RESEARCH ARTICLE OPEN ACCESS

A Comparative Study of RSA and ECC

Dr. K.L. Vasundhara [*], Y. V. S. Sai Pragathi[**], Y. Sai Krishna Vaideek[***]
**(Associate Professor of Mathematics, Stanley College of Engineering & Technology for Women*
*** (Associate Professor of CSE Department, Stanley College of Engineering & Technology for Women,*
Corresponding Author : Dr. K.L.Vasundhara

ABSTRACT
Network is a collection of interconnected nodes which are spread over a large region. A node can be any device such as personal computer, mobile phone, tablet, WAP devices, pager, etc. Data is transmitted over channel of this network, which is prone to security threats such as loss of confidentiality, loss of integrity, fabrication attacks, etc. So, there is a need to secure this data transmission. It is achieved through Cryptography [9].The present work focuses on cryptography to secure the data while transmitting in the network. Firstly, the data which is to be transmitted from sender to receiver in the network must be encrypted using the encryption algorithm in cryptography. Secondly, by using decryption technique the receiver can view the original data. Many research papers have been submitted on this cryptographic algorithm.This paper aims at study of the two asymmetric-key algorithms i.e. Rivest-Shamir-Adlemann (RSA) and Elliptic-Curve cryptography (ECC).A comparative analysis of both the algorithms has been done and observed that RSA is one of the effective public key cryptographic algorithms, which needs time and memory whereas ECC provides a strong alternative with smaller key lengths and more secure [1][2].

Keywords: Cryptography, encryption, asymmetric key encryption

---

Date of Submission: 23-12-2017 Date of acceptance: 08-01-2018

I. INTRODUCTION

Cryptography, a word with Greek origins, means "secret writing" is the science of devising methods that allow for information to be sent in a secure form in such a way that the only person able to retrieve this information is the intended recipient. The message to be sent through an unreliable medium is known as plaintext, which is encrypted before sending over the medium. The encrypted message is known as cipher text, which is received at the other end of the medium and decrypted to get back the original plaintext message. Hence a cryptosystem is a collection of algorithms and associated procedures for hiding and revealing information [3].

II. CRYPTOGRAPHIC ALGORITHMS

Cryptographic algorithms have evolved over time to answer various needs. Cryptography algorithms can be divided into two broad categorizes -Symmetric key cryptography and asymmetric key cryptography. In this paper, a study of two well known asymmetric key cryptographic algorithms is done [5][7].

In asymmetric key cryptography, different keys are used for encryption and decryption; hence it is called as public key encryption. The two keys are a private key and a public key. The public key is announced to the public; whereas the private key is kept by the receiver. The sender uses the public key of the receiver for encryption and the receiver uses his private key for decryption. Here the number of keys required is small, but it is not efficient for long messages. In asymmetric key encryption Rivest-Shamir-Adlemann (RSA) and Elliptic-Curve cryptographic (ECC) algorithms, different factors are studied [7] [4].

III.RIVEST-SHAMIR-ADLEMANN (RSA)

RSA is based on the use of two large prime numbers according to the mathematical fact that it is easy to find to large prime numbers but difficult to factorize their product.RSA generates two keys: Public key for encryption and Private key for decryption. The public key consists of public-key modulus and public-key exponent. The private-key consists of private-key modulus and private-key exponent.

Algorithm:

1. Take two prime numbers, p and q.
2. Calculate, n = p*q. n is called the modulus of both public and private keys.
3. Calculate, $\varphi(n) = (p - 1)(q - 1) = n - (p + q - 1)$, where φ is Euler's totient function and its value is kept secret.
4. Choose an integer e, $1 < e < \varphi(n)$ and $\gcd(e, \varphi(n)) = 1$.e and $\varphi(n)$ are co-prime.
e is called the public key exponent.
5. Calculate, $d \equiv e^{-1} \pmod{\varphi(n)}$.
d is called the private key exponent.

EXAMPLE

To demonstrate the RSA public key encryption algorithm, let's start it with 2 smaller prime numbers 5 and 7.
Generation the public key and private key with prime numbers of 5 and 7 can be illustrated as:

- Given p as 5
- Given q as 7
- Compute n = p*q: n = 5*7 = 35
- Compute m = (p-1)*(q-1): m = 4*6 = 24
- Select e, such that e and m are coprime numbers: e = 5
- Compute d, such that d*e mod m = 1: d = 29
- The public key {n,e} is = {35,5}
- The private key {n,d} is = {35,29}

With the public key of {35,5}, encryption of a cleartext M represented as number 23 can be illustrated as:

- Given public key {n,e} as {35,5}
- Given clear text M represented in number as 23
- Divide B into blocks: 1 block is enough
- Compute encrypted block C = M^e mod n:

C = 23^5 mod 35 = 6436343 mod 35 = 18

The ciphertext C represented in number is 18 With the private key of {35, 29}, decryption of the cipher text C represented as number 18 can be illustrated as:
Given private key {n,e} as {35,29} Given ciphertext C represented in number as 18 Divide C into blocks: 1 block is enough Compute encrypted block M = C^d mod n:
M = 18^29 mod 35
= 18*18^28 mod 35
= 18*(18^4)^7 mod 35
= 18*(104976)^7 mode 35
= 18*(104976 mod 35) ^7 mod 35
= 18*(11)^7 mod 35
= 18*19487171 mod 35
= 350769078 mod 35
= 23
The clear text M represented in number is 23

IV.ELLIPTIC-CURVE CRYPTOGRAPHY (ECC)

The primary advantage of using Elliptic Curve based cryptography is reduced key size and hence speeds. Elliptic curve based algorithms use significantly smaller key sizes than the non-elliptic curve equivalents. The difference in equivalent key sizes increases dramatically as the key sizes increase. ECC is a public key cryptography(PKC) which has public and private keys for authentication. It is based on elliptic curves over finite fields.
A field is a set of elements with operations defined for the elements of that set that equate to operations like addition, subtraction, multiplication and division. The elements could be numbers, or they could be something else entirely. The following conditions should meet in order to be a field:

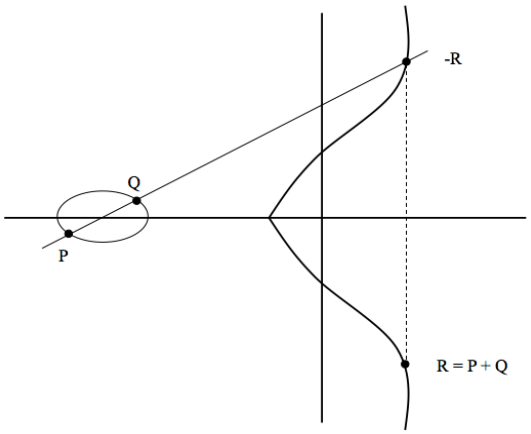
- Both addition and multiplication are closed over the set, so for example if a and b are in the set then so are a + b and a * b
- Addition and multiplication must be associative: so a + (b + c) = (a + b) + c and similarly for multiplication
- Addition and multiplication must be commutative: so a + b = b + a and similarly for multiplication
- Both addition and multiplication must have identity elements. So, for example 0 and 1 where: a + 0 = a, and a * 1 = a
- There must be additive and multiplicative inverses for all elements in the set. So, for example, for every element a in the set there is -a so that a + (-a) = 0 (where 0 is the identity element for addition). Similarly, for multiplication.
- Multiplication distributes over addition: if a, b and c are in the set then a * (b + c) = (a * b) + (a * c)

A finite field is simply a field where the set has a finite number of elements. So, for example, the set of all integers could not be used as the basis for a finite field because there are an infinite number of them. However, the set of integers from 0 to 100 could form the basis of a finite field [6].
So now we can define an Elliptic Curve. In general, an Elliptic Curve is one of the form:
$y^2 = x^3 + ax + b$, where x, y, a and b are elements of some Field.

In Elliptic Curve Cryptography, we restrict such that x, y, a and b are elements of a finite field.
We can define a group over elliptic curves specifically as:

- the elements of the group are the points of an elliptic curve;
- the identity element is the point at infinity 0;
- the inverse of a point PP is the one symmetric about the x-axis;
- addition is given by the following rule: given three aligned, non-zero points P, Q and R, their sum is P+Q+R=0.

We can write P+Q+R=0as P+Q=−R. This equation, in this form, lets derive a geometric method to compute the sum between two points P and Q: **if we draw a line passing through** P **and** Q**, this line will intersect a third point on the curve,** R (this is implied by the fact that P, Q and R are aligned). **If we take the inverse of this point,** −R, **we have found the result of** P+Q.



Elliptic curve addition

In principle, there are many different types of field that could be used for the values x and y of a point (x, y). In practice, however there are two primary ones used. The simplest is typically referred to as the prime field Fp where p is a prime number. In cryptographic applications p must be a very large prime number. The elements of the set are simply the numbers 0 through to p-1, and addition and multiplication over the field have the normal meaning for modular (or clock) arithmetic. So, if p=7 then the elements of the set are {0, 1, 2, 3, 4, 5, 6} and

$0 + 1 = 1$
$2 + 3 = 5$
$3 + 3 = 6$
$4 + 3 = 0$
$5 + 4 = 2$and so on.

The next common type of field is referred to as the binary field F2m. Elements of a binary field is typically represented as polynomials and not as numbers. So, for example an element could be:

$$x^4+x^2+1$$

This can then be expressed as a binary number ({1 0 1 0 1} in this case), where each term represents one bit in the binary representation. Addition of such polynomials is done as normal but with the result of each term reduced modulo 2. So, for example:

$$(x^2 + 1) + (x^2 + x) = 2x^2 + x + 1$$

Each term is then reduced modulo 2 to give an answer 0

$$x^2 + x + 1 = x + 1$$

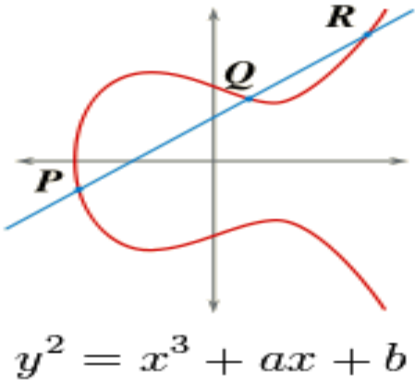
In binary representation, this sum could be expressed as follows:

$$\{1\ 0\ 1\} + \{1\ 1\ 0\} = \{0\ 1\ 1\}$$

Note then that addition is just a simple XOR operation.

Multiplication in the binary field is done respective to an irreducible polynomial. Multiplication of polynomials is done in the normal way and the result is then divided by the irreducible polynomial. The remainder is the result of the multiplication.

E -> Elliptic Curve
P -> Point on the curve
n -> Maximum limit (This should be a prime number)



$$y^2 = x^3 + ax + b$$

The figureshows a simple elliptic curve [9]. Key Generation

Key generation is an important part where we have to generate both public key and private key. The sender will be encrypting the message with receiver's public key and the receiver will decrypt its private key.

Now, we have to select a number **'d'** within the range of **'n'**. Using the following equation, we can generate the public key $Q = d * P$

Where, d = The random number that we have selected within the range of (**1 to n-1**). **P**is the point on the curve.

'Q' is the public key and **'d' is the private key.**

Encryption

Let 'm' be the message that we are sending. We have to represent this message on the curve. Consider *'m'* has the point *'M'* on the curve *'E'*. Randomly select 'k' from [1 – (n-1)].

Two cipher texts will be generated let it be **C1** and **C2**.

$C1 = k*P$
$C2 = M + k*Q$

C1 and C2 will be send.

Decryption

We have to get back the message 'm' that was send to us,

$M = C2 – d * C1$

M is the original message that we have send.

Proof

To get back the message, $M = C2 – d * C1$

'M' can be represented as 'C2 – d * C1'

$C2 – d * C1 = (M + k * Q) – d * (k * P)$
(C2 = M + k * Q and C1 = k * P)
$= M + k * d * P – d * k * P$
(Canceling out k * d * P)
= M (Original Message)

V. CONCLUSION

RSA and ECC are known as the most efficient PKC among all asymmetric encryption algorithms. They boast alarge number of merits in comparison with other cryptosystems. ECC is a very encouraging and new field to work in order to find a more cost-efficient method to perform encryption for portable devices and to secure image transmission over internet. Elliptic curves are believed to provide good security with smaller key sizes, something that is very useful in many applications. Smaller key sizes may result in faster execution timings for the schemes, which is beneficial to systems where real-time performance is a critical factor. We have estimates of parameter sizes providing equivalent levels of security for RSA and ECC systems [8]. These comparisons illustrate the appeal of elliptic curve cryptography especially for applications that have high security. The application of ECC is highly recommended to create more security and higher speed without increasing the computational load. On the other hand, with the increase of smaller embedded devices design with extra limitations (i.e. Computation Power, Memory and Battery life) and cryptographic schemes especially in resource constrained devices, need to be not only secure but also practical and cheaper. ECC has smaller cost ration. Furthermore, to maximize the performance of the newly designed devices, ECC itself needs consistent enhancement.

REFERENCES

[1]. Kumari Archana, VibhutiSikri, "Comparative analysis of RSA and ECC", International journal of innovative research in computer and communication engineering, Vol.3 Issue 7, July 2015.

[2]. Rounak Sinha, Hemant Kumar Srivastava, Sumita Gupta," Performance based comparison study of RSA and Elliptic curve cryptography", International journal of scientific & engineering research, Vol. 4, Issue 5, May 2013.

[3]. Nivedita Bisht, Sapna Singh," A Comparative study of some symmetric and asymmetric key cryptography algorithms", International journal of innovative research in science, engineering and technology", Vol. 4, Issue 3, March 2015.

[4]. VivekB.Kute ,P.R.Paradhi, G.R.Bamnote," A software comparison of RSA and ECC", International journal of computer science and applications, Vol. 2, No.1,April/May 2009.

[5]. William Stallings, cryptography and network security (4/e, Pearson Education).

[6]. Koblitz, N. (1987), elliptic curve cryptosystems, Mathematics of Computation, Vol. 48.

[7]. Menzer, Alfred et al, handbook of applied cryptography (2/e, crc press 1996).

[8]. Lenka and Jozef, practical cryptography-the key size problem: pgp after years 21 dec 2001.

[9]. https://www.certicom.com/?action=ecc.

International Journal of Engineering Research and Applications (IJERA) is **UGC approved** Journal with Sl. No. 4525, Journal no. 47088. Indexed in Cross Ref, Index Copernicus (ICV 80.82), NASA, Ads, Researcher Id Thomson Reuters, DOAJ.

Dr. K.L. Vasundhara . "A Comparative Study of RSA and ECC ." International Journal of Engineering Research and Applications (IJERA), vol. 8, no. 1, 2018, pp. 49-52.