International Journal of Engineering Research and Advanced Technology (IJERAT)

DOI: 10.31695/IJERAT.2019.3582

E-ISSN : 2454-6135

Volume.5, Issue 11
November -2019

Subject Review: Comparison between RSA, ECC & NTRU Algorithms

Ahmed Othman Khalaf [1], Shaimaa Khudhair Salah[2], Hind Jumaa Sartep[3], and Zainab Khyioon Abdalrdha[4]

[1,2,4] Teacher, [3]Assistant Teacher
[1-4] Department of Computer Science, Collage of Education
University of Mustansiriyah, Iraq

ABSTRACT

Encryption technology is one of the main means of protecting information security and includes many forms in terms of digital signatures, authentication, system security, confidentiality and data integrity and other functions. Therefore, Encryption and decryption are the best solution to protect data, especially not only sensitive data and protect them from attackers who aim to steal information. In this paper we use asymmetric encryption algorithms such as (RSA, Elliptic Curve, NTRU) that are used to send data over the network to provide security to users. We work on a review of the algorithms mentioned because of their importance in the encryption side and will give a summary of the performance of its work.

Key Words: *Cryptography, Encryption techniques, RSA, Elliptic curve cryptography, NTRU.*

1. INTRODUCTION

Information security plays a very important role when Internet connectivity is provided. There are many encryption methods that provide security. To achieve this level of security, different security protocols of the symmetric key type and asymmetric encryption type are all about increasing the level of privacy of individuals and groups individuals [1].

The purpose of encryption is to provide a secure environment for communication and to keep information safe from unauthorized access. In encryption terminology, an unencrypted message is called explicit text and encrypted message contents whose contents cannot be detected by unauthorized persons are called encryption. The encrypted text recovery process is called decryption. There are four basic principles for the purpose of encryption [2]. Confidentiality, Data integrity, Authentication & Non-repudiation.

2. TYPES OF ENCRYPTION TECHNIQUES

Encryption techniques to be implemented in networks ensure all encryption requirements, as There are two types of encryption that we'll explain in the next section.

2.1 Symmetric Encryption Techniques:

This type of encryption involves using the same key for the encryption and retrieval of a message or data and is the oldest known encryption method. Because the same key is used for encryption, one of the disadvantages of encryption is when compared to public key encryption, This type of encryption can use encryption (stream or block). Several algorithms are dependent on this type of encryption including AES, RC5, DES, 3DES and IDEA [3].

2.2 Asymmetric Encryption techniques:

Public key encryption, or so-called asymmetric, uses two keys, one public and the other private. The public key is used in the message encryption process and is declared to the parties while the decryption key is kept secret, the private key[3]. Davy and Hillman in 1978 were the first two people to spread the idea of asymmetric encryption algorithms. There are many algorithms of this class are RSA, ECC, NTRU etc [4] . We will introduce three algorithms within asymmetric encryption techniques (RSA, ECC &NTRU) algorithm :

2.2.1. RSA Algorithm :

The RSA algorithm is an asymmetric encryption algorithm that involves three steps [5].

a. Generation of Key:

RSA algorithm uses two keys (public and private) where public key for encryption and private for decryption, RSA algorithm keys are created in the following way [6].

1. Randomly choose two prime numbers that are of a similar length for safety and the numbers are (f and l).

2. Calculate m = f l. For public and private keys, m is a modulus.

3. Calculate φ (m) = (f - 1) (l - 1), where φ is the totter function in Euler.
4. Randomly select the encryption key e with 1 <e < φ (m) and gcd (e, φ (m)) = 1.
5. The encryption key can be found using d as d ≡ e - 1 (mod φ (m)); that is, d is given d·e ≡ 1 (mod φ (m)).

- Public Key Encryption: PU = {e, m} which is publicly available.
- Secret decryption key: PR = {d, m} which is kept secret.

b. Encryption Operation[5]:

Encrypts the message (N).
-The recipient's public key is PU = {e, m}.
- Calculate the coding according to the equation: C = Ne mod m, where 0 N ≤ m

c. Decryption Operation[5]:

We use to decrypt the private key for C:
- PR = {d, m} private key
- Calculate decoding according to the equation: N = Cd mod.

2.2.2 ECC Algorithm :

The elliptic curve algorithm is another type of asymmetric cryptographic algorithm that uses a pair of keys, one private and one generic to execute the encryption and decryption process. $4c^3 + 27d^2 \bmod p \neq 0$, we use the equation whose coefficient c and d generate different elliptic curve points for (x, y) and p is a large prime number [7].

a. Elliptic curve operations[7]:

1. We take a prime number p and values for factors a and b to be applied according to equation $4c^3 + 27d^2 \bmod p \neq 0$.
2. Calculate y2 mod p, Where all y values take between 0 and p-1, note that 4c3 + 27d2 mod p ≠ 0 .
3. Calculate (x3 + cx + d) mod p . Where all x values take between 0 and p-1 .
4. Add the y values from step 2 which corresponds to the values calculated in step.
5. We add all values to the point (x,y) from step 4. 6. Suppose the base point is the value of G which belongs to step5 points.
7. The values of iG are calculated from the (G +G) , the result is 2G, then the(2G+ G) , produces 3G and so on points.
8. Calculate the sender's public key (for example, A):
Choose a large integer nA, that will be 1 and n. Calculate PA = nAG
9. Calculate the recipient's public key (for example, B):
Choose a large integer nB, Will be 1 and n. Calculate PB = nBG
10. Encryption operation
Sender A will use public key B to encrypt the message.
- let's assume that the plain text Pm which is similar to a point specified in the calculation in step 5.
Let L is a random integer that is between 1 and n. Calculation - (LG, Pm + LPB)
11. Decryption operation
We calculate LGnB, then we calculate Pm L PB- LGnB to get Pm.
In the figure 1. the points (x, y) of the curve are shown according to the irreducible polynomial equation that (x3 + cx + d) mod p.
.

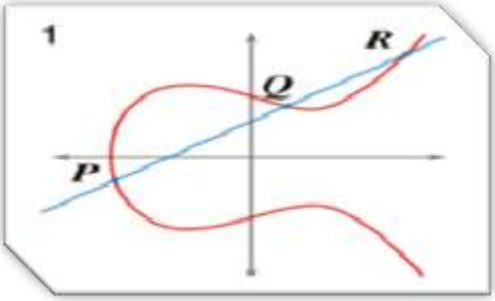

Figure. 2. Elliptic Curve [8]

This ECC algorithm performs an alphanumeric sequence of data and uses an ASCII value to encode and decode a particular character.

DOI : 10.31695/IJERAT.2019.3582

2.2.3. NTRU Algorithm

NTRU is cryptography system that does not rely on operators or separate logarithmic problems. NTRU - N-polynomial ring units (R = Z [X] / (X $^{N-1}$) [9] .

- **Operations of NTRU Algorithm[10] :**

Its base objects on the polynomial ring are truncated R=Z[X]/(X^{N-1}) , and the polynomial is $N\text{-}1: a^0 + a^1x + a^2x^2 + \cdots + a^{N-1}x^{(N-1)}$, NTRU includes three steps: generation of key, encryption for NTRU, and c. decryption for NTRU.

a. Generation of Key:

Step1. Randomly, user B selects (2) polynomials l and f in R (polynomial).
- Polynomial values must be kept secret.
- There must be a polynomial chosen inverse.
Step2. An inverse will be calculated for both l modulo p and l modulo q: l * l-1 q = 1 (modulo q) and l * lp-1 = 1 (modulo p).
Step3. The polynomial product will be calculated: n = p * ((l^{-1} q) * l) mod q , Private key B will be: (l and lp) and public key B: polynomial n.

b. Encryption for NTRU :

The sender A wishes to send a message will follow the following:
Step1. Sets the message in a polynomial form whose coefficients are selected coefficient That will be -p / 2 and p / 2 (central lift).
Step2. Randomly selects another polynomial is small p (to hide the message).
Step3. Message encoding: e = r * n + m (modulo q).

c. Decryption for NTRU Algorithm:

B receives the message e from A for decryption.
Step1. Using its polynomial counterpart l calculates the polynomial a = l * e (mod q). B needs to choose coefficients of length q which are considered as longitudinal separation for decoding.
Step2. Polynomial is calculated as b = a (mod p). B reduces both coefficient coefficients p.
Step3 . B uses lp which is polynomial to compute the other c = l-1 p * b (modulo p), which represents the original message of A.

- **Benefits of NTRU**

  - The algorithm is more effective in coding and decrypting applications in both hardware and software.
  - The process of creating a key is much faster than allowing the use of keys (because the account can be created because of key licenses).
  - Used in mobile devices and smart card for the advantage of low memory usage.

3. PERFORMANCE COMPARISON OF RSA , ECC AND NTRU ALGORITHM

The basic concepts indicate that asymmetric encryption algorithms of NTRU, ECC, RSA and the like that produce keys based on mathematical calculations are skilled, In order to better understand the performance of these algorithms a detailed discussion of these encrypted systems must be conducted. The purpose of this part is to provide a comparative analysis of encryption performance used in the NTRU, RSA, and ECC algorithms, including key size, encryption generation, and decoding timing. In Table 1, we will show a comparison between the three algorithms NTRU, RSA and ECC. Table 1: Performance comparison between RSA, ECC and NTRU algorithms.

Table 1. Comparison between RSA and ECC &NTRU Algorithm .

Method of Algorithm	RSA	ECC	NTRU
The way	Public	Public	Public
Encryption Method	Slow	LESS FAST	Very fast
Decryption Method	Slow	FAST	Very fast
Distribution of Key	Easy	less easy	Easy
Complexity	O(N^3)	O(N^4) or O(LogN)	O(NLogN)
Security algorithm	High	high security	Very High

DOI : 10.31695/IJERAT.2019.3582

Mathematical Problem	Integer factorization	Separate logarithm elliptic curve	The problem of short vectors (engineering problems)
Describe	Give a the number n, and find the main factors	When giving an elliptic curve E, which has two points P and Q over E, look for x so that Q = x.P	The hardness of the lattice problems are outdone,
Execution times	Exponential sub	Exponential for ECC	Exponential for NTRU

4. List of Abbreviations

In this section we will show the abbreviations of the algorithms used in this paper according to Table 2: List of Abbreviations.

ABBREVIATION	THE DESCRIPTION
RSA	**R**ivest-**S**hamir-**A**dleman
NTRU	**N**-th **t**runcated **r**ing polynomial
AES	**A**dvanced **E**ncryption **S**tandard
RC5	**R**ivest **C**ipher **5**
DES	**D**ata **E**ncryption **S**tandard
3DES	Triple **D**ata **E**ncryption **A**lgorithm
IDEA	**I**nternational **D**ata **E**ncryption **A**lgorithm
ECC	**E**lliptic **C**urve **C**ryptography

5. CONCLUSION

In this paper, we looked at a review of the achievement of asymmetric encryption algorithms (NTRU, RSA and ECC). By focusing on the performance of Asymmetric encryption systems including NTRU and other such as RSA and ECC by comparison, it can be concluded that one in three ECC has the best method in terms of key size and in terms of security level, RSA has small keys compared to NTRU, the greater the size of the RSA key the higher the security level and when it comes time to analyze the actual performance, we get the same security levels, NTRU has a good performance which is better than ECC and RSA and through review, we identified NTRU and how it works against RSA and ECC. There has been much focus and analysis on security and performance issues. Eventually, NTRU will serve as a backup for future use because NTRU is an alternative and productive algorithm for the future of public key cryptography, and the nature of the problem in the NTRU algorithm on which the algorithm is based is quite different from the current public key cryptographic systems (number theoretical problems). NTRU is a relatively good coding system, but we cannot replace both the ECC or RSA algorithms with NTRU so easily.

ACKNOWLEDGMENT

The authors would like to thank AL_Mustansiriyah University (www.uomusiriyah.edu.iq), Baghdad-Iraq for its support in the present work.

REFERENCES

[1] M. Mani Roja, Ravdeep Johar, Ankit Chadha, Sushmit Mallik and Aman Chadha, “ Dual-Layer Video Encryption using RSA Algorithm” , International Journal of Computer Applications (0975 – 8887) Volume 116 – No. 1, 2015 .

[2] Neha Garg and Partibha Yadavm , “Comparison of Asymmetric Algorithms in Cryptography”, IJCSMC, Vol. 3, Issue. 4, April 2014, pg.1190 – 1196.

[3] Swapna B Sasi1, Dila Dixon2, Jesmy Wilson2 , “A General Comparison of Symmetric and Asymmetric Cryptosystems for WSNs and an Overview of Location Based Encryption Technique for Improving Security”, IOSR Journal of Engineering (IOSRJEN) www.iosrjen.orgISSN (e): 2250-3021, ISSN (p): 2278- 8719, Vol. 04, Issue 03 (March. 2014), ||V3|| PP 01-04

[4]Manish Singh, Shailender Gupta and Bharat Bhushan, YMCA University of Science and Technology, Faridabad, 2012, “Comparison of symmetric and asymmetric key cryptography: A study”, Proceeding of the National Conference “Science in Media 2012” Organized by YMCA University of Science and Technology, Faridabad, Haryana (India).

[5] Rasha Samir Abdeldaym, Hatem Mohamed Abd Elkader, Reda Hussein ,"Modified RSA Algorithm Using Two Public Key and Chinese Remainder Theorem", I.J. of Electronics and Information Engineering, Vol.10, No.1, PP.51-64, Mar. 2019 (DOI: 10.6636/IJEIE.201903 10(1).06)

[6] Merlyne Sandra Christina 1 , Karthika 2, Vasanthi3, Vinotha4 (2016) :Video Encryption and Decryption using RSA Algorithm" International Journal of Engineering Trends and Technology (IJETT) – Volume 33 Number 7- March.

[7] Gupta Shubhi, Department of Computer Science and Engineering, Amity university, Greater Noida, "Implementation of ECC using socket programming in Java", International Organization of Scientific Research (IOSR), , Volume 16, Issue 4, Ver. I (Jul-Aug. 2014), PP 87-89

[8]Shubhi Gupta, Divya Singh ,Swati Vashisht &Pradeep kushwaha , "Enhancing Big Data Security using Elliptic Curve Cryptography", 2019 International Conference on Automation, Computational and Technology Management (ICACTM) Amity University.

[9] Hien Ba Nguyen, "AN OVERVIEW OF THE NTRU CRYPTOGRAPHIC SYSTEM ",A Thesis, In Partial Fulfillment of the Requirements for the Degree Master of Arts in Mathematics, Fall 2014.

[10] Qingxuan Wang, Chi Cheng, and Ling Zuo, " Analysis and Improvement of a NTRU-Based Handover Authentication Scheme, IEEE , 2019 .

DOI : 10.31695/IJERAT.2019.3582