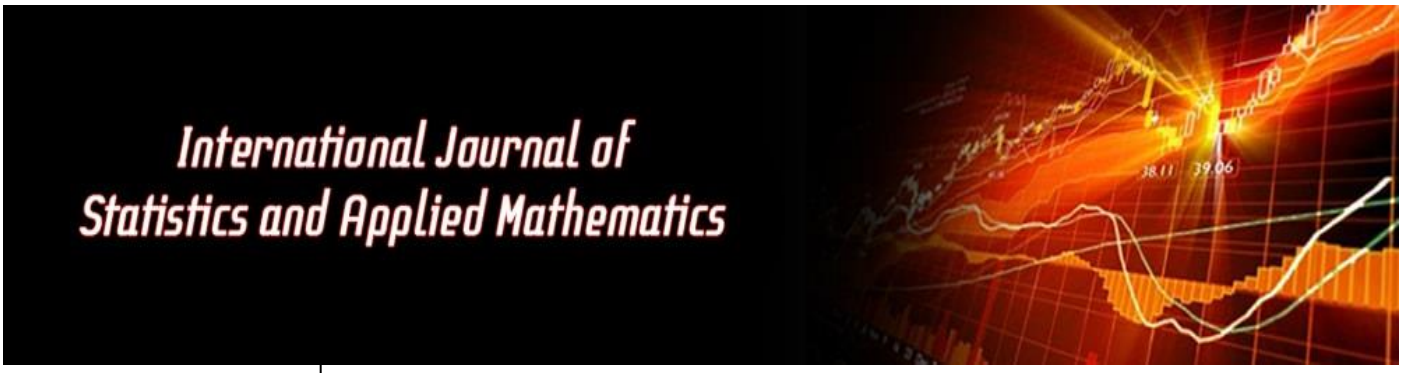
International Journal of Statistics and Applied Mathematics 2024; 9(2): 113-115



ISSN: 2456-1452
Maths 2024; 9(2): 113-115

https://www.mathsjournal.com
Received: 14-01-2024
Accepted: 22-02-2024

Kamal Kumar
Department of Mathematics, BMU, Rohtak, Haryana, India

Manoj Sharan
Department of Mathematics, BMU, Rohtak, Haryana, India

Inderjit Singh
Department of Mathematics, Dayanand P.G. College, Hisar, Haryana, India

Corresponding Author:
Kamal Kumar
Department of Mathematics, BMU, Rohtak, Haryana, India

Image encryption and decryption using affine-RSA cryptosystem

Kamal Kumar, Manoj Sharan and Inderjit Singh

Abstract
In this paper we proposed a technique to encrypt and decrypt a color image using Affine-RSA cryptosystem, the encrypted image pixels are again encrypted using RSA. We focus mainly on increasing the layers of encryption and hence increasing the complexity of decryption performed by attacker. Three different layers of encryption can protect original message more efficiently.

Keywords: Cryptography, affine cipher, encryption, decryption, RSA

1. Introduction
Cryptographic systems are used extensively to ensure secrecy and authenticity of sensitive information. Cryptography allows us to transmit data in such a way that it is understood only at the receiver end. The original image data is the plaintext, which must be kept secure. This is encrypted into the cipher-text (encrypted image data), which is then transmitted through unsecured network. At the receiver end, transmitted data is decrypted back into the plaintext. The aim of cryptography is to ensure high end communication between the sender and receiver without any loss of information. Security, refers to the following aspects-confidentiality, data integrity, authentication and non-repudiation. Cryptanalysts try to break the security of data, and this process is known as hacking. There are several techniques by which image data may be encrypted and decrypted. But the security of color images by the proposed cryptosystem is developed by affine hill cipher over SLn(Fq) and Mn(Fq) domains with Arnold transformation.. How-ever, according to, recent studies for the security of RGB images, some attacks such as: brute-force attack, cropping attack, noise attack, etc. can penetrate the security (robustness) of the cryptosystem. The proposed cryptosystem is free from such types of attacks. In this paper, we proposed a technique to encrypt and decrypt a color image using Affine-RSA cryptosystem, the encrypted image pixels are again encrypted using RSA.

2. Affine Cipher
An affine cipher is a type of substitution cipher where each letter in an alphabet is mapped to its numeric equivalent, encrypted using a simple mathematical function, and then converted back to a letter. The formula used means that each letter is replaced by another letter according to a modular arithmetic operation.

The general formula for encrypting a letter x using an affine cipher is:
$E(x) = (ax + b) \bmod m$

Where:
E(x) is the encrypted letter.
x is the numerical value of the original letter.
a and b are the keys of the cipher (integers).
m is the size of the alphabet (number of letters).

Here's a simple example
Let's use the English alphabet with capital and small letters ABCDEFGHIJKLMNOPQRSTU

VWXYZ abcdefghijklmnopqrstuvwxyz: m = 52.

Encryption keys: a = 3, b = 5.
Plaintext: "Hello"

First, convert each letter to its numerical equivalent
'H' = 7
'e' = 30
'l' = 37
'l' = 37
'o' = 40

Encrypt each numerical value using the formula
E(x) = (3x + 5) mod 52

Encrypting 'H'
E(7) = (3×7 + 5) mod 52 = (21 + 5) mod 52 = 26 mod 52 = 26
So 'h' encrypts to 'a'.

Encrypting 'e'
E(30) = (3×30 + 5) mod 52 = (90 + 5) mod 52 = 95 mod 52 = 43

So 'e' encrypts to 'r'.
And so on for the remaining letters. Then 'Hello' would be encrypted to 'arMMV'.

3. RSA Cryptosystem
RSA, named after its inventors Rivest, Shamir and Adleman, was proposed in 1977.

Encryption and Decryption schemes of RSA Cryptosystem
RSA (Rivest-Shamir-Adleman) is a widely used public-key encryption algorithm for secure data transmission. Here are the steps involved in the RSA encryption and decryption process:

1. Key Generation
Choose two distinct prime numbers, p and q.
Calculate n = pq.
Calculate Euler's totient function $\phi(n) = (p-1)(q-1)$.
Choose an integer e such that $1 < e < \phi(n)$ and e is coprime with $\phi(n)$
Calculate the private exponent d such that $d*e = 1 \bmod \{\phi(n)\}$. D is the private exponent.

2. Public Key
The public key is (n, e). This key is used for encryption.

3. Encryption
Convert the plaintext message M into an integer m such that 0< m < n.
Compute the cipher text C using the formula $C = m^e \bmod\{n\}$.

4. Message Transmission
Transmit the cipher text C to the recipient.
These are the fundamental steps involved in the RSA algorithm for encryption. It relies on the mathematical properties of modular arithmetic and the difficulty of factoring large prime numbers for its security.

5. Encryption and Decryption Scheme of Affine-RSA

$M \rightarrow (\text{Affine Cipher Enc})CG \rightarrow (\text{RSA Enc})C1$
$\rightarrow (\text{RSA Dec})C2 \rightarrow (\text{Affine Cipher Enc})CG \rightarrow M$

In this chapter, we present the encryption part of the above scheme.

Step 1
Consider the image for encryption

Step 2
Let Affine parameters are

$a = 59, b = 143$

Then the encrypted image is given below

Step 3
Let the public key of RSA is n =2210878273, e = 37627 (encryption exponent) public-key = (n,e) then by using the above RSA parameters the pixel values of the image obtained in Step 2 are encrypted in following array:
[1020229085, 1406739600, 1802623639, 290438432, 504569576, 933709452, 449471170, 804652920, 672093019, 1589524938, 2187239216, 1629844004, 1299978970, 1934182793, 455498990, 1917956647, 1854872587, 448033728, 178799911,…….. 2141241370, 283151930, 523934217, 2040256513, 1680235323, 1496023048, 1397649312]

5. Encryption and Decryption Scheme of Affine-RSA
$M \rightarrow (\text{Affine Cipher Enc})CG \rightarrow (\text{RSA Enc})C1$
$\rightarrow (\text{RSA Dec})C2 \rightarrow (\text{Affine Cipher Enc})CG \rightarrow M$

In this chapter, we present the decryption part of the above scheme.

Step 1
The private key of RSA is N =2210878273, d = 1947497683 (decryption exponent) private_key = (n,d) then by using the above private key the decrypted pixel array of the encrypted pixel array obtained Step 3 of Chapter 4 is given below
[7565066, 11461898, 2397824, 4918321, 4918380, 13992556, 14007719, 4978914, 4978717, 4928285,

16543438,…. 6710886, 11842740, 11776947, 7895160, 131586, 10658466, 5395026, 1381653, 13290186]

The corresponding image of the above decrypted pixel array is given below

Step 2

Decryption Affine parameters corresponding to encrypted parameters $a = 59, b = 143$ are

$c = 243, b = 113$

Then the decrypted image is given below

6. Security Analysis

- The proposed techniques will not have effect of Brute Force and other Cryptanalytic attacks as different layers of security are generated for the image.
- There is no effect of Integer Factorization because n size is very large.
- To break this technique cannot be an easy task for external adversaries even they are using supercomputers.
- The algorithm proposed will take less time also.
- This also can be used for most crucial applications where it requires a significant security of transmitting images.

References

1. Mishra DC, Sharma RK, Ranjan R, Hanmandlu M. Security of RGB image data by affine hill cipher over SLn(Fq) and Mn(Fq) domains with Arnold transform. Optik. 2015;126:3812-3822.
2. Mishra DC, Sharma RK. Grayscale-image encryption using random hill cipher over SLn(F) associated with discrete wavelet transformation. AAM. 2013;8:777–791.
3. Boneh D, Franklin M. Identity-based encryption from the Weil pairing. SIAM J. Computer. 2003;32(3):586-615.
4. Boneh D, Lipton RJ. Algorithms for black-box fields and their application to cryptography (extended abstract). In: Proceedings of the 16th Annual International Cryptology Conference, Advances in Cryptology. Springer; c1996. p. 283-297.
5. Boneh D, Rivest R, Shamir A, Adleman L. Twenty Years of Attacks on the RSA Cryptosystem. Notices of the AMS. 1999;46:203–213.
6. Bleichenbacher D, Bosma W, Lenstra AK. Some remarks on Lucas-based cryptosystems. In: Proceedings of the 15th Annual International Cryptology Conference, Advances in Cryptology. Springer; c1995. p. 386-396.
7. Bernstein DJ, Buchmann J, Dahmen E. Post-Quantum Cryptography. Springer; 2009.
8. Bernstein DJ. Multi-digit multiplication for mathematicians. Available from: http:// cr.yp.to/papers.html.
9. Bailey DV, Paar C. Efficient arithmetic in finite field extensions with application in elliptic curve cryptography. J Cryptology, 2001, 14.
10. Naccache D, M'Rahi D. Cryptographic smart cards. IEEE Micro. 1996;16(3):14-24.
11. Hong D, Sung J, Hong S, *et al*. Hight: A new block cipher suitable for low-resource device. In: Proceedings of the 8th. International Workshop on Cryptographic Hardware and Embedded Systems. Springer; c2006. p. 46-59.
12. Diehard Battery of Tests of Randomness CD; c1995. Available from: http://i.cs.hku.hk/ diehard/.
13. Digital Signature Law Survey. Available from: https://dsls.rechten.uvt.nl/.
14. Denning DER. Cryptography and Data Security. Addison-Wesley Longman Publishing Co., Inc.; c1982.
15. Biham E. A fast new DES implementation in software. In: Fourth International Workshop on Fast Software Encryption, volume 1267 of LNCS. Springer; c1997. p. 260-272.
16. ECC Brainpool. ECC Brainpool Standard Curves and Curve Generation; c2005. Available from: http://www.ecc-brainpool.org/ecc-standard.htm.