تطبيق تشفير RSA العام والمنحنيات الإهليلجية في تشفير المفتاح

هدى محمد خلاط [1] ، نعيمة الفيتوري علي [2]
قسم الرياضيات، كلية العلوم، جامعة صبراته
قسم الرياضيات، كلية العلوم، جامعة الجبل الغربي

مستخلص:

في السنوات الأخيرة ، وجدت الدراسات المعاصرة حول التشفير أن تشفير RSA هو أسلوب للأمان يتم استخدامه في تطبيقات مختلفة مثل التحويلات المالية للاتصالات العسكرية و في أي منطقة كمبيوتر نحتاج فيها إلى الأمان ، علاوة على ذلك فإن البيانات المستخدمة في الاتصال حساسة للغاية وتحتاج إلى حماية .

تتضمن هذه الورقة نظرية الأعداد المتعلقة ب RSA التي تقدم بعض النظريات ولديها إثبات ل RSA وخوارزمياتها مع إنشاء المفتاح العام وتعتمد قوة الأمان على حجم المفتاح الكبير.

بالإضافة إلى ذلك ، يعتمد تشفير المفتاح العام على صعوبة حل مشكلة رياضية معينة مثل خوارزمية RSA وهي آمنة على افتراض أنه من الصعب تحليل عدد صحيح كبير يتكون من عاملين أوليين أو أكثر .

علاوة على ذلك في هذا البحث يتم تضمين تشفير جديد يعتمد على منحنى إهليجي مع مقارنة قصيرة بين طريقة RSA وتشفير المنحنيات الإهليلجية وأمثلة مفيدة مختلفة ذات صلة.

الكلمات المفتاحية: طريقة تشفير RSA , خوارزمية منفصلة ، تشفير المنحنى الإهليجي ، حقول محدودة.

Application of RSA cryptography and Elliptical Curves in Public key cryptography

***Huda M. Khalat*[1] , *Naema Fituri Ali*[2]**

1. Dept of. mathematics, Faculty of Science , Sabratha University

2. Dept of. mathematics, Faculty of Science , AL-Jabal AL-Gharbi University

Abstract:

In recent years, contemporary studies on cryptography have found that RSA cryptography is an essential technique for security that is used in different applications such as military, communication, financial transfers any computer area where we need security. Furthermore, it is the data used in communication, that is very sensitive and it needs to be protected.

This paper involves the number theory related to RSA providing some theorems and has a proven of RSA and its algorithms with key generation; the strength of security depends on large key size. Whereas the ECC has displayed same level of security with relatively small key sizes. In addition, public key cryptography is based on the intractability of certain mathematical problem, such as the RSA algorithm, are secure assuming that it is difficult to factor large integer composed of two or large prime factors.

Furthermore, a new cryptography based on an Elliptic Curve is involved in this paper, with a short comparison between ECC and RSA, and different related useful examples.

Keywords: RSA cryptography, Discrete Algorithm, Elliptic Curve Cryptography, finite field.

1- Introduction:

Nowadays, information is considered as one of the most important commodities of humanity; whilst protecting it is one of the most fascinating challenges of these times. Cryptography is the main tool that has helped meet that challenge; it is best defined as,

the science that studies methods and procedures to modify data, in order to achieve the security features.

The concept of public key cryptography has a vast history starting with the scheme introduced by Deffie and Hellman [21] in 1976.

Various mathematical algorithms are used to try to cover one or more of these basic safety features. The level of compliance with objectives is difficult to evaluate, since several algorithms can be vulnerable to various attack techniques. Current cryptography started in the second half of the 19-70s, with the invention of a system known as DES (Data Encryption Standard) in 1976 that became known widely, especially in the industrial and commercial world. Later the RSA (Rivest, Shamir and Adleman) in 1978, marked the beginning of cryptography in a wide range of applications: military transmissions, financial transactions, satellite communication, computer networks, telephone lines, television broadcasts and so on. Cryptography is divided into two main branches, private key cryptography or symmetric cryptography, where encryption and decryption use the same key, such as data encryption standard and advanced encryption standard. Instead of using the same key to encrypt and decrypt data, the RSA system uses a combined pair of keys. Each key gives a one-way transformation in the data. Therefore, each key is the inverse of the other: what one does, only the other can undo.

The Public Key, RSA is published by the owner, while the private key is kept secret. To send a private message, the sender encrypts it with the desired recipient's public key. Once that has been encrypted, the message can only be decrypted using the recipient’s private key. Conversely, the user can encrypt data using a private key. In other words, the keys of the RSA system can be used in any direction. This provides the foundation for digital signatures: if a user can decrypt a message with someone else’s public key, the other user must necessarily have used their Private Key to encrypt it originally.

From the moment that only the owner can use its private key, the encrypted message becomes a kind of digital signature and is a document that no one else can produce [1], [3] and [4].The aims of this paper are to study RSA cryptography, its goal is to save data secured that's related to the RSA theory. Consequently, early public key systems, such as the RSA algorithm, are secured supposing that it is hard to investigate a large integer composed of two large prime factors or more. Moreover, the researchers have attached the RSA algorithm with comprehensible examples.

In this paper, we have discussed another complex, algebraic object which is known as an "Elliptic Curve". Elliptic Curve Cryptography (ECC) is a mathematical technique that has been used form more than 25 years. It was explained in 1985 by Neal Koblitz and Victor Miller. Based on using a group of points on an Elliptic Curve (EC) public key cryptography, the ECC was born[15].

In addition, this research investigates Elliptic curve in terms of applications as a new variation on the RSA scheme, which is based on algebraic geometry and shows how it uses in secure cryptography. Finally, in section 12 we explain Elliptic Curves to illustrate point addition and doubling and ECC which is also considered over field Z_2^m and Z_p in the affine coordinate and projective coordinate, wherein the main point in this section is that ECC is related to RSA cryptography regarding encrypting and decrypting messages. Additionally, a few simple examples are provided.

2-The GCD and LCM Algorithm

Both the Greatest Common Divisor (denominator) *gcd*, which is also named as the Highest Common Factor *hcf* and the Least Common Multiple *lcm* are necessary concepts behind understanding RSA where the *gcd* of two or more integers, *b* and *c* which is denoted by *gcd(b,c)* is defined as the biggest number *a* that satisfies *a\b* and a\c.

For example, *gcd(6,15)=3* since$6 = 2 * 3$ and $15 = 3 * 5$, where each factorization, has one 3 common as a result hcf(6,15)=3, thus3/6 and 3/15 .

Furthermore, the focus point is that when the *gcd* is equal to one *(b,c)*=1 then *b* and *c* are called Co-prime or Relatively Prime. This is used in RSA cryptography technique [7], [13].

For instance *hcf(13,24)=1* since 13=13 and 24=$2 * 2 * 2 * 3$, have no visible common prime factor , also *gcd(5,6)*=1 since 5=5 and 6=$2 * 3$.

On the other hand the Least Common Multiple *lcm* is known as the smallest nonnegative integer that is a multiple of each integer which is symbolized by *lcm(b,c)* .

3-Euler's Function$\emptyset(n)$, Fermat's and Euler's theorems:

Both these theorems are essential for public key cryptography, where the Euler function $\emptyset(n)$ is the size of the set of integers between 1 and *n-1*which are co-prime to *n*. For example to determine $\emptyset(3)$ we have the set Z_3={0, 1 ,2 } ;therefore, the co-prime number is the set{1,2} so (3)=2, as well as$\emptyset$ (9)=6 since{1,2,4,5,7,8} are relatively prime to 9, In addition$\emptyset$ (3*2)= $\emptyset$ (3)* $\emptyset$ (2)=2 same as $\emptyset$ (6) which is 2 since{1,5} are co-prime to 6 . Furthermore there is a lemma which says that if *a* and *b* are primes then $\emptyset(ab) = (a-1)(b-1)$. Euler's Theorem says "for any integer $m > 1$ if *gcd(a,m)=1* then $a^{\emptyset(m)} \equiv 1(mod\ m)$ "[6],[11],[12]. For example if *m=5* then $\emptyset$ (5) =4 since 5 is a prime number so applying the theorem give us: If *a=1* then $1^4 = 1$,also if a=2,3,4 then as a result 16, 81 and 256$\equiv 1(mod\ 5)$.

Also investigation was done into [13] Fermat's Theorem also known as 'Fermat's Little Theorem' which says if *hcf(a,p)=1* where *p* is prime and *a* is integer then $a^{p-1} \equiv 1(mod\ p)$.

For instance if *p*=11 and *a*=7 where 7 is co-prime to11 , then Fermat's theorem tells us that $7^{11-1} \equiv 1(mod\ 11)$ =282475249.

Consequently this theorem is helpful for determining the multiplicative inverse of an integer *a* due to $a^{p-2} \equiv a^{-1}(mod\ p)$.

In addition it is a special case of Euler's Theorem when the modulus *m* is prime.

Corollary:

If a is an integer, p a prime, does not divide a and $n \equiv m(mod\ p-1)$, then the following relation is satisfied$a^n \equiv a^m(mod\ p)$.

4- The Chinese Remainder Theorem:

The Chinese Remainder Theorem (CRT) says that there is a unique solution to the system of linear congruencies if the moduli are pair-wise co-prime.

CRT is useful for factoring the huge numbers which are needed in RSA cryptography.

Theorem: (Chinese Remainder Theorem) Let $n_1, n_2, \dots\dots, n_k$ be positive integers that satisfy $\gcd(n_i, n_j) = 1, \forall\ i \neq j$,(i.e are relatively primes in pairs) , furthermore let $m_1, m_2, \dots\dots, m_k$be integers ,then the system of linear congruencies :

$$x \equiv m_1(mod\ n_1)$$
$$x \equiv m_2(mod\ n_2)$$
$$x \equiv m_k(mod\ n_k)$$

Has a simultaneous solution x, where $0 < x < m-1, m = m_1 * m_2 * \dots * m_k$.

In addition, any two solutions are congruent to one another modulo *m* , proof [6], [3].

Example 1

Find the solution of $x \equiv 3(mod\ 12)$….(1), and $x \equiv 6(mod\ 35)$….(2).

Solution: It can Clearly be seen that 12 and 35 are relatively prime *gcd(12,35)=1* , therefore CRT can be used to solve the system by following the steps for the first solution of congruence (2), which should be written as the form $x = 6 + 35 * y$, where *y* denote an integer, then substitutes it into congruence (1), to give $6+35y \equiv 3(mod\ 12)$, so $35y = -3(mod\ 12)$,which equal to

$y \equiv 3(mod\ 12)$ because 35=36-1, therefore $(36-1)y \equiv -3(mod\ 12), 36 \equiv 0(mod\ 12)$, as a result $y=3$, then $x=111$, finally the check for the solution is easy and thorough due to: $111 \equiv 3(mod\ 12)\ and\ \ 111 \equiv 6(mod\ 35)$.

5- Public Key Encryption:

Public Key Algorithm is asymmetric when there are two different keys, one used to encrypt the message and one used to decrypt it.

The encryption key is named as a public key, while the key which decodes the message is known as a private key.

5-1-Definition (Public Key Cryptosystems):

"A cryptosystem consisting of a set of enciphering transformations $\{ E_e\}$ and a set of deciphering transformations $\{ D_d\}$ is called a public key cryptosystem or an Asymmetric cryptosystem if , for each key pair *(e,d)* , the enciphering key *e* , called the public key , is made publicly available , while the deciphering key *d* , called the private key , is kept secret.

The cryptosystem must satisfy the property that it is computationally infeasible to compute *d* from *e*, "[4].

5-2 -The Basic Principle:

Suppose that Ala intends to send a decryption message to her sister Fatema, therefore the recipient (Fatema) has to know the key. On the other hand, it may be unsafe for the sender (Ala) to tell Fatema what the key is. Because she does not want her Brother Ali listening in on their conversation and discovering what the key is. As a result, Ala and Fatema decided to use public key cryptography, so they have their own key pairs which consist of a public and a private key.

If they use the public key to encrypt a message, then only the private key can decrypt it, therefore it is impossible to know the private key, so this technique means that Ala and Fatema are unconcerned if Ali knows their public keys. Consequently, if the

message is sent to Fatema, it is encrypted using Fatema's public key, after which it is decrypted by using Fatema's private key.

In addition, the message cannot be decrypted by Ali, since Ali do not know Fatema's private key.

6-The RSA cryptography:

The mathematical principle for RSA cryptography is explained in [6] by the following lemma.

Lemma:

Let n be a positive integer which satisfies $(a,n)=1$. Therefore for any positive integers and such s that $s' \equiv 1(mod \emptyset(n))$ then $a^{ss'} \equiv a(mod\ n)$.

Proof:

The number ss' can be written as $ss' = 1 + r\emptyset(n)$, where r is a non-negative integer , then by applying Euler's Congruence the following result is found

$$a^{ss'} = a^{1+r\emptyset(n)} = a * a^{r\emptyset(n)} = a(a^{\emptyset(n)})^r = a * 1^r = a(mod\ n)$$

$(a^s, n) = 1$, is true since *(a,n)=1* and *a* is a positive integer.

Consequently if $m = \emptyset(n)$ and $r_1, r_2, \dots\dots, r_m$ is a system of reduced residues*(mod n)* then the numbers $r_1^s, r_2^s, \dots., r_m^s$ are also reduced residues.

The special case $s = \emptyset(n)$ tells us that the s^{th} powers may not all be distinct *(mod n).*

However according to the lemma that " *n* is a positive integer and *(a,n)*=1. If s and s' are positive integers such that $ss' \equiv 1(mod\ \emptyset(n))$then $a^{ss'} = a(mod\ n)$ "[4].

The s^{th} powers are distinct *(mod n)*,$\big(s, \emptyset(n)\big) = 1$, for s^{th} powers that is distinct *(mod n)* then $r_i^s \equiv r_j^s (mod\ n)$ and $\big(s, \emptyset(n)\big) = 1$, also by the Theorem " if *(a,n)*=1 then there is an x such that $ax \equiv 1(mod\ n)$ any two such x are congruent *(mod n)* if $(a,n) > 1$, then there is no such x " [4].

The positive integer s'such that $ss' \equiv 1(mod\ \emptyset(n))$is determined, after that the lemma:

$$r_i \equiv r_i^{ss'} = (r_i^s)^{s'} = r_j^{ss'} \equiv r_j(mod\ n)$$

This implies that $i = j$ and the numbers $r_1^s, r_2^s, \ldots, r_m^s$ are distinct *(mod n)* only if, $(s, \emptyset(n)) = 1$, as a result if $(s, \emptyset(n)) = 1$ the map $a \to a^s$permutes the reduced residues *(mod n)* then the further map $b \to b^s$ is the inverse permutation.

6 -1- The RSA Algorithm:

The RSA cryptosystem uses the following algorithm:

1- There are two positive integers of the public section of the key pair:

- N which is the modulus such as n-bit key.
- E which is public exponent.

2- There are positive integers of the private portion:

- P is a prime number.
- Q is a prime number.
- N is a modulus that derived from P and Q.
- E is the public exponent.
- D is a private exponent.

6-2- Description of the Algorithm:

In the public key cryptography algorithm the expression with exponentials is used.

The message is encrypted in blocks, where each block has a binary value which is less than n, namely the size of block is less than or equal to $\log_2(n)$. So $2^k < n < 2^{k+1}$ where the block size is k+1 bits, the following form illustrates the Encryption and Decryption:

$$B = A^e (mod\ n)$$
$$A = B^d (mod\ n) = A^{ed} (mod\ n)$$

Where *A* is a plaintext block and *B* is a cipher text block.

In particular, the value of *n* must be known by Ala (sender) and Fatema (receiver), the value of *e* is known by Ala, whereas the value of *d* is only known by Fatema.

Consequently the public key is *Pub={e,n}*, while the private key is *i={d,n}* , with the RSA algorithm [5].

7-RSA Key Generations:

The algorithm of RSA is broken into two portions which are explained by the assumption that Ala wants to send a message to Fatema:

A- RSA key Generation:

1. Two huge random prime numbers are generated by Fatema, such that $p \neq q$ and are nearly the same size.
2. She calculate $n = p * q$ and $\emptyset(n) = (p-1) * (q-1)$, where the integer n is Fatema's RSA modulus.
3. The random $e \in N$ is selected to satisfy $1 < e < \emptyset(n)$ and $(e, \emptyset(n)) = 1$, where the integer e is Fatema's RSA enciphering exponent.
4. The extended Euclidean algorithms are used, where Fatema computes the integer, where $1 < d < \emptyset(n)$, which satisfies $ed \equiv 1(mod \emptyset(n))$.
5. The integers (n, e) are published while d, p, q and $\emptyset(n)$,are kept secret .

Thus these items are dependent items. If one of them is known the remainder can be determined.

As a result, Fatema's RSA public key is $\{n, e\}$ and her RSA private key is d , where the integer d is Fatema's RSA deciphering exponent [14].

B- RSA Correctness Theorem

This is an important theorem related to inverse transformation of the RSA algorithm which says that the original message is recovered by decrypting an encrypted one .

$Pub(Pri\ M) = Pri(Pub\ M) = M,$ where $Pub(M) = M^e (mod\ n)$ and $Pri(M) = M^d (mod\ n)$. . [12]

Proof:

The left hand side becomes $Pub\big(Pri(M)\big) = \big(Pri(M)\big)^e (mod$ n) = $(M^d)^e (mod\ n) = M^{ed} (mod\ n)$.

Which is equal to M , the requirement is that:

$M^{ed}(mod\ n) = M(mod\ n)$, since $ed \equiv 1(mod\ \emptyset(n))$, this yields to:

$ed \equiv 1 + K(p-1)(q-1)$, where K is an integer.

Recall that $n = p * q$, we must first calculate for modulo p or q ,so there are two cases:

1- $M \neq 0(mod\ p)$, this implies

$M^{ed} \equiv M^{1+k(p-1)(q-1)}(mod\ p)$.

According to the Fermat's Little Theorem we have:

$M^{ed} \equiv M(1)^{k(q-1)}(mod\ p)$, so $M^{ed} = M(mod\ p)$.

$2 - M \equiv 0(mod\ p)$, this implies that $M^{ed} = M(mod\ p) \equiv 0(mod\ p)$,"if M is divisible by P ,the power of M is divisible by p "[12].

Therefore, $M^{ed} = M(mod\ p)\ \forall M < n$, similarly$M^{ed} = M(mod\ q)\ \forall M < n$,

According to the Chinese Remainder Theorem , $M^{ed} = M(mod\ n)$.

Example 2:

If the two prime numbers of Ala are $p = 5$ and $q = 7$,then she find $n = pq = 5 * 7 = 35$, after that she chooses numbers which are relatively prime to $\emptyset(n) = (p-1)(q-1)$,so $\emptyset(35) = 4 * 6 = 24$, therefore is a good choice, thus the public key is {35,11}, so Fatema is told the public key . Now Fatema can encode a message to Ala , , if the message is the number $M = 16$, the value c which satisfies $c = Me(mod\ n)$ is calculated by Fatema , so $c = 16_{11}(mod\ 35) = 11$, therefore the number 11 is the encoding message. Now Ala wants to decode it, so the number d which satisfies $ed = 1(mod\ \emptyset(n))$, must be found by Ala .

$11d = 1(mod\ 24)$, this implies that $d = 11$, since $11 * 11 = 121 = 5(24) + 1 = 1(mod\ 24)$.

Then Ala must determine $cd(mod\ n) = 11_{11}(mod\ 35)$. Initially Ala found this hard but she noticed that $11 = 10 + 1$, so $11_{11} = 11_{10+1} = 11_{10} * 11$, therefore the separate modulo calculation is determined:

$11(mod\ 35) = 11$,and $11_{10}(mod\ 35) = 11$.

Consequently, the final result is $11 * 11(mod\ 35) = 121(mod\ 35) = 16$

8-Definition:(Elliptic curve cryptography)

An elliptic curve $E_k = y^2 = x^3 + Ax + B$, k is a field of characteristic not equal to two or three.

In addition, different values of A and B which belong to k give different elliptic curves, the points $(x, y) \in k^2$ which are solutions of $E_k$equation together with an infinite point, from the elliptic curve.

A point in the curve represents the public key while a random number represents the private key.

Therefore, the domain parameter of elliptic curve cryptography consists of the creator point G and the parameters A and B [16], [17].

9- Discrete Logarithm Problems (DLP):

The security of ECC depends on the difficulty of ECDLP, (elliptic curve discrete logarithm problem).

Points on EC such that $p_{1,}, s = p_2$, where s is a scalar, here if s huge number s " is the discrete logarithm of p_2 to the base p_1 "[18].

Consequently, point multiplication is involved in ECC.

10- Point Multiplication:

Here we multiply the point p_1 which is on an Elliptic curve by a scalar s to have the point p_2 on same EC ($p_1 s = p_2$).

There are two operations of EC to achieve point multiplication.

1- Two points p_1 and p_2 are added to have new point $p_3 = p_1 + p_2$ in point addition.
2- The point p_1 is added to itself to have $p_2 = 2p_1$ in the point doubling [16],[18].

Example 3:

Suppose that there is a point p_1 on an Elliptic curve and another one p_2 obtained from multiplying the scalar s in the first one on EC, so we need to find $p_2 = 2p_1$.

Let $s = 13$ this implies that

$sp_1 = 13 * p_1 = 2\big(2(2p_1 + p_1)\big) + p_1.$

Therefore, the operations 1 and 2 are repeated to get the result, also this method is referred as "Double and Add".

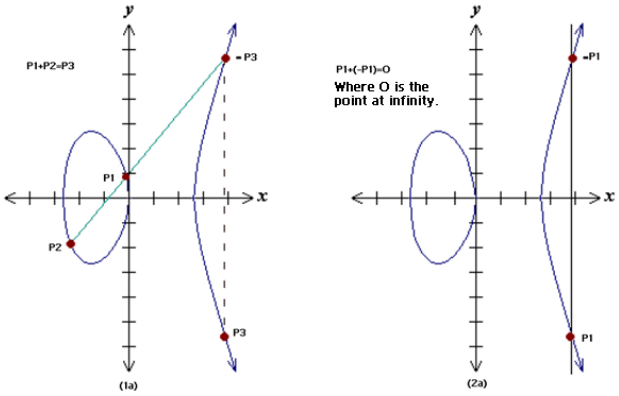
11-Point Addition:

Addition of points p_1 and p_2 on the EC lead to point p_3 on this curve representing point addition.

11-1-Geometrically:

Figure1 (1a and 2a) illustrate the points $p_1$and $p_2$on the Elliptic curve, where there is another point $-p_3$ that comes from the intersection of the line which is based through the points p_1 and p_2 where $p_1 \neq p_2$ on the EC. This gives us another point p_3 that comes from the reflection of $-p_3$ on x-axis, this is yield to $p_3 = p_1 + p_2$ which is on Elliptic curve.

On the other hand, the figure tells us that there is a point O at infinity that comes from the case when $p_1 = -p_2$consequently, $p_1 + (-p_2)$ =O ,where point O is defined as the additive identity of the EC group.



Point addition [18].

11-2-Analytically:

If the points $p_1 = (x_1, y_1)$ and $p_2 = (x_2, y_2)$ are considered then the point $p_3 = (x_3, y_3)$ is a result of $p_1 + p_2$,after that $x_3 = m^2 - x_1 - x_2$ and $y_3 = -y_1 + m(x_1 - x_3)$ where $m = \frac{y_1 - y_2}{x_1 - x_2}$ define the slope that comes from the line through $p_1$and p_2 .

There is another case that is when $p_1 = -p_2$, so $p_1 + p_2$= O , while the case when $p_1 = p_2$ give us $p_1 + p_2 = 2p_1$.

Furthermore, the case $p_1 + p_2 = p_2 + p_1$ is true [18].

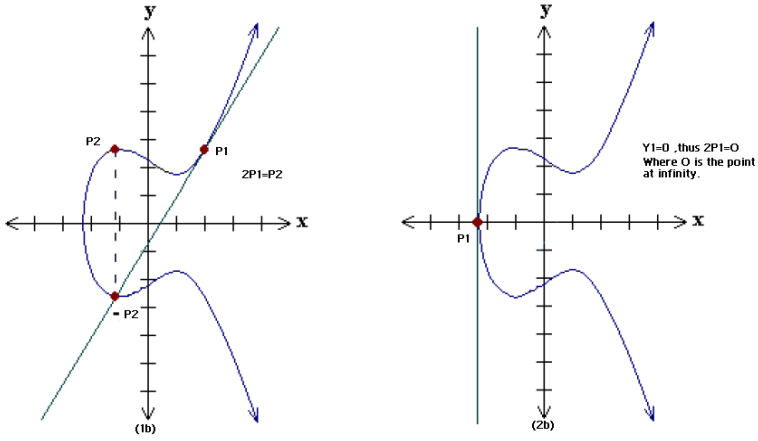
12-Point Doubling:

The point p_1 adding to itself on the Elliptic curve is called point doubling such that $p_2 = 2p_1$.

12-1- Geometrically:

The figure (1b) shows that a point p_1 is considered on the EC, then $p_2 = 2p_1$ is found, also there is a point $-p_2$ which comes from the intersection from the tangent line at point p_1 and EC, this situation happens if the y coordinate of $p_1$is not zero and the reflection of this point with the x-axis give us the point where .

Whereas figure (2b) illustrates that " if the y coordinate of the point is zero then the tangent at this point intersects at a point at infinity O, so $2p_1$ = O, when $y_1 = 0$ " [18].



Point doubling [18].

12-2-Analytically:

If the point is $p_1 = (x_1, y_1)\ \forall\ y_1 \neq 0$ considered we have $p_2 = 2p_1, p_2 = (x_2, y_2)$ then $x_2 = m^2 - 2x_1$ and $y_2 = -y_1 + m(x_1 - x_2)$ where $m = \frac{3x_1^2 + A}{2y_1}$, is the tangent at p_1 and A is the EC's parameter. There is a special case when $y_1 = 0$ that $2p_1$ =O; it can be noticed that these operations are done regarding the real numbers, but because of slowness and inaccuracy on the EC the finite fields are defined [18].

13-Finite Fields:

It is proposed to make operations on the EC more efficient, accurate and faster, thus there are two finite fields that are defined over the ECC.

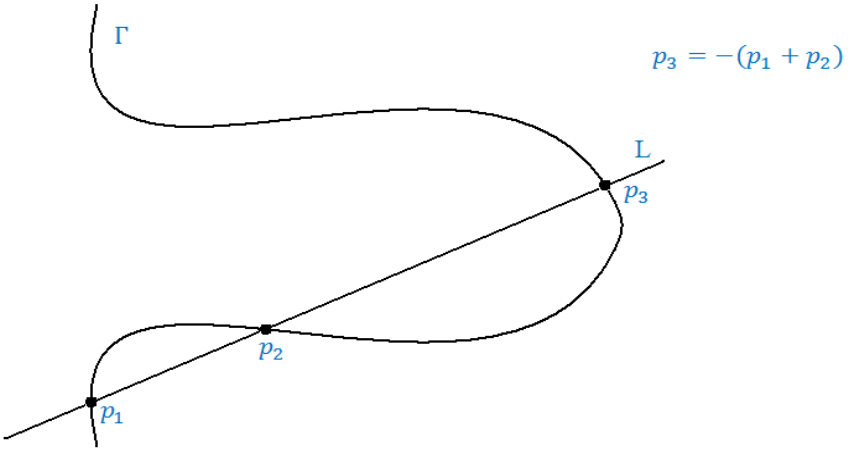
1- Prime field z_p .
2- Binary field z_2^m.

So we chose the field with finitely huge numbers of points that are suitable for cryptographic operation.

Here the affine coordinate system is presented which is a normal coordinate plane except that the point $p = (x, y)$ is represented by a vector see [18].

14-Theorem:

There is $abelian^*$ a group structure on EC, Γ with O element that is a point at infinity and for any line L in Cp^2 $L \cap \Gamma = \{p_1, p_2, p_3\}$ we have $p_1 + p_2 + p_3 = \mathrm{O}$.



$*$ $abelian$ group is a mathematical structure which consists of a set A with a group operation (i.e. (A , 0)), the (A,0) should satisfy the axiom of closure , associative , identity and inverse ,together with the property that if $x, y \in A$ then $xoy = yox$ [17].

Furthermore, if we have the group (A, X) then the encryption and decryption process for the message M is as follows:

$M \xrightarrow[decrypt]{encrypt} M^e = M * M * \dots \dots * M$ (e times multiplying).

$C \longrightarrow C^d = C * C| * \dots \dots * C$ (d times multiplying) where e and d are a public and private keys respectively and $ed \equiv 1(mod|A|)$for example in RSA the group A is that:

$(p-1)(q-1) = \emptyset(pq)$, where p and q are large prime.

On the other hand, if we have the group (A, +) then:

$M \xrightarrow[decrypt]{encrypt} eM = M + M + \cdots \dots . + M$ (e times addition)

$C \longrightarrow dC = C + C + \cdots \dots . + C$ (d times addition) and also .

15-Advantage and Disadvantage of ECC compared with RSA cryptography:

1- The main advantage for ECC is that the secure key size of ECC is smaller than the RSA key size with a 160 bit and a 1024 bit key respectively [18].

The following table also illustrates the key size comparison of MIPS years required for one key to be recovered, where MIPS means a million instructions per second [20].

Time to break in MIPS years	RSA/ECC key size ration
10^4	5:1
10^8	6:1
10^{11}	7:1
10^{20}	10:1
10^{78}	35:1

Key size equivalent strength comparison [15]

2- A disadvantage of ECC is that ECC requires a system of parameters, while RSA does not.

3-The similarity is that both ECC and RSA have both a public and a private key but the computation is different [24].

4-ECC is hard for an attacker to break.

5-ECC is more efficient than RSA.

6- One main disadvantage is that ECC has complicated algorithms.

Example 4:

Explain point addition and doubling on the Elliptic curve $y^2 = x^3 + 2x + 1$ over the field z_5 then perform an encryption and a decryption for the public key $e = 3$, private key $d = 5$ and the plain text $M = (0,1)$.

First, let us find the point that satisfies the EC equation; so there are seven points on this curve which are in the group where the table below shows that:

x	0	1	2	3	4
$y^2 = x^3 + 2x + 1$	1	4	3	4	3
	1 4	2 3	- -	2 3	- -

Ecliptic's curve points

Where $y^2 = 1$ implies that $y = \mp 1$,1(mod 5) =1 and $-1(mod\ 5) = 4$.

$y^2 = 4$ implies that $y = \mp 2(mod\ 5) = 2\ and\ 3$.

Consequently, $abelian$ group is (0,1) , (0,4) , (1,2) , (1,3) , (3,2) , (3,3) and O (infinity point).

In addition, every point has an inverse point such that:

(0,1)=-(0,4), (1,2)=-(1,3), (3,2)=-(3,3)

Now point addition can be explained as following:

Let $p_1 = (0,1)$ and $p_2 = (1,3)$ then$p_3 = p_1 + p_2$ to determine this point we need to find the line that passes through both points $p_1$and $p_2$so this line is $y = mx + b$, where $m = \frac{y_2 - y_1}{x_2 - x_1} = 2$, then by substituting one of the points $p_1$or p_2 we will have $b = 1$ therefore the line is $y = 2x + 1$ now we will examine

which point from abilian group satisfies this line to be the third point so , $p_3 = (3,2)$where $2 = 2 * 3(mod\ 5) + 1 = 2$.

In conclusion, $(0,1) + (1,3) = -(3,2) = (3,3)$.

Then point doubling is calculated as following:

Let $p_1 = (0,1)$, we need $p_2 = 2p_1$, in the point doubling we need to calculate the tangent line so, by differentiating the elliptic curve equation with respect to x to have $2y\frac{dy}{} = 3x^2 + 2$ then $\frac{dy}{dx} = \frac{3x^2+2}{2y}$ this equation at (0,1) implies that $\frac{dy}{dx} = 1$, therefore, the line is $y = x + 1$ where the point (1,2) satisfies it so ,$2(0,1) = -(1,2) = (1,3)$.

Finally, we will explain the encryption and decryption stage by the following steps:

We have $e = 3$ so $d = 5$, is a good choice because $ed = 1(mod\ 7)$, for $M = (0,1)$the encrypted process is $eM = 3M = 2M + m = 2(0,1) + (0,1) = (1,3) + (0,1) = (3,3)$ [by using the previous result in point addition and doubling].

Encoding message is $c = (3,3)$.

Now let us decrypt it so, $dc = 5c = 2(2c) + c$.

$2c = (3,3) + (3,3)$, so we need a tangent line which is $2y\frac{dy}{dx} = 2x^2 + 2$, at the point (3,3) we have $\frac{dy}{dx} = 4$ therefore , the tangent line is $y = 4x + 1$ and (0,1) lies on it this yield to $2c = (3,3) + (3,3) = -(0,1) = (0,4)$ then $4c = (1,2)$.

Finally 5c=-(0,4) [since $(1,2), (3,3)$ and$(0,4)$ lie on $y = 3x + 4$]

$5c = -(0,4) = (0,1) = M$

[The original plain text].

16- Conclusion:

This project has presented RSA cryptography to demonstrate that the prime numbers p and q used in the RSA algorithm must be large to make this system secure. In addition, it illustrates that RSA is widely used in real life and it is asymmetric, which is better than the old system (symmetric cryptography) that uses only one key to encrypt and decrypt messages. Whereas, RSA has two keys public

and private keys, as a result to break RSA algorithm is more difficult than another schemes such as symmetric one.

These issues are explained by a short comparison between public and secret keys.

Also this research is supported by strong theorems such as the Chinese reminder theorem that is used in RSA cryptography. In the final part of the project, ECC was defined over the field; to summarize this paper, ECC is more efficient than RSA, although its mathematical operations are more complicated than those of RSA. This research could be extended to more advanced investigations of ECC, in order to obtain a more secure system.

References:

1. *Yaschenko V. V.,"Cryptography An Introduction", AMS American Mathematical Society, 2002.*
2. *Stalling, William. "Crypotgraphy and network security".New Riders,June 3,2010.*
3. *Riesel H." Prime Numbers and Computer Methods for Factorization " , Birkhauser Boston. Basel. Stuttgart,1985.*
4. *Mollin A. R.,"RSA Public-Key Cryptography", Edition, Chapman &Hall/CRC, 1947.*
5. *Patel S. and Nayak P. P., "A Novel Method of Encryption Using Modified RSA Algorithm and Chinese Remainder Theorem".*
6. *Niven I. , Zuckerman S. H. and Montgomery ,"An Introduction to The Theory of Numbers", Edition, John Wiley & Sons, Inc. , 1991.*
7. *Pelikan J. , Lovasz L. and Vesztergombi, '' Discrete Mathematics Elementary and Beyond'' Springer – Verlag New York Berlin Heidelberg, 2003.*
8. *V. Miller, ''Uses of elliptic curves in cryptography'', Advances in Cryptology,Springer-Verlog New York,1986.*
9. *J. Krasner ''Using Elliptic Curve Cryptography (ECC) for Enhanced Embedded Security-Financial Advantages of ECC over RSA or Diffie-Hellman(DH) '' Embedded Market Forecasters Amercican Technology International, Inc. November 2004 .*

10. Korevaar N. ,"Powers in Modular Arithmetic and RSA Public Key Cryptography " Lecture notes , 2008.
http://www.math.http://www.math.princeton.edu/math_alive/1/Notes2.pdf
11. Konheim G. A., "Cryptography: A Primer" ,John Wiley & Sons, 1981.
12. Plummer R.," Number Theory , Examples , and RSA", October 31, 2008,
http://www.stanford.edu/class/cs103a/handouts/40%20Theorems,%20Examples,%20RSA.pdf
13. Grobschadl J. ,"The Chinese Remainder Theorem and its Application in a High-Speed RSA crypto chip".
14. Davis, T. ,"RSA encryption", October, 2003,
http://www.geometer.org/mathcircles
15. "The elliptic curve cryptosystem" , Certicom White paper , May , 1998,
http://www.comms.scitech.susx.ac.uk/fft/crypto/ECC_SC.pdf
16. Botes, J.J. and Penzhorn W.T.,"Public- key cryptosystems based on elliptic curves", IEEE, 1993.
17. Win D.E. and Preneel B.,"Elliptic curve public key cryptosystems –an introduction".
18. Ms A. ,'' Elliptic curve cryptography an implementation tutorial'',
http://www.reverse-engineering.info/Cryptography/AN1.5.07.pdf
19. Jeffrey L. Vagle, ''A Gentle Introduction to Elliptic Curve Cryptography'',BBN Technology , Nov21,2010.
20. " overview of elliptic curve cryptosystem",27th June , 1997,
http://www.rsa.com/rsalabs/node.asp?id=2013
21. W.Deffie and M.E.Hellman. New direction in cryptography. IEEE Transactions on Information Theroy,22:644-654,1976.