7th National Conference on
"Role of Engineers in Nation Building" organized by VIVA Institute of Technology, Mumbai
(1st and 2nd March 2019)
International Journal of Engineering Research & Science (IJOER)
ISBN: [978-93-5321-411-1] ISSN: [2395-6992] [Vol-5, Issue-3, March- 2019]

Image encryption using RSA algorithm and additive cipher

Karishma Raut[1], Archana Ingle[2], Madhura Ranade[3]

Department of EXTC, VIVA Institute of Technology, Virar

Abstract**—** *Cryptographic techniques are of prime importance for security of data communication. Data can be text, image, and video. Data integrity and confidentiality are main aspects of information security. As asymmetric cryptography uses two different keys for encryption and decryption, key becomes secured which ensures data security. RSA is a most significant approach which resists brute force attack. Images can be made more secure using simple additive cipher as a second level encryption. The paper describes combination of asymmetric and symmetric cryptography working together to enhance the image security. RSA algorithm for image encryption with additive ciphering with self-generated key.*

Keywords— asymmetric cryptography, decryption, encryption, key, RSA algorithm**.**

I. INTRODUCTION

Cryptography is the practice of storing and communicating data in such a form that only whom it is intended for can read and process it. In cryptography the data to be transmitted is encoded into an unreadable format using certain algorithms so that it cannot be used and modified to produce unauthorized effects.

Modern cryptography is based on mathematical theory and such cryptographic algorithms are hard to break by an adversary. Symmetric and asymmetric (public) key cryptography exists in parallel and are complements of each other. The conceptual difference between the two systems are based on how these systems uses key. In symmetric key method both the sender and the receiver use the same single key for both encryption and decryption purposes. Whereas in asymmetric key method the sender and the receiver use different keys [1, 2].

Asymmetric algorithms rely on one key for encryption and a different but related key for decryption. It is computationally infeasible to determine the decryption key with given knowledge of the cryptographic algorithm and the encryption key. Also either of the two related keys can be used for encryption, with the other used for decryption [2, 3].

The best known and widely used public key system is RSA algorithm named for its inventors Ron Rivest, Adi Shamir, and Len Adelman. It is based on modular exponentiation. Its security is based on the difficulty of the large number prime factorization, which is a well-known mathematical problem that has no effective solution [3, 4, and 5].

II. RSA CRYPTOSYSTEM AND ADDITIVE CIPHER

The cryptography techniques are classified as symmetric and asymmetric key. Symmetric key cryptography. In symmetric key cryptography both the sender and the receiver know the same secret key. The sender is encrypting the data or the information using the secret key and the receiver is decrypt the information using the same secret key. In the symmetric cryptography the key is playing a very important role which is depends on the nature of key. Additive cipher is a symmetric cipher [1].

Asymmetric key cryptography uses pair of keys for encryption and decryption. RSA algorithm is asymmetric cipher.

RSA makes use of an expression with exponentials. Plaintext is encrypted in blocks, with each block having a binary value less than some number n [6, 7].

RSA key generation

International Journal of Engineering Research & Science (IJOER)
ISBN: [978-93-5321-411-1] ISSN: [2395-6992] [Vol-5, Issue-3, March- 2019]

{

Select two large prime numbers p and q such that p≠q //Primality testing

n=p*q

Ø (n) =(p-1)*(q-1)

Select e such that 1<e< Ø (n) and e is coprime to Ø (n) //e is selected using pseudo randomly

$d=e^{-1} \bmod Ø(n)$ // use of extended Euclid's algorithm

Public key = {e, n} and private key= {d, n}

}

RSA encryption

{

$C=M^e \bmod n$ // use of fast exponentiation algorithm

}

RSA decryption

{

$M=C^d \bmod n$ // use of fast exponentiation algorithm

}

Example:

Key generation:

Select p=11 and q=17

n=p*q=11*17=187

Ø (n) = (p-1)*(q-1) = (11-1)*(17-1) =160

Select e=7

$d=e^{-1} \bmod Ø(n)=7^{-1} \bmod 160=23$

Encryption:

Let plaintext to be encrypted is M=88

$C=M^e \bmod n=88^7 \bmod 187 =11$

International Journal of Engineering Research & Science (IJOER)
ISBN: [978-93-5321-411-1] ISSN: [2395-6992] [Vol-5, Issue-3, March- 2019]

Decryption:

$M=C^d \bmod n = 11^{23} \bmod 187 = 88$

The algorithm can work efficiently on text as well as image and video.

Additive cipher is also known as shift cipher. It is mostly used for text encryption. Mathematically it can be described as follows

Encryption of data

C=P+K // P is original data, C is encrypted data and K is key

Decryption of data

P=C-K

Example: P=13, K=15

C=P+K=13+15=28

Recovered data is

P=C-K=28-15=13

III. DUAL ENCRYPTION USING RSA ALGORITHM IN MATLAB

The proposed system uses double encryption to secure images. First stage of encryption is to encrypt image using RSA algorithm and second stage is to encrypt again using additive cipher. There is no need to generate key externally for additive ciphering. Image itself generates key by sum of image pixels. The sum is also encrypted in asymmetric manner and send in image itself. It automatically avoids brute force attack as there is no question of identification of key.

Algorithm

At sender

1. Generate public and private keys for encryption
2. Generate sum of image pixels in modulo n
3. Encrypt image and sum using public key
4. Encrypt image using additive cipher with sum as a key and send encrypted value of sum in image itself.

At receiver

1. Extract sum from image and decrypt it using private key.
2. Decrypt image using additive cipher with sum as a key.
3. Decrypt image using private key.

International Journal of Engineering Research & Science (IJOER)
ISBN: [978-93-5321-411-1] ISSN: [2395-6992] [Vol-5, Issue-3, March- 2019]

IV. RESULTS AND DISCUSSION

The proposed method is implemented on different images and for different key values. The output of encryption and decryption is as shown below

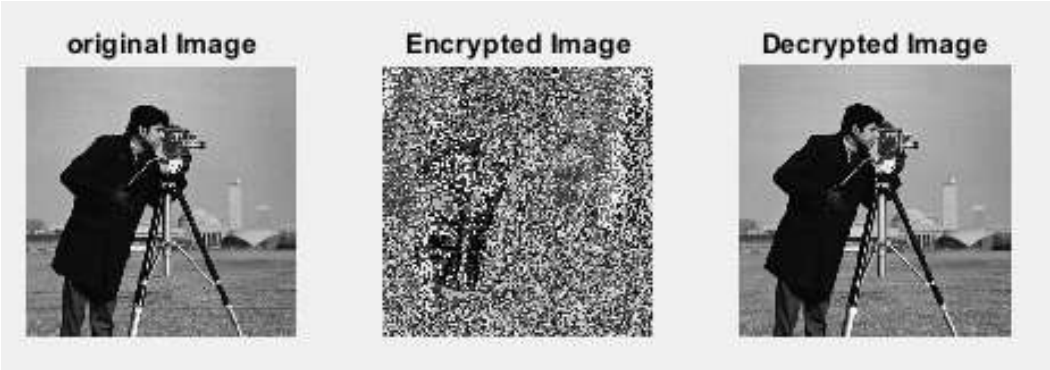

Fig. No. 1 RSA encryption without additive ciphering

The output of RSA encryption depends on key used for encryption and decryption. Also with smaller values of keys Image recovery is poor. This can be further improve by second level encryption using additive cipher and result for same key values is as shown below.

Fig. No. 2 RSA encryption with additive ciphering

The time required for encryption, decryption and key generation is noted for same key values.

Table No.1
Comparison of methods with respect to execution time

Method	Key generation time(Seconds)	Encryption time (Seconds)	Decryption time(Seconds)
RSA without additive cipher	0.006594	0.678249	0.689156
RSA with additive cipher	0.006570	0.686442	0.688070

It is seen that time required to encrypt and decrypt is not much affected.

V. CONCLUSION

In this paper combination of symmetric and asymmetric key techniques is used to enhance security of images. The key is generated from input image and also carried by image for additive cipher. Hence there is no extra overhead to share key. The

International Journal of Engineering Research & Science (IJOER)
ISBN: [978-93-5321-411-1] ISSN: [2395-6992] [Vol-5, Issue-3, March- 2019]

results showed that RSA along with additive cipher provides highest security to images.

REFERENCES

[1] Behrous Forouzen, "Cryptography and Network Security", Tata Mc Graw –Hill Education 2011.

[2] William Stallings, "Cryptography and Network Security", Pearson Education Asia Publication, 5th edition

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

[4] Ali E. Taki El_Deen, El-Sayed A. El-Badawy, Sameh N. Gobran, "Digital Image Encryption Based on RSA Algorithm", IOSR Journal of Electronics and Communication Engineering (IOSR-JECE), (Jan. 2014), PP 69-73

[5] Borko Furht, Darko Kirovski, "Multimedia Encryption and Authentication Techniques and Applications", ISBN: 0-8493-7212-7, 2006.

[6] Andreas Uhl, Andreas Pommer, "Image and Video Encryption from Digital Rights Management to Secured Personal Communication", ISBN: 0-387-23403-9, Springer, 2005.

[7] Jonathan Katz, Yehuda Lindell, "Introduction to Modern Cryptography: Principles and Protocols", ISBN: 978-1-58488-551-1, 2008.