International Journal of Research in Engineering, Science and Management
Volume 4, Issue 6, June 2021
https://www.ijresm.com | ISSN (Online): 2581-5792

A Novel Approach for Encryption and Decryption by RSA Algorithm in Secure Multimedia Communication

Parvathy Kaladhar Kalabhavan[1*], Bijin Bodheswaran[2]
[1]*Student, Department of Electronics and Communication Engineering, Sree Buddha College of Engineering, Pathanamthitta, India*
[2]*Assistant Professor, Department of Electronics and Communication Engineering, Sree Buddha College of Engineering, Pathanamthitta, India*

***Abstract*: Now-a-days the data security becomes one of the most crucial issues that are being addressed by this digital world. With the further developments in the IT evolution, the data can be secured in many ways. For a system end – to – end encryption is the most widely used method for providing security for the entire communication. In this paper, we propose a novel approach for the transmission of data using RSA asymmetric cryptographic algorithm through a web application over a secured channel. The proposed system provides the advantages of both SHA 256 and RSA algorithm. The proposed system transfers a large number of data in a quicker way.**

***Keywords*: Data security, end-to-end encryption, RSA asymmetric cryptographic algorithm, secure hash algorithm 256 (SHA 256), web application.**

1. Introduction

By the rapid increase in the use of multimedia communications, the data security has become crucial issue in this digital world. Consequently, the hackers and attackers are gradually increasing, more secured data transmission methods are to be implemented. The secured data transmission deals with the transfer of confidential information over a secure channel. There are several secure transmission methods to provide security in entire communication process.

This paper proposes the method of transmitting data securely in an application over a secured channel. For this, each user has to register in the application by creating username and password and hence the user can login to the application. This password is hashed by the hashing algorithm and hence key is generated. Hashing is the basic building block for secure password storage. This hashed value is stored into the database. When a user attempts to login, it takes the password given by user and performs a one – way hash and compares it to the database value. If the password matches, then the login is successful.

After the successful login, the user (sender) can upload any data which is stored in the application to transmit to any other user by RSA cryptographic algorithm. In here, the data is an image and this image can be transmitting to other users. For that, the sender selects the image from the device and uploads it. After the successful uploading process, the image is then converted into a plain text and transmits by the RSA algorithm.

The hashing algorithm commonly used is SHA 256. It provides more secure communication between the user and the server to login properly. The SHA 256 is a kind of signature for a text or a data file. The SHA 256 generates an almost – unique 256 – bit signature for a text. The authentication and encryption protocols, like SSl, TLS, IPsec, SSH and PGP works on SHA 256.

The biggest critical advantage of using RSA algorithm is that it is a public – key cipher, and this makes it a lot easier to solve the fundamental problem of cryptography, which is safely to distribute the keys. The public key systems can provide digital signatures that cannot be repudiated. It provides a way to ensure that electronic message and data storage are kept secret, complete, and accurate.

By using these two algorithms together the entire communication become more secured and hence thereby prevent hacking attacks, intrusion, spoofing, etc. The personal confidential data can be transmits to any others who are already logged in the application.

2. Literature Survey

Recently, there are many methods to implement the secured data transmission over a secured channel by the development of the new technologies. Omer Mert Candan, Albert Levi, Cengiz Togay [1] proposes a key distribution mechanism for WebRTC peers based on hash chains. This mechanism produces keys on both ends synchronously without any initial interaction. This method eliminates communication overhead and increase the security during the key exchange process. Xin Zhou, Xiaofei Tang [2] proposes the implementation and study of RSA public key algorithm. And also gives the details of encryption procedure and code implementation based on NET platform. Rajeev Sobti, Geetha Ganesan [3] introduces the features of hash functions, its various structures and the progressive

*Corresponding author: parvathyvinums@gmail.com

development in this field. The hash function is a function that takes an input data of arbitrary size and produces a fixed sized output. The hash functions are commonly used for authenticity, digital signatures, pseudo random generators and digital stamping. Abbas Cheddad, Joan Condell, Kevin Curran, Paul Mckevitt [4] describes a mechanism for providing the password protection to the digital images by using 1D SHA 2 algorithm. A spatial mask is formed and is XORed with the bit stream of the original digital image. Lamport L [5] defines a mechanism for providing user password authentication in the entire communication between the user and the system. This system focuses on a secure one – way encryption function, which can be implemented in the user's terminal. Tejaswini Bhorkar [6] focuses on the authentication process of the user by login to a web application by using their own provided username and password and checks if the given username and password already exist in the database and that the password is identical to the password set by that user. The user password may be directly stored in the database or the hash value of the password may be stored. Seyed Mohammad Seyedzade, Reza Ebrahimi Atani, Sattar Mirzakuchaki [7] explains the image encryption using SHA 512 and aims to increase the image entropy. The algorithm firstly, preprocesses to shuffle one half of the image and generate a random number mask using hash function. Then the mask is XORed with the other part of the image to encrypt.

3. Proposed System

A. Account creation

Each user has to create an account in this application by creating username and password. The password which is creating should be high confidential. The password is created must follow the instructions listed in the application form. Thereby creating an account, the user can login to the application using the user credentials.

B. Password hashing

Hashing is one – way cryptographic function that validates the authenticity and integrity of various inputs. It is commonly used to avoid storing plain text passwords in databases, but also is used to validate the files, documents and other data. Hash functions are irreversible. The output of a hash function is a fixed - length string of characters called hash value, digests or simply hash. One of the important properties of hash function is that when hashed a unique input, the result will be the same hash value. Hashing is almost used to encrypt when storing passwords inside databases. When a user attempts to log in, it takes the supplied password, performs a one – way hash and compares it to the database value. If these two passwords match, the login is successful.

C. Uploading image

After the successful login of the user, the upload the image form the device. The user can decide to whom which the image has to send. The uploaded image is then transmitted to the receiver by RSA asymmetric cryptographic algorithm. Before the transmission, the image is converted to the plain text by converting the pixels of the image directly into text files. These txt files are encrypted and transmitted across the channel.

D. RSA Algorithm

RSA asymmetric cryptographic algorithm is a public key cryptographic algorithm which uses two types of keys namely, public and private keys. The public keys are provided to everyone and are used to encrypt the message. But the private key is provided only for receiver and is used for decrypt the encrypted data. The public and private keys generation is the most complex part of RSA cryptography.

RSA derives its security from the difficulty of factoring large prime numbers. Multiplying these two numbers is easy, but determining the original prime numbers from the total – or factoring is considered unfeasible due to the time using even todays supercomputers.

1) Key Generation

The key is generated by the following steps:

1. Choose two different large prime numbers *'p'* and '*q'* and should be kept secret.
2. Calculate the modulus for both the keys: $n = p * q$
3. Calculate the totient function: $\Phi(n) = (p-1)(q-1)$.
4. Choose an integer *e* such that, $1 < e < \Phi(n)$ and *e* is the co – prime to $\Phi(n)$. The e is the public key exponent.
5. Compute the private key, d to satisfy the congruence relation $de = 1 + x.\ \Phi(n)$ for some integer *x*.

2) Encryption

Before the encryption process, the image is converted to the text files. This text files are given to encryption process. Firstly, the user sends the public key (n,e) to the receiver. The user divides the plain text M into smaller texts, m using the protocol named padding scheme. To maintain the security in the numerical structure of RSA encryption, the padding scheme is used. It increases the size of the message and it perceives pseudo – random information that encrypted to a wide range of different cipher texts. The cipher text is determined by the equation, $c = m^{e} \bmod n$.

3) Decryption

Given m, the receiver can recover the original distinct prime numbers by applying the Chinese Remainder Theorem (CRT). It states that, by knowing the remainders of the Euclidean division of an integer n by several integers, and then it can determine uniquely the remainder of the division of n by the product of these integers under the condition that the divisors are pairwise co – prime. The receiver knows only private key, *d*. The original message is recover by the following equations:

$M^{ed} = m \bmod (p * q)$

Thus, $c^{d} = m \bmod n$

Therefore, $m = c^{d} \bmod n$.

Therefore, the decrypted data is converted to the original image and can be retrieved by the receiver by this algorithm. The encryption and decryption are more secured because of the strong key generation process of public and private keys.

4. Results

By running the command "py manage.py runserver" in the command window of the Pycharm, a link that consists of

application site will appear as shown in the fig. 1.

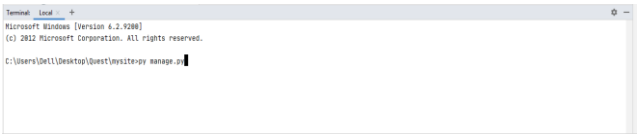

Fig. 1. Terminal view of the Pycharm

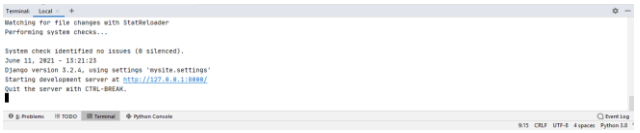

Fig. 2. Link description

By clicking on the link a new web page will appear as shown in the Fig. 2. Hence a new application web page will appear as seen in fig. 3.

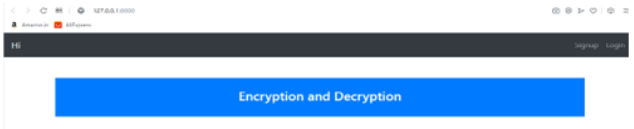

Fig. 3. Application web page

For the account creation, the user has to sign up and create the username and password in the registration form as shown in the fig. 4.

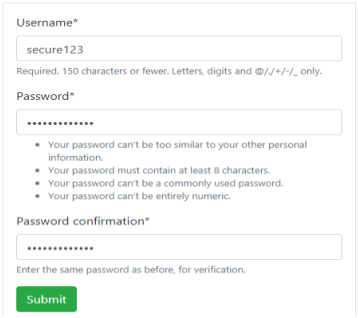

Fig. 4. Registration form

By creating username and password, the user can successfully login to the application site. The user can upload an image that has to be sending from the device and can select the receiver.

Fig. 5. Image uploading page

The input image shown in the fig. 6 is given to the encryption process and an encrypted image shown in the Fig. 6 is formed by RSA asymmetric cryptographic algorithm. This encrypted image is transmitted along with the generated public key to the receiver and the receiver decrypts the image by the generated private key and forms decrypted image as shown in the Fig. 7 and hence the original image is retrieved by the receiver.

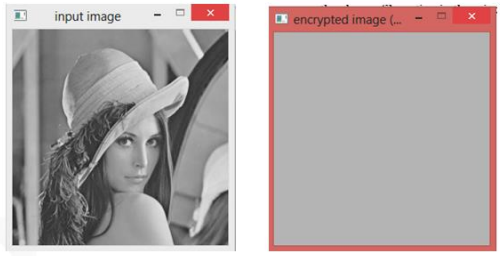

Fig. 6. Input and encrypted images

Fig. 7. Decrypted image

5. Conclusion and Future Work

The system provides more secured transmission over a channel. Each user can login to the application by creating the username and password securely. Using the hash algorithm, the user can login successfully by preventing any type of hacking attacks. The RSA algorithm provides more security while transmitting the data and also it generates the public and private keys more complex to preventing the hacking issues. The future work can include by adopting this mechanism over the mobile phones and increasing the number of data that has to be transmit and also increases the number of receivers to transmit the data to different receivers at a time.

References

[1] Omer Mert Candan, Albert Levi, Cengiz Togay, "Generating One – Time Keys for Secure Multimedia Communication," in *IEEE International Conference on Communications Workshops (ICC Workshops)*, May 2018.

[2] Xin Zhou and Xiaofei Tang, "Research and Implementation of RSA Algorithm for Encryption and Decryption", in *Proceedings of 2011 6th International Forum on Strategic Technology*, 2011.

[3] Rajeev Sobti, Geetha Ganesan," Cryptographic Hash Functions: A Review "*IJCSI International Journal of Computer Science Issues*, vol. 9, no. 2, March 2012.

[4] Abbas Cheddad, Joan Condell, Kevin Curran, Paul Mckevitt, "A hash-based image encryption algorithm", October 2009.

[5] Lamport, L. "Password authentication with insecure communication". In: Commun. ACM 24.11 (1981), pp. 770–772.

[6] Tejaswini Bhorkar, "A Survey of Password Attacks and Safe Hashing Algorithms", *International Research Journal of Engineering and Technology*, vol. 4, no. 12, Dec. 2017.

[7] Seyed Mohammad Seyedzade, Reza Ebrahimi Atani, Sattar Mirzakuchaki, "A Novel Image Encryption Algorithm Based on Hash Function," *6th Iranian Conference on Machine Vision and Image Processing*, October 2014.

[8] Samir Brahim Belhaouari, Shaheen Saad Al-Kaabi, "Methods Toward Enhancing RSA Algorithm: A Survey," in *International Journal of Network Security & Its Applications*, vol. 11, no.3, May 2019.

[9] Sudhansu Bala Das, Sugyan Kumar Mishra and Anup Kumar Sahu, "A New Modified Version of Standard RSA Cryptography Algorithm," April 2020.

[10] Ljupco Kocareva and Marjan Sterjev, "Public-key encryption with chaos," in *Interdisciplinary Journal of Nonlinear Science*, 2004.