Natural Image Encryption and Decryption Method using Proposed Modified Short Range Natural Number (mSRNN)

Harinandan Tunga*, Diptanil Das, Satyaki Siddhanta, Stainlee Bakhla and Debadeep Basu

Department of CSE, RCCIIT, Kolkata – 700015, West Bengal, India; harinandan.tunga@gmail.com

Abstract

Symmetric Key Cryptography is fast and efficient. However key exchange continues to be a hindrance towards its optimal usage. The person who encrypts the message and the person, who decrypts the message in Symmetric Key Cryptography use the same key and hence maintaining the privacy of the common key, without it coming into the knowledge of others, is a tough ask. Asymmetric Key Cryptography is beneficial in eradicating this problem. Here every communicating party uses two keys to form a key pair - one key is made public (and hence called public key) that is used to encrypt the message to be securely sent to the party and the other key is kept private (and hence called private key) that is used to decrypt the encrypted message. The Short Range Natural Number (SRNN) Algorithm is an enhanced asymmetric cryptographic technique that some what has its resemblance to RSA Algorithm. The modifications (mSRNN) done on this algorithm impose better security of the cryptosystem. **General Terms:** Cryptography, Image Encryption and Decryption Algorithm, Modified Short Range Natural Number (mSRNN)

Keywords: Asymmetric Key Cryptography, Modified Short Range Natural Number (mSRNN)

1. Introduction

Data can be anything starting from numbers, texts to images. Data in simpler term can be defined as information. So these data are highly valuable and certainly no one wants these data to fall in wrong hands. For example, a bank account passwords, credit information need to be kept safely and undisclosed from adversaries (third party). However a data during transmission from a client to a server or vice-versa is where it is most vulnerable. This particular point is where most of the data falls to the wrong hands and which might lead to havoc. And that is how this particular problem leads to the concept of cryptography. Cryptography is an idea where the original data is coded into a stream of alpha-numeric array, transmitted and then decoded back to its original form by only those who are intended for can read and process.

*Author for correspondence

This idea leads to two advantages, firstly it definitely avoids the original data to fall in the hands of an adversary and secondly even if the alpha numeric data finds its place in wrong hands, it becomes not much of a use since the coded stream standalone means nothing but rubbish. After the transmission this stream of alpha numeric data should then be decoded back in order to retrieve to its original form. So the function that is used to code and decode the actual data at the two end points remains completely unknown to the third party and therefore an upper hand is obtained in the process.

2. Review of the Literature

As security and integrity of data has become the main concern in past few years due to exponential rise of threats from third party[3]. And in the present scenario almost all the data is transferred via network pathways and so are vulnerable to various threats.[1,2]Has given a brilliant approach to image encryption based on Short Range Natural Algorithm (SRNN). This approach can be used on both color and black and white images (.TIF images only). [5]Has given a performance analysis on[1] and was concluded that the modified SRNN Algorithm is as strong as the original SRNN Algorithm. [6]In this method only an encryption is involved in which the whole image is encrypted with a slight variation in SRNN Algorithm, reduces the computation time marginally.

This paper is based on image encryption and decryption based on user provided image.

3. Algorithm Used

- SRNN Algorithm which is advancement on RSA Algorithm - SRNN Algorithm is a Public key cryptography algorithm. In this algorithm we have extremely large number that has two prime factors. In addition this we have used two short range natural numbers in pair of keys. One key (public key) for encryption and other corresponding key (private key) for decryption. This modification increases the security of the cryptosystem. So its name is short range natural number public key algorithm.
- Modified SRNN Algorithm which is advancement on SRNN Algorithm.

4. Algorithm

p, q, u, a and e are randomly generated.
$n = p * q$
$r = (p - 1) * (q - 1)\ (e * d) \bmod r = 1$
m represents the ASCII value of individual characters of the message that is accepted as a string.
c represents the cipher text that we compute on encrypting the message.

4.1 Method of Encryption

The public key generated is (n , e , u^{a}) $c = (m * u^{a})^{e} \bmod n$.

4.2 Method of Decryption

The private key is (d, a, u) $v = u^{r-a} \bmod n$.
$m = (c * v^{e})^{d} \bmod n$.

4.3 Theoretical Proof of SRNN Algorithm

$e*d \equiv 1–1)(q\text{mod}[(p–1)]$

Let us assume a variable 'h' such that, $e*d - 1$

$$= h*[(p–1)(q–1)]$$

$m^{ed} = m^{ed-1} * m$

$= m^{h*[(p-1)(q-1)]} * m$

Fermat's little theorem states that if 'p' is prime and 'p' does not divide an integer 'a' then $a^{p-1} \equiv 1 \bmod p$.

$$\text{Hence} \left[m^{\substack{(p-1)h(q-1) \\ |}} \right] = 1\,\mathrm{mod}^{\substack{(q-1)h(p-1)] \\ p|}} \quad \text{and} \equiv |$$

1 mod q

i.e, $m^{h*[(p-1)(q-1)} \equiv 1 \bmod pq$

or, $m^{ed-1} \equiv 1 \bmod n[\text{since } pq = n]$

or, $m^{ed} \equiv m \bmod n$....Equation….(1)

Now decrypted message, $m' = (v^e * c)^d \bmod n$

$= [v^{e\,*} (m^* u^a)^e]^d \bmod n$

$= [v\,^* m\,^* u^a]^{ed} \bmod n$

$= (v\,^* u^{a\,*} m) \bmod n$ [using Equation 1]

$= [u^{(p-1)(q-1)-a\,*} u^{a\,*\,m}] \bmod n$

$= [u^{(p-1)(q-1)} \bmod n]\,^* m$

$= 1\,^* m$

$= m$

5. Modification done on SRNN that has Diminished the Execution Time

In the SRNN Algorithm for 1024 bits the time taken was 5080 milliseconds. But our objective was to decrease the time for the whole process. So we have modified the algorithm as follows:

The time complexity of the

$m = (v^e c)^d \bmod n$ has been diminished by modifying the Equation into $(v^e \bmod n * c)^d$

mod n.

Therefore:

- Key generation time – 87 milliseconds.
- Encryption time – 193 milliseconds.
- Decryption time – 660 milliseconds.

Hence the algorithm is theoretically valid.

Modification done on SRNN that has diminished the execution time.

In mSRNN Algorithm public key cryptography is increased security. It provides digital signature that cannot be repudiated. We can select large prime numbers for enhancement of security of keys. Public key cryptography may be used with secret key cryptography.

6. Illustrations and Results of the Cryptosystem

Example 1:

Input: A

Hence m = 65. (m<n)

Generated terms, p = 199

q = 179

e = 7589 (1<e<r) u = 137 (u<r–1)

a = 191 (r>a>u)

Computed terms,

$n = 35621$ $(n = p * q)$

$r = 35244$ $(r = (p - 1) * (q - 1))$ $d = 3497$

$u^a = 137^{191}$ (very long term so manual computation avoided)

Method of Encryption,

$c = (m * u^a)^e \bmod n$ $c = 27699_{10} = 6C33_{16}$

Method of Decryption, $v = u^{r-a} \bmod n$

$m = (c * v^e)^d \bmod n$ $v = 23066$

Example 2:

Input: Abc

Hence m = 65 98 99 (m<n)

Generated terms, p = 167

q = 131

e = 21389 (1<e<r) u = 149 (u<r-1)

a = 223 (r>a>u)

Computed terms,

n = 21877 (n = p * q)

r = 21580 (r = (p – 1) * (q – 1))

d = 14349

$u^a = 149^{223}$ (very long term so manual computation avoided)

Method of Encryption,

$c = (m * u^a)^e \bmod n$

$c = 16273\ 6147\ 1334_{10} = 3F91\ 1803\ 536_{16}$

Method of Decryption, $v = u^{r-a} \bmod n$

$m = (c * v^e)^d \bmod n$ v = 1329

m = 65 98 99 (in ASC

Example 3:

Input: aBc DeF

Hence m = 97 66 99 32 68 101 70 (m<n)

Generated terms, p = 193 q = 199

e = 14999 (1<e<r) u = 227 (u<r–1)

a = 223 (r>a>u)

Computed terms,

n = 38407 (n = p * q)

r = 38016 (r = (p – 1) * (q – 1))

d = 8615

$u^a = 227^{223}$ (very long term so manual computation avoided)

Method of Encryption,

$\equiv \quad A\ c = (m * u^a)^e \bmod n$

$c = 15870\ 12162\ 34192\ 33521\ 24832\ 27754\ 23538_{10}$

$= 3DFE\ 2F82\ 8590\ 82F1\ 6100\ 6C6A\ 5BF2_{16}$

Method of Decryption, $v = u^{r-a} \bmod n$

$m = (c * v^e)^d \bmod n$ v = 17751

m = 97 66 99 32 68 1 aBc DeF

Example 4:

Natural Image that had been encrypted and decrypted with modified SRNN Algorithm. Illustration of the Cryptosystem on a Matrix resembling pixel values.

$$\begin{tikzcd}
\begin{pmatrix} 97 & 66 \\ 99 & 32 \end{pmatrix} \arrow[r] & \begin{pmatrix} 15870 & 12162 \\ 34192 & 33521 \end{pmatrix}_{10} \arrow[d] \\
\begin{pmatrix} 97 & 66 \\ 99 & 32 \end{pmatrix} & \begin{pmatrix} 3DFE & 2F82 \\ 8590 & 82F1 \end{pmatrix}_{16} \arrow[l]
\end{tikzcd}$$

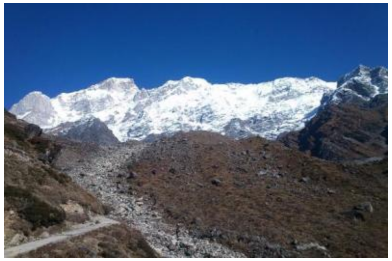

Figure 1. Original image.

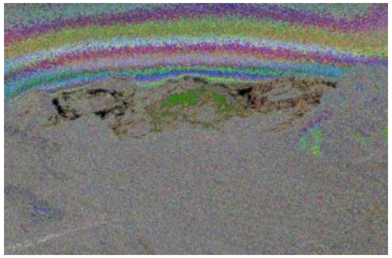

Figure 2. Cipher image.

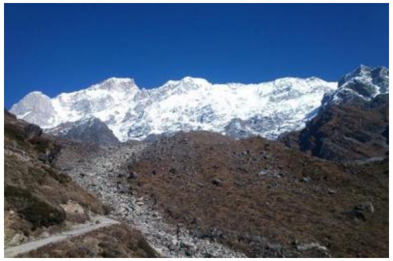

Figure 3. Decipher image.

7. Conclusion

Hence it can be concluded that overall performance of SRNN Algorithm is better in security but slower in speed. Difference of SRNN and RSA with modulus length 1024 bits are approximately 5080 milliseconds (SRNN 1024 bits > RSA 1024 bits) whereas difference of RSA 2048 bits and SRNN 1024 bits are 5338 milliseconds (RSA 2048 bits > SRNN 1024 bits). We have tried to diminish the time taken by our modified algorithm which is approximately 900-1100 milliseconds. Hence modified SRNN with modulus length 1024 bits is a good balance between speed and security. This modification increases the security of the cryptosystem as compared to RSA and enhances speed with respect to SRNN.

8. References

1. Losetti M. Kan Enhanced RSA Algorithm for Low Computational Device. Journal of Advanced Research and Innovations. 1(2):114–8.
2. Singh K, Verma R, Chehal R. Modified Prime Number Factorization Algorithm (MPFA) for RSA Public Key Encryption IJSCE. 2012 Sep; 2(4):204–6. ISSN: 2231-2307.
3. Sharma S, Yadav JS, Sharma P. Modified RSA public key cryptosystem using short range natural number algorithm. Int Journal of Advanced Research in Computer Science and Software Engineering. 2012 Aug; 2(8):134–8.
4. Wiener MJ. Cryptanalysis of short RSA secret exponents. IEEE Transactions on Information Theory. 1990 May; 36(3):553–8.
5. Gennaro R. Based Undeniable RS Signatures. Journal. 2000; 4:397–416.
6. Cramer R, Shoup V. Signature schemes based on the strong RSA assumption. ACM Tr on Information and System. 2000 Aug; 3(3):161–85.