Computer Science and Engineering 2017, 7(1): 12-21
DOI: 10.5923/j.computer.20170701.02

Data and Information Security in Modern World

Md Obaidur Rahaman

Department of Computer Science and Engineering, European University of Bangladesh, Bangladesh

Abstract Data Security has become very important in today's world, as a result of which various methods are adopted to bypass it. With the advent of the internet, security became a major concern and the history of security allows a better understanding of the emergence of security technology. The internet structure itself allowed for many security threats to occur. The mechanism of the internet, when modified can reduce the possible attacks that can be sent across the network. Knowing the attack methods, allows for the appropriate security to emerge. Many modern spare secure themselves from the internet by means of decryption and encryption mechanisms. This paper outlines the various attack methods which are used, as well as various mechanism against them.

Keywords Data and Information Security

1. Introduction

Data security is one of the most important issues in the modern civilization. In this modern world most of the data are transferred and stored using internet. So it is important to secure our data from unauthorized access. Computer scientists are developing different types of mechanism to secure data. As old mechanisms are destroyed by different types of unauthorized attacks, computer scientists are developing new and modern types of security mechanism to protect data. Data are encrypted thus unauthorized user can't get actual data and decrypted to use by authorized user. Cryptology is the study of secure communications, which encompasses both cryptography and cryptanalysis [1]. Encrypted data must be decrypted to authorize user to make that data useable. Encryption is the conversion of plaintext or data into unintelligible form by means of a reversible translation, based on a translation table or algorithm, this is also called enciphering [1]. On the other hand decryption is the translation of encrypted text or data (called ciphertext) into original text or data (called plaintext), this is also called deciphering [1]. A strong data encryption and decryption technique is required to provide confidentiality of sensitive data from security attacks.

2. Security Goals and Threats

Security Goals

All information security measures try to address at least one of three goals:

- Protect the confidentiality of data
- Preserve the integrity of data
- Promote the availability of data for authorized use

These goals form confidentiality, integrity, availability (CIA) triad, the basis of all security programs. Information security professionals who create policies and procedures must consider each goal when creating a plan to protect a computer system [2].

2.1. Confidentiality

Confidentiality is the concealment of information or resources. The need for keeping information secret arises from the use of computers in sensitive fields such as government and industry. For example, military and civilian institutions in the government often restrict access to information to those who need that information. Valuable information or sensitive data must be protected from unathorized access. Access control mechanisms support confidentiality. A cryptographic key controls access to the unscrambled data, but then the cryptographic key itself becomes another datum to be protected.

2.2. Integrity

Integrity refers to the trustworthiness of data or resources, and it is usually phrased in terms of preventing improper or unauthorized change. Integrity includes data integrity, (the content of the information) and origin integrity (the source of the data, often called authentication). The source of the information may bear on its accuracy and credibility and on the trust that people place in the information. Integrity mechanisms fall into two classes: prevention mechanisms and detection mechanisms. Prevention mechanisms seek to maintain the integrity of the data by blocking any

* Corresponding author:
obaidur.rahman988@gmail.com (Md Obaidur Rahaman)
Published online at http://journal.sapub.org/computer

unauthorized attempts to change the data or any attempts to change the data in unauthorized ways. The distinction between these two types of attempts is important. Detection mechanisms do not try to prevent violations of integrity; they simply report that the data’s integrity is no longer trustworthy.

2.3. Availability

Availability refers to the ability to use the information or resource desired. Availability is an important aspect of reliability as well as of system design because an unavailable system is at least as bad as no system at all. The aspect of availability that is relevant to security is that someone may deliberately arrange to deny access to data or to a service by making it unavailable. System designs usually assume a statistical model to analyze expected patterns of use, and mechanisms ensure availability when that statistical model holds. Someone may be able to manipulate use (or parameters that control use, such as network traffic) so that the assumptions of the statistical model are no longer valid. This means that the mechanisms for keeping the resource or data available are working in an environment for which they were not designed. As a result, they will often fail.

3. Threats to Security Goals

A threat is a potential violation of security. The violation need not actually occur for there to be a threat. The fact that the violation might occurs means that those actions that could cause it to occur must be guarded against (or prepared for). Those actions are called attacks. Those who execute such actions, or cause them to be executed, are called attackers.

Our three goals of security – confidentiality, integrity, and availability – can be threatened by security attacks. The threats are divided into three groups related to the security goals [1].

3.1. Threats to Confidentiality

In data confidentiality two types of attack can be mention as threat. They are snooping and traffic analysis. Unauthorized access or interception of a confidential data is known as snooping. Snooping the unauthorized interception of information, is a form of disclosure. It is passive, suggesting simply that some entity is listening to (or reading) communications or browsing through files or system information. For example, a file transferred through the Internet may contain confidential information.

3.2. Threats to Integrity

The integrity of data can also be threatened by several kinds of attack such as: modification, masquerading, replaying and repudiation. After intercepting or accessing information data can be modified by unauthorized access. Modification means some portion of legitimate data is altered or delayed or reordered. The attacker intercepts the message and changes the types of transaction to benefit her. Unlike snooping, modification is active; it results from entity changing information. Active wiretapping is a form of modification in which data moving across a network is altered; the term active distinguishes it from snooping (passive wiretapping).

3.3. Threats to Availability

In security goal, there is only one attack threatening availability is called denial of service (DoS). Denial of service, a long-term inhibition of service, is a form of usurpation, although it is often used with other mechanisms to deceive. The attacker prevents a server from providing a service. The denial may occur at the source (by preventing the server from obtaining the resources needed to perform its function), at the destination (by blocking the communications from the server), or along the intermediate path (by discarding messages from either the client or the server, or both). Denial of service poses the same threat as an infinite delay [3]. Availability mechanisms counter this threat. Denial of service or delay may result from direct attacks or from non security related problems.

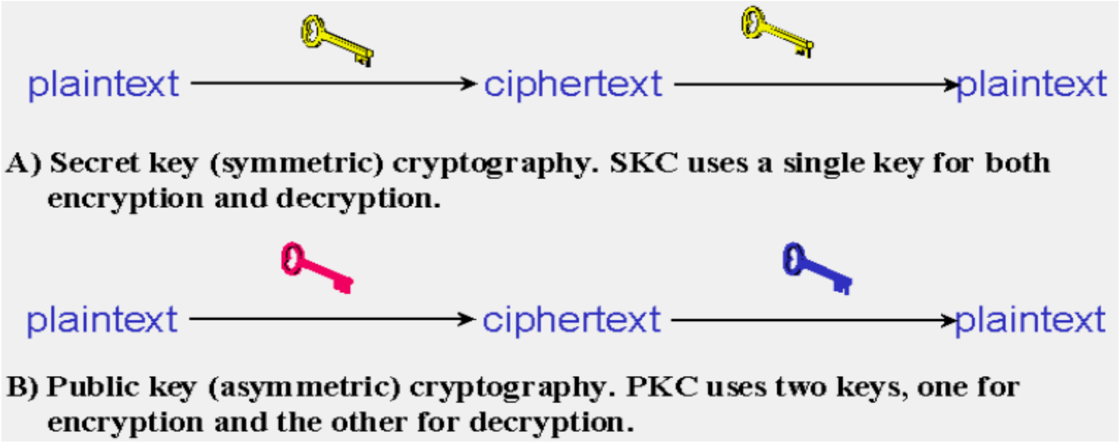
4. Cryptography

Cryptography is closely related to the disciplines of cryptology and cryptanalysis. Cryptography includes techniques such as microdots, merging words with images, and other ways to hide information in storage or transit. However, in today's computer-centric world, cryptography is most often associated with scrambling plaintext (ordinary text, sometimes referred to as cleartext) into ciphertext (a process called encryption), then back again (known as decryption). Individuals who practice this field are known as cryptographers. The basic component of cryptography is a cryptosystem.

4.1. Types of Cryptographic Algorithms

There are several ways of classifying cryptographic algorithms. For purposes of this paper, they will be categorized based on the number of keys that are employed for encryption and decryption, and further defined by their application and use. The two types of algorithms that will be discussed are (Figure 3.1):

- **Secret Key Cryptography (SKC):** Uses a single key for both encryption and decryption.
- **Public Key Cryptography (PKC):** Uses one key for encryption and another for decryption.



A) Secret key (symmetric) cryptography. SKC uses a single key for both encryption and decryption.

B) Public key (asymmetric) cryptography. PKC uses two keys, one for encryption and the other for decryption.

Figure 3.1. The two types of algorithms SKC & PKC

4.2. Secret Key Cryptography

With **secret key cryptography**, a single key is used for both encryption and decryption. As shown in Figure 3.1A, the sender uses the key (or some set of rules) to encrypt the plaintext and sends the ciphertext to the receiver. The receiver applies the same key (or ruleset) to decrypt the message and recover the plaintext. Because a single key is used for both functions, secret key cryptography is also called symmetric encryption.

There are two basic types of symmetric key/secret key ciphers:

- **Transposition ciphers**
- **Substitution ciphers**

Transposition Ciphers

In cryptography, a **transposition cipher** is a method of encryption by which the positions held by units of plaintext (which are commonly characters or groups of characters) are shifted according to a regular system, so that the ciphertext constitutes a permutation of the plaintext. That is, the order of the units is changed (the plaintext is reordered). A transposition cipher rearranges the characters in the plaintext to form the ciphertext. The letters are not changed.

Substitution ciphers

A **substitution cipher** changes characters in the plaintext to produce the ciphertext. It is a method of encoding by which units of plaintext are replaced with ciphertext, according to a fixed system; the "units" may be single letters (the most common), pairs of letters, triplets of letters, mixtures of the above, and so forth. The receiver decrypts the text by performing the inverse substitution. There are a number of different types of substitution cipher. If the cipher operates on single letters, it is termed a simple substitution cipher; a cipher that operates on larger groups of letters is termed polygraphic.

4.3. Public-Key Cryptography

Public-key cryptography is any system of encryption that uses a pair of cryptographic keys, where the system has the property that simply possessing one does not allow the practical calculation of the other. Typically the public key is used for encryption and may be disseminated widely, while the other - the private key, is used for decryption and is known only to the owner. Using the public key, any person can encrypt a message for the owner, and such message can only be decrypted with the owner's private key. Thus a message intended for a specific recipient can be encrypted and hosted safely on public servers with only the private key owner being able to read it. This system of using two different paired keys is called an asymmetric key encryption algorithm. The symmetric encryption/decryption is based on simpler algorithms and is much faster. [1] Public-key cryptography algorithms that are in use today for key exchange or digital signatures include.

4.4. Elliptic Curve Cryptography (ECC)

An elliptic curve is simply the locus of points in the x-y plane that satisfy an algebraic equation $y^2 = x^3 + ax + b$ of the form. Each choice of numbers a and b yields different elliptic curves. The value of x, y, a and b may be from any field, namely complex number, real number, finite number and so on [5].

4.5. ElGamal Cryptosystem using Elliptic Curve [2]

Several methods have been used to encrypt and decrypt using elliptic curves. The common one is to simulate the ElGamal cryptosystem using an elliptic curve over GF(p) or GF(2^n), as shown in the following figure 3(a).

Here $E_p(a,b)$, e_1 and e_2 are public key and d is the private key of the receiver.

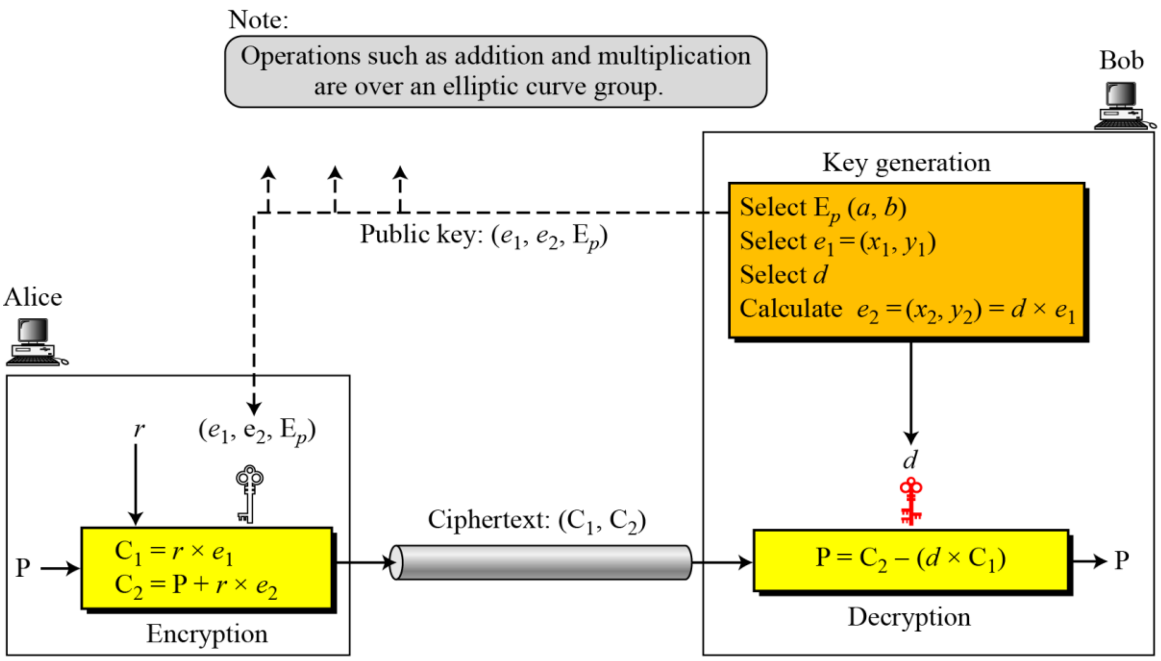

Note:
Operations such as addition and multiplication are over an elliptic curve group.
Bob
Key generation
Select E_p (a, b)
Select $e_1 = (x_1, y_1)$
Select d
Calculate $e_2 = (x_2, y_2) = d \times e_1$
Public key: (e_1, e_2, E_p)
Alice
r
(e_1, e_2, E_p)
P
$C_1 = r \times e_1$
$C_2 = P + r \times e_2$
Encryption
Ciphertext: (C_1, C_2)
d
$P = C_2 - (d \times C_1)$
P
Decryption

Figure (3a). ElGamal Cryptosystem using the Elliptic Curve

5. Elliptic Curve Cryptography

5.1. Finding Points on the Curve

Algorithm in the following shows the pseudocode for finding the points on the curve $E_p(a,b)$.

Algorithm

Pseudocode for finding points on an elliptic curve

```
            ellipticCurve_points (p,a,b)            //p is
the modulus
                  {    x←0
                       while(x < p)
                       {        w← (x^3+ax+b) mod p
//w is y^2
                                 if(w is a perfect square in
Z_p)output (x,√w)(x,-√w)
                                x←x+1
                       }
    }
```

Example: Consider $y^2 = x^3 + 2x + 3 \pmod 5$

$x = 0 \Rightarrow y^2 = 3 \Rightarrow$ no solution (mod 5)
$x = 1 \Rightarrow y^2 = 6 = 1 \Rightarrow y = 1{,}4 \pmod 5$
$x = 2 \Rightarrow y^2 = 15 = 0 \Rightarrow y = 0 \pmod 5$
$x = 3 \Rightarrow y^2 = 36 = 1 \Rightarrow y = 1{,}4 \pmod 5$
$x = 4 \Rightarrow y^2 = 75 = 0 \Rightarrow y = 0 \pmod 5$

Then points on the elliptic curve are , (1,1) (1,4) (2,0) (3,1) (3,4) (4,0) and the point at infinity: ∞.

5.2. Addition of Two Points

Let the points $P = (x_1, y_1)$ and $Q= (x_2, y_2)$ be in the elliptic group E_p (a, b), and O is the point at infinity. The rules for addition over the elliptic group E_p (a, b) are:

1. P+O=O+P=P

2. If $x_2= x_1$ and $y_2 = -y_1$, that is $P = (x_1, y_1)$ and $Q= (x_2, y_2) = (x_1, -y_1) = -P$, then P+Q=O.

3. If $Q \neq -P$, then the sum $P+Q = (x_3, y_3)$ is given by:

$$x_3 = \lambda^2 - x_1 - x_2 \bmod p$$
$$y_3 = \lambda(x_1 - x_3) - y_1 \bmod p$$

Where

$$\lambda \triangleq \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1}, & \text{if } P \neq Q \\ \dfrac{3x_1^2 + a}{2y_1}, & \text{if } P = Q \end{cases}$$

5.3. Subtraction of Two Points

Let the points $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be in the elliptic group E_p (a, b). The rules for subtraction over the elliptic group E_p (a, b) are:

1. P−Q=P+(−Q)=P+(inverse of Q), so the inverse of Q is $Q(x_2, y_2)= Q(x_2, -y_2)= Q(x_2, p-y_2)$.

5.4. Multiplication Points by a Constant

Let the points $P = (x_1, y_1)$ and the integer be k in the elliptic group E_p (a, b). Then Pk= Add P with k times.

e.g., $2P = P+P = (x_1, y_1) + (x_1, y_1) = (x_3, y_3)$.

where $\lambda = \left\{ \dfrac{3x_1^2 + a}{2y_1}, \text{ if } P = Q \right.$

and $x_3 = \lambda^2 - x_1 - x_2 \bmod p$, $y_3 = \lambda (x_1 - x_3) - y_1 \bmod p$.

5.5. Finding an Inverse

Let the points P = (x_1, y_1) and Q = (x_2, y_2) be in the elliptic group $E_p(a, b)$. Then the inverse of $Q(x_2, y_2)$ can be calculated as $Q(x_2, n - y_2)$ in Z_n where $n - y_2$ is called additive inverse in Z_n.

5.6. Point generation on Elliptic Curve

Let P = (3,10) ∈$E_{23}(1,1)$. Then 2P = (x_3, y_3) is equal to:

$$2P = P + P = (x_1, y_1) + (x_1, y_1)$$

Since P=Q and $x_2 = x_1$, the values of λ, x_3 and y_3 are given by:

$$\lambda = \frac{3x_1^2+a}{2y_1} \text{mod } p = \frac{3\times 3^2+1}{2\times 10} \text{ mod } 23$$

$$= \frac{5}{20} \text{ mod } 23 = 4^{-1} \text{ mod } 23$$

Considering, M_1^{-1} = (4^{-1} mod 23); where, M_1 = 4 and m_1 = 23

Now using extended Euclidean formula:

Here, quotient = q, remainder = r and t = $t_1 – qt_2$

Q	r_1	r_2	R	t_1	t_2	t
5	23	4	3	0	1	-5
1	4	3	1	1	-5	6
3	3	1	0	-5	6	-23
	1	0		6	-23	

Since, r_1 = 1

So that, M_1^{-1} = t_1

The extended Euclidean Algorithm gives t_1 = 6. So, the multiplicative inverse (M_1^{-1}) is 6 mod 23 =6.

$x_3=\lambda^2-x_1-x_2$ mod p = 6^2−3−3 mod 23 = 30 mod 23 = 7

$y_3=\lambda(x_1-x_3)-y_1$ mod p = 6×(3−7)−10 mod 23 = −34 mod 23 = 12

Therefore 2P = (x_3, y_3) = (7, 12).

The multiplication kP is obtained by doing the elliptic curve addition operation k times by following the same additive rules.

Table (4a). Elliptic Curve point generation for $E_{23}(1,1)$

K	$\lambda=\frac{y_2-y_1}{x_2-x_1}(if\ \ P\neq Q)\ or$ $\lambda=\frac{3x_1^2+a}{2y_1}(if\ \ P=Q)$	$x_3=\lambda^2-x_1-x_2$ mod 23	$y_3=\lambda(x_1-x_3)-y_1$ mod 23	kP (x_3, y_3)
1				(3,10)
2	6	7	12	(7,12)
3	12	19	5	(19,5)
4	4	17	3	(17,3)
5	11	9	19	(9,16)
6	1	12	4	(12,4)
7	7	11	3	(11,3)
8	2	13	16	(13,16)
9	19	0	1	(0,1)
10	3	6	4	(6,4)
11	21	18	20	(18,20)
12	16	5	4	(5,4)
13	20	1	7	(1,7)
14	13	4	0	(4,0)
15	13	1	16	(1,16)
16	20	5	19	(5,19)
17	16	18	3	(18,3)
18	21	6	19	(6,19)
19	3	0	22	(0,22)
20	19	13	7	(13,7)
21	2	11	20	(11,20)
22	7	12	19	(12,19)
23	1	9	7	(9,7)
24	11	17	20	(17,20)
25	4	19	18	(19,18)

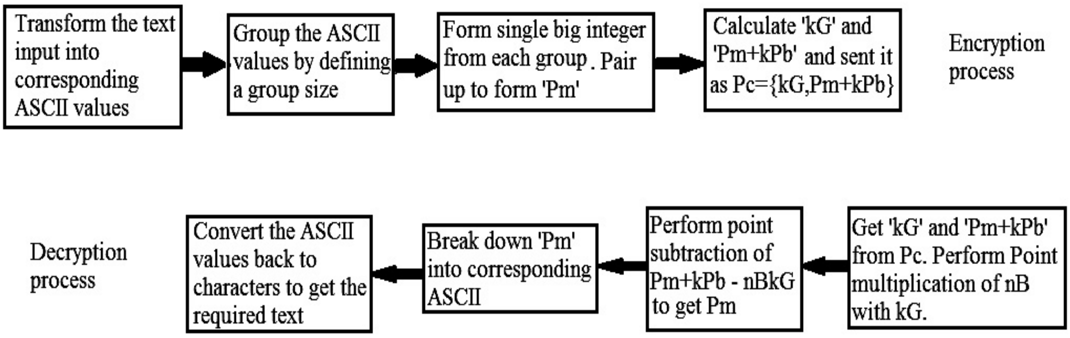

Transform the text input into corresponding ASCII values
Group the ASCII values by defining a group size
Form single big integer from each group. Pair up to form 'Pm'
Calculate 'kG' and 'Pm+kPb' and sent it as Pc={kG,Pm+kPb}
Encryption process
Decryption process
Convert the ASCII values back to characters to get the required text
Break down 'Pm' into corresponding ASCII
Perform point subtraction of Pm+kPb - nBkG to get Pm
Get 'kG' and 'Pm+kPb' from Pc. Perform Point multiplication of nB with kG.

Figure (5a). Encryption and Decryption process

6. Implementation of Text Encryption Using Elliptic Curve Cryptography

"Implementation of Text Encryption using Elliptic Curve Cryptography" [6] which avoids the costly operation of mapping and the need to share common lookup table between the sender and the receiver. They design the algorithm such a way that can be used to encrypt and decrypt any types of script with defined ASCII values. They discuss security issues and simulation of their algorithm.

The communicating parties agrees upon an Elliptic curve equation

$$y^2 = x^3 + ax + b \bmod p \qquad (1.1)$$

with the generator 'G' and makes the public keys ' P a' and ' P b' known to all and private keys '$n A$' and '$n B$' are kept secret. Here, they do not map the ASCII values of the characters to affine points of the elliptic curve. They group the ASCII values of the characters and perform cryptographic operation on the group. The size of each group is given by

$$\text{group size} = \text{Length[IntegerDigits}[p, 65536]] - 1 \qquad (1.2)$$

IntegerDigit [n, b] function in Mathematica gives a list of the base b digits in the integer n. Here, they choose base as 65536 because ASCII value is defined till 65535. Length is used to count the number of elements in the given expression. The group size help us to find the maximum number of characters that can be grouped up. Each group is converted into big integer values. They pair up the big integer value and use it as 'Pm' in the ECC operation. Pairing reduces the operation of mapping to elliptic coordinates and the need to share a common look up table. The whole encryption and decryption is shown as a block diagram in Fig. (5a).

6.1. Encryption

- Obtain the text to be send.
- Convert to its corresponding ASCII values.
- Partition the ASCII value as

Partition[ASCII values, group size, groupsize, 1, {}] (1.3)

This operation group the ASCII values with size given by group size with no overlapping and the later sub lists that have size lesser than group size are left as it is without padding.

- Each group obtained from the above step is converted into big integer values taking base as 65536.

FromDigits[Group of ASCII values, 65536] (1.4)

- Pad with 32 to the end of the list from the above step if the count of the above list is odd, to make it even for performing complete pairing. Each single pair will be an input to the ECC system as 'P m'. We pad with 32 because 32 represent blank space in ASCII code.
- Select random k value, k = Random value with range 1 to n − 1. Compute k G and k Pb using Point multiplication operation.
- Compute P m + k P b using point addition or point doubling as required.
- Send P c = {k G, P m + k P b} as cipher text to the receiver side.

6.2. Decryption

- Get the cipher text P c.
- Get the left part k G and right part P m + k P b of the P c separately.
- Multiply with n B to the left part and subtract it from the right part to get P m.

$$\{P_m + k\,P_b\} - n\,B\,k\,G = P\,m \qquad (1.5)$$

Since

$$P_b = n\,B\,G. \qquad (1.6)$$

Subtraction operation can be converted to addition by multiplying with −1 to the y coordinate. This operation can be justified with point addition operation. In point addition we used to get the mirror image point over the x -axis.

Example:- {97, 24} = {97, −24}.

- The above operation will yield the big integer value which is formed by combining group of ASCII values. Convert it back to list of ASCII values.

IntegerDigits[big integer, 65536] (1.7)

IntegerDigits [n, b] in Mathematica provides a list of the base b digits in the integer n. IntegerDigits and FromDigits function are inverse of each other, so the ASCII values are preserved during encryption and decryption.

- Convert the list of ASCII values to its corresponding characters

6.3. Encryption of Data using Elliptic Curve over Finite Fields

"Encryption of Data using Elliptic Curve over Finite Fields" [7] which describes a new algorithm of text encryption and decryption using a mapping table which is created using elliptic curve.

If two communicating parties Alice and Bob want to communicate the messages then they agree upon to use an elliptic curve $E_p(a,b)$ where p is a prime number and a random point C on the elliptic curve. Alice selects a large random number α which is less than the order of $E_p(a,b)$ and a point A on the elliptic curve. She computes $A_1 = \alpha (C + A)$ and $A_2 = \alpha A$. She keeps the random number α and the point A as her private keys and publishes A_1 and A_2 as her general public keys. Similarly Bob selects a large random number β and a point B on the elliptic curve. He computes

$B_1 = \beta (C+B)$ and $B_2 = \beta B$. He keeps the random number β and the point B as his private keys and publishes B_1 and B_2 as his general public keys. After publishing the public keys, the communicating parties again calculate the following quantities and publish them as their specific public keys of each other.

Alice calculates $A_B = \alpha B_2$ and publishes it as her specific public key for Bob.

Bob calculates $B_A = \beta A_2$ and publishes it as his specific public key for Alice

Alice's private key 1 = α, a large random number less than the order of the generator

Alice's private key 2 = a point A on the elliptic curve Ep(a,b)

Alice's general public key 1 = a point A 1on the elliptic curve Ep(a,b)

Alice's general public key 2 = a point A 2 on the elliptic curve Ep(a,b)

Alice's specific public key for Bob = a point A B on the elliptic curve Ep(a,b)

Bob's private key 1 = β, a large random number less than the order of the generator

Bob's private key 2 = B, a point on the elliptic curve Ep(a,b)

Bob's general public key 1 = B 1, a point on the elliptic curve Ep(a,b)

Bob's general public key 2 = B 2, a point on the elliptic curve Ep(a,b)

Bob's specific public key for Alice = B A, a point on the elliptic curve Ep(a,b).

6.3.1. Encryption

If Bob wants to communicate the message M then all the characters of the message are coded to the points on the elliptic curve using the code table which is agreed upon by the communicating parties Alice and Bob. Then each message point is encrypted to a pair of cipher points E_1, E_2. He uses a random number γ which is different for the encryption of different message points.

$$E_1 = \gamma C$$

$$E_2 = M + (\beta + \gamma) A_1 - \gamma A_2 + A_B$$

After encrypting all the characters of the message Bob converts the pair of points of each message point into the text characters using the code table. Then he communicates the cipher text to Alice in public channel.

6.3.2. Decryption

After receiving the cipher text, Alice converts the cipher text into the points on the elliptic curve and recognizes the points E_1 and E_2 of each character. Then she decrypts the message as follows.

$$= E_2 - (\alpha E_1 + \alpha B_1 + B_A)$$

Decryption works out properly:-

$$\begin{aligned}(\beta + \gamma) A_1 - \gamma A_2 + A_B &= \gamma (A_1 - A_2) + \beta A_1 + A_B \\ &= \gamma \alpha C + \beta \alpha C + \beta \alpha A + \beta \alpha B \\ &= \gamma \alpha C + \beta \alpha (A+B+C)\end{aligned}$$

$$\begin{aligned}\alpha E_1 + \alpha B_1 + B_A &= \alpha \gamma C + \alpha \beta C + \alpha \beta B + \alpha \beta A \\ &= \gamma \alpha C + \beta \alpha (A+B+C)\end{aligned}$$

Therefore, $(\beta + \gamma) A_1 - \gamma A_2 + A_B = \alpha E_1 + \alpha B_1 + B_A$

$E_2 - (\alpha E_1 + \alpha B_1 + B_A = [M + (\beta + \gamma) A_1 - \gamma A_2 + A_3] - [\alpha E_1 + \alpha B_1 + B_A]$
$= M + [\gamma \alpha C + \beta \alpha (A+B+C)] - [\gamma \alpha C + \beta \alpha (A+B+C)]$
$= M$

In this method a group of communicating parties A, B, C, D……. can communicate with one another securely, non-repudiatively in an authentic manner. Here each communicating party say X publishes two general public keys X_1, X2. X also publishes a specific public key X_Y to be used by the communicating party Y for communication with Y. When Y wants to communicate with X, Y uses the general public keys of X (X_1, X_2), the specific public key published by X for Y (X_Y) and Y's secret key y. To decrypt the message X uses Y's general public keys (Y_1, Y2), the specific public key published by Y for X (Y_X) and X's secret key x. Here X creates specific public key X_Y for Y using Y's public keys and X's secret key. So, this method of encryption using elliptic curves over finite fields is highly suitable for communication between groups of corporate/government institutions.

Example

Consider an elliptic curve whose equation is $y^2 = x^3 + 2x + 9$. The graph of the function is shown in fig. (5b).

In the above graph the right lines can be drawn in xy-plane such that 1) there is no intersection between the right line and elliptic curve 2) the line intersects the elliptic curve at one point or two points or three points.

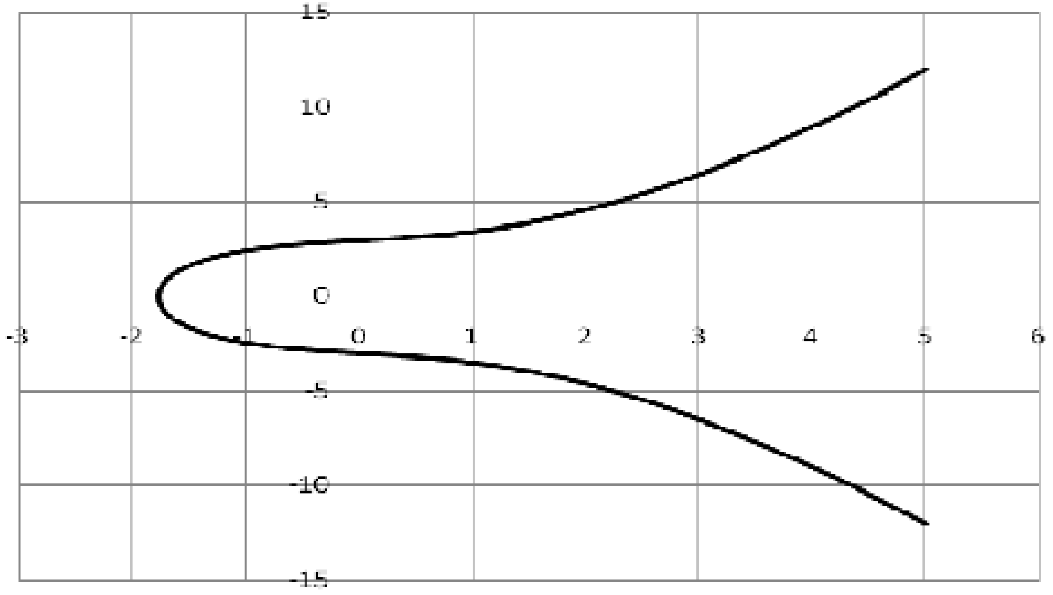


Figure (5b). Elliptic curve equation $y^2 = x^3 + 2x + 9$

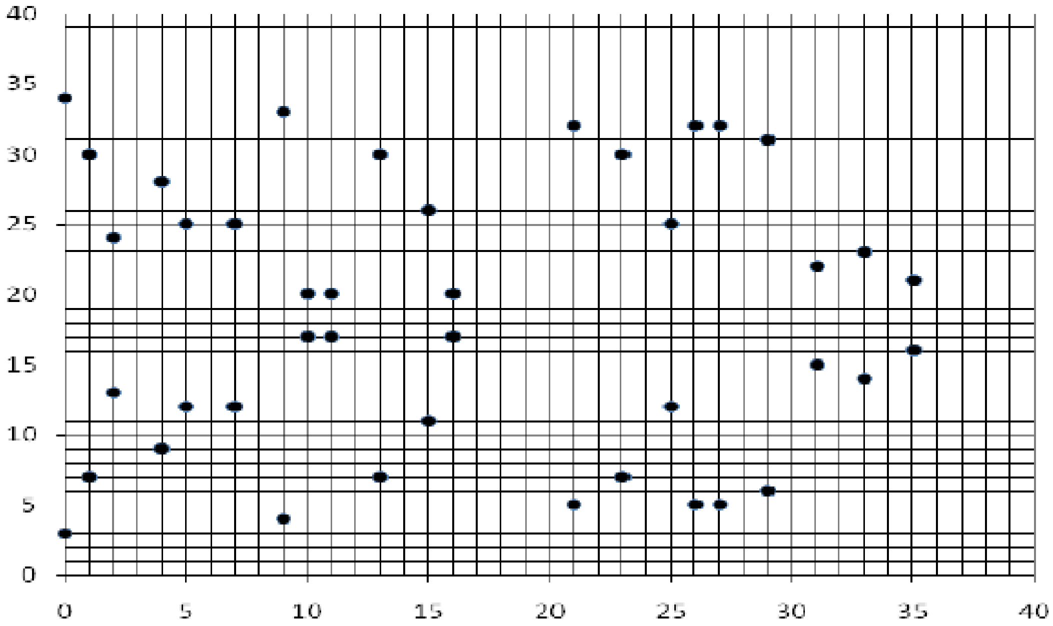


Figure (5c). Elliptic Curve Group (Cyclic) $E_{37}(2, 9)$

Table (5a). Code table "Encryption of Data using Elliptic Curve over Finite Fields"

*	A	b	C	D	e	F	g	h
∞	(5,25)	(1,30)	(21,32)	(7,25)	(25,12)	(4,28)	(0,34)	(16,17)
I	J	k	L	M	n	O	p	q
(15,26)	(27,32)	(9,4)	(2,24)	(26,5)	(33,14)	(11,17)	(31,22)	(13,30)
R	S	t	U	V	w	X	y	z
(35,21)	(23,7)	(10,17)	(29,6)	(29,31)	(10,20)	(23,30)	(35,16)	(13,7)

1	2	3	4	5	6	7	8	9	0
(31,15)	(11,20)	(33,23)	(26,32)	(2,13)	(9,33)	(27,5)	(15,11)	(16,20)	(0,3)
#	@	!	&	$	%				
(4,9)	(25,25)	(7,12)	(21,5)	(1,7)	(5,12)				

Now consider an elliptic curve ($y^2 = x^3 + 2x + 9$) mod 37, $E_{37}(2, 9)$. The points on the elliptic curve $E_{37}(2, 9)$ are

{∞, (5,25), (1,30), (21,32), (7,25), (25,12), (4,28), (0,34), (16,17), (15,26), (27,32), (9,4), (2,24), (26,5), (33,14), (11,17), (31,22), (13,30), (35,21), (23,7), (10,17), (29,6), (29,31), (10,20), (23,30), (35,16),(13,7), (31,15), (11,20), (33,23), (26,32), (2,13), (9,33), (27,5), (15,11), (16,20), (0,3), (4,9), (25,25), (7,12), (21,5), (1,7), (5,12)}

The graph of the function is shown in Figure (5c).

Let C = (9,4). Alice selects a random number α = 5, any point A = (10,20) on the elliptic curve. She computes

$$A_1 = \alpha\ (C+A) = 5[(9,4) + (10,20)] = (1,7)$$
$$A_2 = \alpha\ A = (33, 23).$$

She keeps the random number α = 5 and the point A on the elliptic curve as her secret keys and publishes A_1 and A_2 as her public keys.

Bob selects β = 7, B = (11, 20) on the elliptic curve. He computes

$$B_1 = \beta\ (C+B) = (11, 17)$$
$$B_2 = \beta\ B = (23, 30).$$

He keeps the random number β = 7 and the point B on the elliptic curve as his secret keys and publishes B 1 and B 2 as his public keys.

Alice calculates $A_B = \beta\ B_2 = (15, 11)$ and Bob calculates $B_A = \beta$ A 2 = (2, 13). Alice publishes A_B as the specific public key for Bob and Bob publishes B_A as specific public key for Alice.

6.3.2.1. Encryption

If Bob wants to communicate the message 'attack' to Alice, Bob converts all the text characters of the message into the points on the elliptic curves using the agreed upon code table.

1). In the message 'attack' the first character 'a' corresponds to the point (5,25) using the code table. Bob selects a random number γ = 8 for encrypting the character 'a'. Then the point (5,25) is encrypted as

$E_1 = \gamma\ C = (1,30)$ which corresponds to the character 'b' in the conversion table. $E_2 = M + (\beta + \gamma)\ A_1 - \gamma\ A_2 + A_B = (2,13)$ which corresponds to '5' in the code table. So, the character 'a' in the plain text is encrypted to two characters {b,5} in the cipher text.

2) 't' is a point (10,17) in the code table. Let γ = 12

$E_1 = (21,32)$ which corresponds to 'c' in the code table.

$E_2 = M + (\beta + \gamma)\ A_1 - \gamma\ A_2 + A_B = (2,24)$ which corresponds to 'l' in the code table. So, 't' is encrypted as {c,l}.

3) 't' is a point (10,17) in the code table. Let γ = 19

$E_1 = (4,9)$ which corresponds to '#' in the code table.

$E_2 = M + (\beta + \gamma)\ A_1 - \gamma\ A_2 + A_B = (27,32)$ which corresponds to 'j' in the code table. So, 't' is encrypted as {#,j}

4) 'a' is a point (5,25) in the code table. Let γ = 2

$E_1 = (29,31)$ which corresponds to 'v' in the code table.

$E_2 = M + (\beta + \gamma)\ A_1 - \gamma\ A_2 + A_B= (1,30)$ which corresponds to 'b' in the code table. So, 'c' is encrypted as {v,b}

5) 'c' is a point (21,32) in the code table. Let γ = 3

$E_1 = (1,30)$ which corresponds to 'b' in the code table.

$E_2 = M + (\beta + \gamma)\ A_1 - \gamma\ A_2 + A_B= (31,22)$ which corresponds to 'p' in the code table. So, 'a' is encrypted as{b,p}.

6) 'k' is a point (9,4) in the code table. Let γ = 23

$E_1 = (25,25)$ which corresponds to '@' in the code table.

$E_2 = M + (\beta + \gamma)\ A_1 - \gamma\ A_2 + A_B = (4,28)$ which corresponds to 'f' in the code table. So, 'k' is encrypted as {@,f}

Bob communicates {b,5; c,l; #,j; v,b; b,p; @,f }as the cipher text to Alice in public channel.

6.3.2.2. Decryption

Alice after receiving the cipher text {b,5; c,l; #,j; v,b; b,p; @,f} converts the cipher characters into the points (1,30), (2,13), (21,32), (2,24) (4,9), (27,32) (29,31) (1,30) (1,30) (31,22) (25,25) (4,28). She decrypts the message taking two points at a time as the points E1 and E2.

1. $M = E_2 - (\alpha E_1 + \alpha\ B_1 + B_A) = (5,25)$ which corresponds to the character 'a' in the code table.
2. $M = E_2 - (\alpha E_1 + \alpha\ B_1 + B_A) = (10,17)$ which corresponds t the character 't' in the code table.
3. $M = E_2 - (\alpha E_1 + \alpha\ B_1 + B_A) = (10,17)$ which corresponds to the character 't' in the code table.
4. $M = E_2 - (\alpha E_1 + \alpha\ B_1 + B_A) = (5,25)$ which corresponds to the character 'a' in the code table.
5. $M = E_2 - (\alpha E_1 + \alpha\ B_1 + B_A) = (21,32)$ which corresponds to the character 'c' in the code table.
6. $M = E_2 - (\alpha E_1 + \alpha\ B_1 + B_A) = (9,4)$ which corresponds to the character 'k' in the code table. Then 'attack' is the original message.

7. Conclusions

Data confidentiality is important to protect data from unauthorized access of confidential information. In this research work we have implemented a new way for text encryption and decryption using which provides data confidentiality. For higher security with lesser key size, we use Elliptic curve in our research work.

From the performance table, comparison table and security analysis section we can observe that our proposed algorithm has a lot of positive aspect. As Elliptic Curve Cryptography provides equal security like other cryptographic system but with less key size, it is very suitable for devices which have power, storage and processing limitation. So, our algorithm can be implemented in that device where less processing power and energy requires.

REFERENCES

[1] William Stallings, ―Cryptography and Network Security, Principles and Practice ‖ , [Forth Edition], Pearson Education Inc., 2006.

[2] Behrouza A. Forouzan and Debdeep Mukhopadhyay, ―Cryptography and Network Security ‖ , [Second Edition], McGraw Hill Education Private Limited, 2008.

[3] Georgios Loukas and Gulay Oke, ―Protection against Denial of Service Attacks: A Survey ‖ , Oxford University Press, 2009.

[4] Ross Anderson, Security Engineering: A Guide to Building Dependable Distributed Systems. The first edition (2001): http://www.cl.cam.ac.uk/~rja14/book.html.

[5] Charles Daney, "Elliptic Curves and Elliptic Functions", 1996, http://www.best.com/~cgd/home/flt/flt03.htm.

[6] Laiphrakpam Dolendro Singh and Khumanthem Manglem Singh, Implementation of Text Encryption using Elliptic Curve Cryptography, ELSEVIER, ScienceDirect, Procedia Computer Science 54(2015) 73-82 (2015).

[7] D. Sravana Kumar, CH. Suneetha and A. Chandrasekh AR, Encryption of Data using Elliptic Curve over Finite Fields, IJDPS Vol.3, No.1, January 2012.

[8] S. Maria Celestin Vigila and K. Munesswaran, Implementation of Text based Cryptosystem using Elliptic Curve Cryptography, International Conference on Advance Computing, IEEE, pp. 82-85, December (2009).