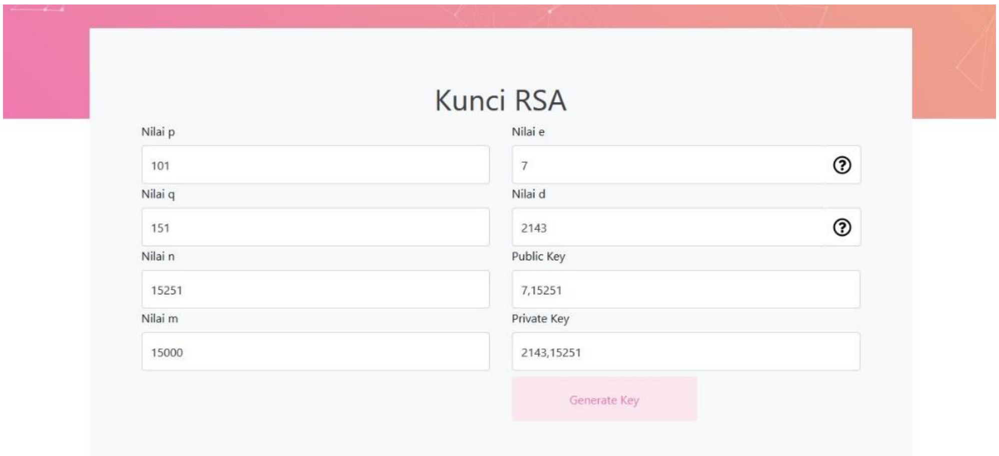
In figure 5. The display when the user will do the file decryption process by entering the encryption file and the public key

3.2. System Testing

Application testing is carried out using black box testing which is used to determine the functionality of the application that has been made.

a. Generate Key

To test whether the system is running properly when generating the key, I enter the values p, q, e and d and the system will generate a public key and a private key.



Kunci RSA

Nilai p: 101

Nilai q: 151

Nilai n: 15251

Nilai m: 15000

Nilai e: 7

Nilai d: 2143

Public Key: 7,15251

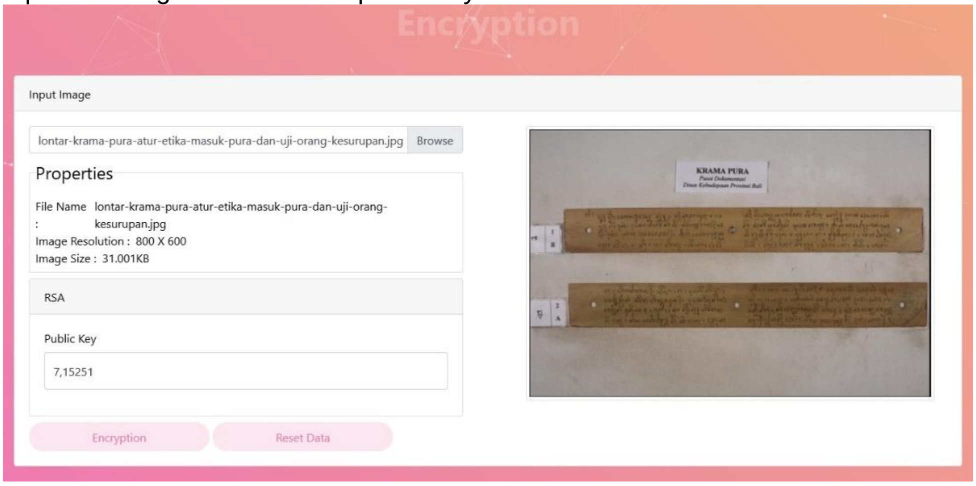
Private Key: 2143,15251

Figure 6. Generate Key Process

In Figure 6., the user will be asked to enter the values for p and q then click generate key and it will generate the values for n and m. After that the user can choose the value e and value d to be entered then click generate key to get the public and private key.

b. Encryption

To test whether the system is running properly at the time of encryption, the author will input the image and enter the public key



Encryption

Input Image

lontar-krama-pura-atur-etika-masuk-pura-dan-uji-orang-kesurupan.jpg

Properties

File Name : lontar-krama-pura-atur-etika-masuk-pura-dan-uji-orang-kesurupan.jpg

Image Resolution : 800 X 600

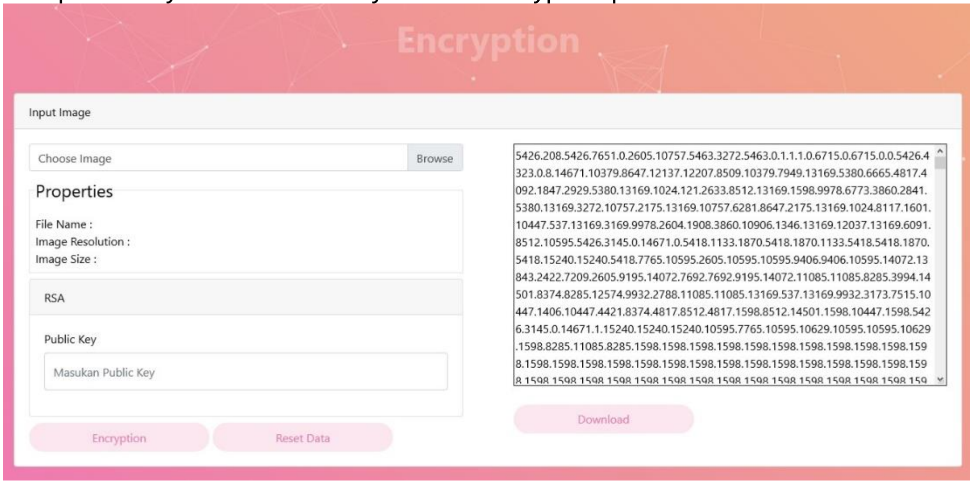
Image Size : 31.001KB

RSA

Public Key: 7,15251

Figure 7. The process of inputting images and public keys

In figure 7. The user enters the image to be encrypted and enters the public key that was previously obtained to carry out the encryption process.



Encryption

Input Image

Choose Image

Properties

File Name :

Image Resolution :

Image Size :

RSA

Public Key: Masukan Public Key

```
5426.208.5426.7651.0.2605.10757.5463.3272.5463.0.1.1.1.0.6715.0.6715.0.0.5426.4
323.0.8.14671.10379.8647.12137.12207.8509.10379.7949.13169.5380.6665.4817.4
092.1847.2929.5380.13169.1024.121.2633.8512.13169.1598.9978.6773.3860.2841.
5380.13169.3272.10757.2175.13169.10757.6281.8647.2175.13169.1024.8117.1601.
10447.537.13169.3169.9978.2604.1908.3860.10906.1346.13169.12037.13169.6091.
8512.10595.5426.3145.0.14671.0.5418.1133.1870.5418.1870.1133.5418.5418.1870.
5418.15240.15240.5418.7765.10595.2605.10595.10595.9406.9406.10595.14072.13
843.2422.7209.2605.9195.14072.7692.7692.9195.14072.11085.11085.8285.3994.14
501.8374.8285.12574.9932.2788.11085.11085.13169.537.13169.9932.3173.7515.10
447.1406.10447.4421.8374.4817.8512.4817.1598.8512.14501.1598.10447.1598.542
6.3145.0.14671.1.15240.15240.15240.10595.7765.10595.10629.10595.10595.10629
.1598.8285.11085.8285.1598.1598.1598.1598.1598.1598.1598.1598.1598.1598.159
8.1598.1598.1598.1598.1598.1598.1598.1598.1598.1598.1598.1598.1598.1598.159
8.1598.1598.1598.1598.1598.1598.1598.1598.1598.1598.1598.1598.1598.1598.159
```

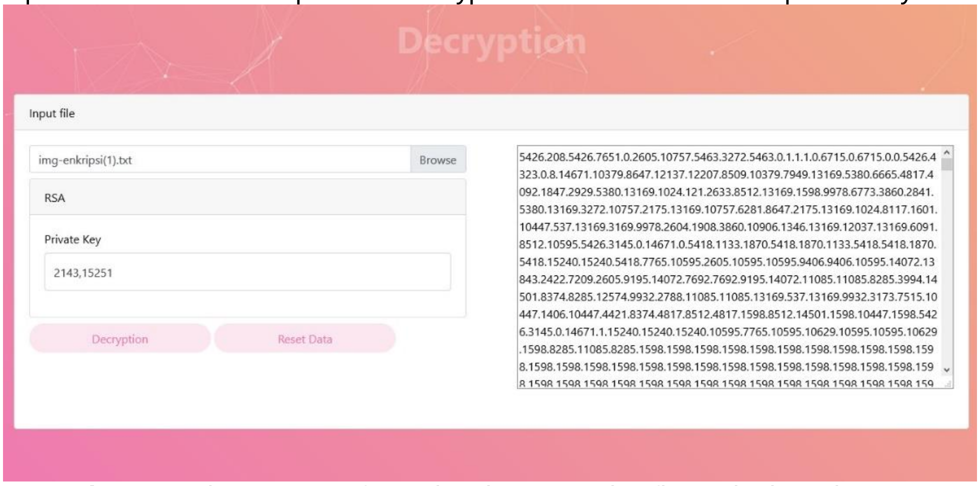
Figure 8. Display of Results After the Encryption Process

p-ISSN: 2301-5373
e-ISSN: 2654-5101

In figure 8, after the user clicks on encryption, the system will run the encryption process and when successful, the system will display the results of the encryption and the user can download the encryption file by clicking the download button

c. Decryption

To test whether the system is running properly at the time of decryption, the author will input the txt file from the previous encryption results and enter the private key.



img-enkripsi(1).txt

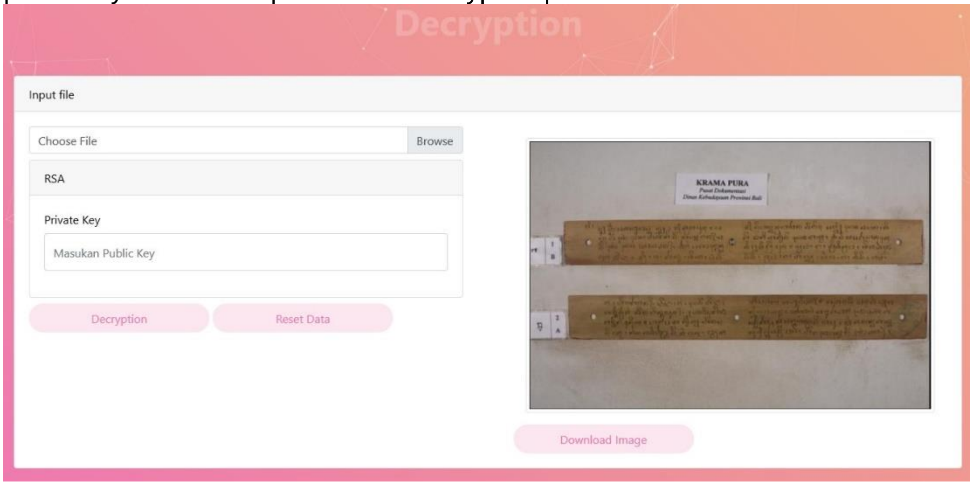
Private Key

2143,15251

```
5426.208.5426.7651.0.2605.10757.5463.3272.5463.0.1.1.1.0.6715.0.6715.0.0.5426.4
323.0.8.14671.10379.8647.12137.12207.8509.10379.7949.13169.5380.6665.4817.4
092.1847.2929.5380.13169.1024.121.2633.8512.13169.1598.9978.6773.3860.2841.
5380.13169.3272.10757.2175.13169.10757.6281.8647.2175.13169.1024.8117.1601.
10447.537.13169.3169.9978.2604.1908.3860.10906.1346.13169.12037.13169.6091.
8512.10595.5426.3145.0.14671.0.5418.1133.1870.5418.1870.1133.5418.5418.1870.
5418.15240.15240.5418.7765.10595.2605.10595.10595.9406.9406.10595.14072.13
843.2422.7209.2605.9195.14072.7692.7692.9195.14072.11085.11085.8285.3994.14
501.8374.8285.12574.9932.2788.11085.11085.13169.537.13169.9932.3173.7515.10
447.1406.10447.4421.8374.4817.8512.4817.1598.8512.14501.1598.10447.1598.542
6.3145.0.14671.1.15240.15240.15240.10595.7765.10595.10629.10595.10595.10629
.1598.8285.11085.8285.1598.1598.1598.1598.1598.1598.1598.1598.1598.1598.159
8.1598.1598.1598.1598.1598.1598.1598.1598.1598.1598.1598.1598.1598.1598.159
8.1598.1598.1598.1598.1598.1598.1598.1598.1598.1598.1598.1598.1598.1598.159
```

Figure 9. The process of entering the encryption file and private key

In figure 9, the user enters the file to be described and enters the private key that was previously obtained to perform the decryption process.



Choose File

Private Key

Masukan Public Key

Figure 10. Display Results After the Decryption Process.

In figure 10, after the user clicks decryption, the system will run the decryption process and when successful, the system will display the results of the decryption and the user can download the files that have been decrypted by clicking the download button

4. Conclusion and Suggestions

4.1 Conclusion

From the explanations that have been made in the previous chapters, it can be concluded that the lontar is an ancient manuscript that must be preserved and preserved so that these lontars can be used for the continuation of future generations. The lontar data can be stored and encrypted using a cryptographic security system, namely Rivest Shamir Adleman.

In this system, the analysis and design process has been successfully carried out. The analysis process involves diagrams, namely flowmaps. Implementation of the design into coding using the PHP programming language with the Laravel framework, the database using MySQL, and for display design using the Bootstrap CSS framework, resulting in an image security system that can generate keys to get public and private keys, encryption and image decryption.

4.2 Suggestions

a. In this web development, it is hoped that it will be able to encrypt images with different formats such as PNG.

b. Can be used as a reference for developing a mobile version of the application for encryption and decryption of palm-leaf images.

References

[1] Munir, Rinaldi. (2006). “Diktat Kuliah IF2153 Matematika Diskrit. Program Studi Teknik Informatika, Institut Teknologi Bandung.

[2] Fahreza, Harbani (2019). Jurnal Ilmiah Teknologi – Informasi dan Sains. “Aplikasi Keamanan Data Gambar Menggunakan Algoritma RSA (Rivest Shamir Adleman” Berbasis Desktop. Volume 9 Nomor 1 Bulan Mei 2019 Hal. 1-9. p-ISSN : 2087-3891 dan e-ISSN : 2597-8918

[3] Sedana, Damayanti dan Khadijah. (2013). Jurnal Kajian Informasi & Perpustakaan. “Preservasi Berbasis Kearifan Lokal (Studi Kasus Mengenai Preservasi Preventif dan Kuratif Manuskrip Lontar Sebagai Warisan Budaya di Kabupaten Klungkung Bali)”. Vol.1/No.1, Juni 2013, hlm 91-105.

[4] Eka Adhitya Dharmawan, Erni Yudaningtyas, M. Saora, Juni 2013, “Perlindungan Web pada Login Sistem Menggunakan Algoritma Rijndael” Jurnal EECCIS, Vol. 7, No.1.

[5] Sentot Kromodimoeljo, Desember 2009, Teori & Aplikasi Kriptografi, SPK IT Consulting

[6] KM. Syarif Haryana, Juni 2008, “Pengembangan Perangkat Lunak dengan Menggunakan PHP”, Jurnal Computech & Bisnis, Vol. 2, No. 1, 14-21 ISSN 1978-9629

[7] Rahmawati Erma Standsyah, Intannia Sari Restu N.S., “Implementasi PHPMyAdmin pada Rancangan Sistem Pengadministrasian”. Jurnal UJMC, Volume 3, Nomor 2, Hal. 38 - 44 pISSN : 2460-3333 eISSN : 2579-907X