Two Level Encryption based on One Time Pad and Koblitz Method of Encoding

Jayashree Katti
PimpriChinchwad College of Engineering, Pune, India

Santoshi Pote
Usha Mittal Institute of Technology,Mumbai, India

B. K. Lande
Director,Vasantdada Patil College of engineering, Mumbai, India

ABSTRACT

With the advent of technology, traditional encryption techniques are facing challenges in key distribution and protection. This paper proposes a novel method of encryption using one time pad and elliptic curve cryptography. Given plain text will be encrypted using one time pad. The resulting cipher text will be encoded using Koblitz method of encoding. This paper describes Koblitz's method to represent a message to a point and point to message. It is already well known that one time pad is unbreakable cipher and is used when highest form of security is desired. The problem of key distribution and protection will be solved using elliptic curve cryptography.

Keywords

One Time Pad, Elliptic curve cryptography, Koblitz method

1. INTRODUCTION

1.1 One Time Pad

Cryptography is the art of keeping secrets, has always been fascinated by the notion of an ''Unbreakable'' cipher. In 1568 AD by the Frenchman B. de Vigenère invented a poly-alphabetic substitution cipher where a single letter of the message gets substituted to different symbols based on a secret key of certain length For sometime this was thought to be unbreakable. However, this was eventually broken by Charles Babbage in 1854. The search for an unbreakable cipher is continued until 1949, when for the first time, a mathematically sound definition of perfect secrecy was provided by Shannon [2]. He used concepts from information theory, which he had proposed to build a systematic mathematical theory of secrecy systems one year before was published. In [3], he showed that the One-Time Pad, invented way back in 1917, is indeed mathematically unbreakable[1]. The One-Time Pad or OTP for short is one of the simplest encryption algorithms. For binary messages, OTP encryption is achieved by an exclusive-OR operation (XOR) between every bit of the message with the corresponding bit of the private key (pad). The private key needs to be as long as the message for OTP to be unbreakable and can be used only once. Hence the name "Onetime Pad". Because of this nature it is used in quantum cryptography, DNA cryptography and classical cryptography, whenever the highest form of security is desired [1]. Until recently, the hot-line between Washington DC and Moscow for very high level communications was secured by OTP encryption [1]. OTP forms the basis of all modern stream ciphers.

1.2 Elliptic curve Cryptography

Elliptic Curve Cryptography (ECC) is a newer approach and considered as a well-known important technique with low key size for the user, and has a hard exponential time challenge for an intruder to break into the system. In ECC a 160-bit key provides the same security as compared to the traditional crypto system RSA with a 1024-bit key, thus lowers the computer power [4]. Therefore, ECC offers considerably greater security for a given key size.ECC makes implementations compact for a given level of security because of its smaller key size.

Elliptic curve cryptography is an asymmetric key cryptography. It includes (i) public key generation on the elliptic curve and its declaration for data encryption and (ii) private key generation and its use in data decryption depended on the points on two dimensional elliptical curve.

An elliptic curve in its standard form is described by $y^2 = x^3 + bx + c$.Public key is a point on the curve and private key is a random number. Multiplication of the generator G with private key will result in public key. Generator G, curve parameters b and c, together form the domain parameters of ECC.

The details of implementation of ECC on prime field and the discrete logarithm problem are discussed here.. An overview of ECC implementation on two dimensional representations of plain text coordinate systems and data encryption through ElGamal Encryption technique has also been discussed[11]. Main attention has been given to Koblitz method of encoding where plain-text will be converted as a series of points on an elliptic curve. Finally, the OTP key exchange through ElGamal cryptosystem will be discussed.

2. RELATED WORK

2.1 One-Time Pad: the unbreakable cipher

The electrical One-Time Pad was invented by Gilbert Vernam in 1917 for telegraph encryption [5]. It was known as the Vernam cipher and encryption was performed by combining each character in the message with a character on a paper tape key by means of an XOR operation. In the 1920s, the Vernam cipher was converted into a paper pad system. J. Mauborgne of the U.S. Army is credited with the development of the OTP in the modern form [8]. He observed that the use of a random,
Non-repeating private-key (pad) vastly improved the security of Vernam cipher. The OTP was extensively used by Russian agents operating in foreign countries. Rudolph Abel, a high ranking Russian agent captured in the United States in 1957 had in his possession a booklet of the size of a postage stamp containing a One-Time Pad [9]. The OTP encryption and decryption is described below:

1) The OTP is a random set of bits which is used as asymmetric key known only to Alice and Bob who want to communicate with each other.

2) The OTP encryption involves an XOR operation of the message M with the OTP key to yield the cipher-text C.

3) The OTP decryption involves an XOR of the cipher text C with the OTP key to get back the original message M.

A binary message $M = m_1 m_2 .... m_l$, is operated on by a binary private key string (the pad) $K = k_1 k_2 .... k_l$, of the same length *l* to produce a cipher text string $C = c_1 c_2 .... c_l$, where,

$$c_i = m_i \oplus k_i 1 \leq \mathrm{i} \leq \mathrm{l}$$

And where $\oplus$ stands for XOR operation (bitwise addition modulo 2). The key string K is composed of bits which are chosen in dependently and randomly. The key K is used only once and never used again.

Sender:	Receiver
M: 0 0 1 0 1 1 0 1 0 1	C: 1 0 0 1 1 1 1 1 0 0
K: 1 0 1 1 0 0 1 0 0 1	K: 1 0 1 1 0 0 1 0 0 1
----------------------------	----------------------------
C: 1 0 0 1 1 1 1 1 0 0	M: 0 0 1 0 1 1 0 1 0 1

Fig 1.Working of OTP

2.2 Security of OTP

Although it was observed that a non-repeating random private-key used only once for encryption vastly increases the security of the OTP, it was only in 1949 that the mathematical basis for this fact was provided by Shannon [3].The notion of perfect secrecy (also known as 'Shannon security mathematically unbreakable and unconditionally secure')defined by Shannon can be understood in the following way. If a passive cryptanalyst has only the cipher text $C = c_1 c_2 c_3 \cdots\ c_L$ which is the result of OTP encryption, the cryptanalyst can do no better than guessing the plaintext/message as being any binary string of length L. In other words, for the cryptanalyst, every binary string of length L is equally likely to be a plaintext [6]. This is the strongest notion of security since it is independent of statistical distribution of the plaintext and also of the computational resources. The uncertainty of the plaintext for the passive cryptanalyst does not reduce with the interception of the cipher text. This means that no information is leaked by the cipher text, whatsoever. This is a strong contrast to all other encryption algorithms, where some amount of information is unavoidably leaked by the cipher text. Shannon's result implies that OTP offers the best possible mathematical security of any encryption scheme.OTP remains as the only known perfectly secure, unbreakable cipher, till date. There have been many cryptographic algorithms in the last sixty years, both private-key and public-key algorithms [6], but none could offer perfect secrecy. In fact, popular algorithms such as RSA, ECC, DES and AES are not even proven to be computationally secure, but only believed to be hard to break, based on the failure of existing attempts. With rapid developments in quantum computing, belief in these algorithms may be under serious threat, whereas the OTP shall forever remain immune to any future developments in computing.

2.3 Elliptic Curve Cryptography

Koblitz and Miller independently suggested using elliptic curves in public-key cryptography in 1985 [7]. Since then, elliptic curve cryptography has attained considerable amount of interest in the cryptographic research community, and increasingly also in the industry. The main reason for the attraction of elliptic curve is that the shorter keys can be used for attaining similar level of security than in traditional public-key cryptography schemes based on the difficulty of integer factorization or discrete logarithm. For example, elliptic curve cryptography achieves approximately the same level of security with 173 bits than RSA with1024 bits. Studies have shown that elliptic curve cryptography is superior to RSA also in terms of speed and area required in implementation [7].

2.4 Role of Discrete Logarithm in ECC

The security due to ECC relies on the difficulty of Elliptic Curve Discrete Logarithm Problem. Let P and Q be two points on an elliptic curve such that kP = Q, where k is a scalar. Given P and Q, it is computationally infeasible to obtain k. If k is sufficiently large, k is the discrete logarithm of Q to the base P. Hence the main operation involved in ECC is related to the point multiplication i.e. multiplication of a scalar k with any point P on the curve to obtain another point Q on the curve.

2.5 Elliptic Curve Arithmetic

An elliptic curve is described by

$$y^2 = x^3 + bx + c$$

For the polynomial, $x^3 + ax + b$, the discriminant is given by

$$D = - (4a^3 + 27b^2) \qquad (2.2)$$

For the discriminant to have three distinct roots the above discriminant must not become zero for the given elliptic curve. If the discriminant is zero, it results in singular curves. It is not safe to use singular curves for cryptography as they are easy to crack. Due to this reason generally non-singular curves are used for data encryption.

2.5.1 Adding Two Points on an Elliptic Curve over Fp

Let Fp, where p an odd prime number, be a prime finite field. In Fig.1, given two points P = (x_1, y_1) and Q = (x_2, y_2) on an elliptic curve E(a, b) to compute the point P + Q. Figure 1 shows an algebraic curve for $y^2 = x^3 - 6x + 6$. First draw a straight line through P and Q. Next, find the third intersection of this line with the elliptic curve. Denote this point of intersection by -R. Then P + Q is equal to the mirror reflection of -R about the x-axis. In other words, if the points P, Q and R are the three intersections of the straight line with the curve, then
P + Q = R.

Addition Law: Let E be given by $y^2 = x^3 + bx + c$ and let
P_1 =(x_1, y_1), $P_2 = (x_2, y_2)$, then

$$P_1 + P_2 = P_3(x_3, y_3)$$

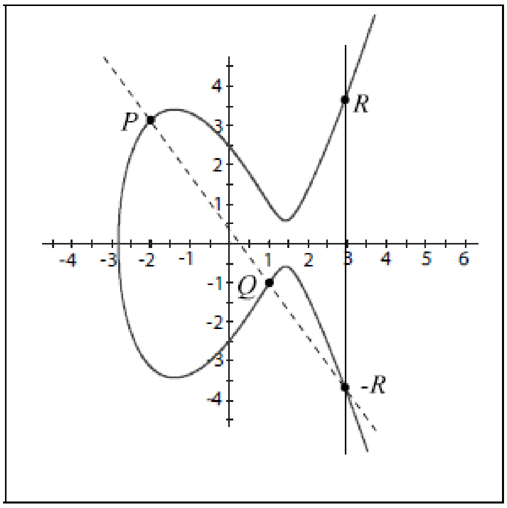
$$x_3 = m^2 - x_1 - x_2 \ \ (mod\ p)$$

$$y_3 = m(x_1 - x_3) - y_1 \ \ (mod\ p)$$

$$m = (y_2 - y_1)/(x_2 - x_1) \quad (mod\ p) \quad \text{if } P_1 \neq P_2$$

Otherwise

$$m = (3x_1^2 + b)/2y_1 \quad (mod\ p) \ \ \text{if } P_1 = P_2$$



$P = (-2, 3.162)$ and $Q = (1, -1)$ yield $P + Q = R = (2.925, 3.671)$ on $y^2 = x^3 - 6x + 6$

Fig 2.Adding two points on an Elliptic Curve

2.5.2 Point doubling

When P1= P2, this case is known as point doubling. Point doubling is similar to point addition. But only difference is take the tangent of a single point and find the intersection with the tangent line.Fig.2 Shows point doubling.

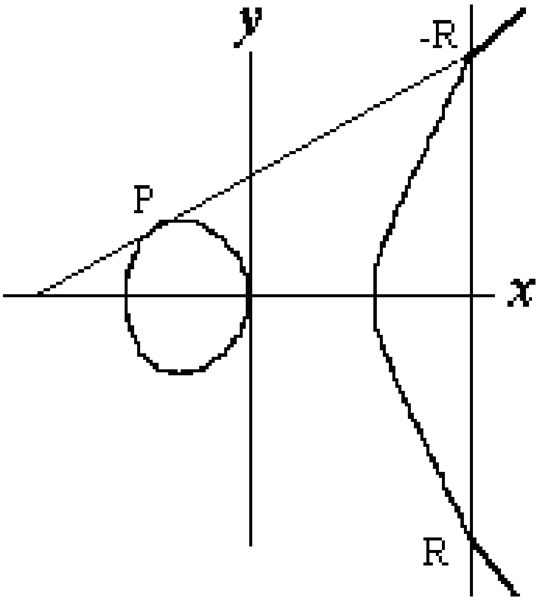
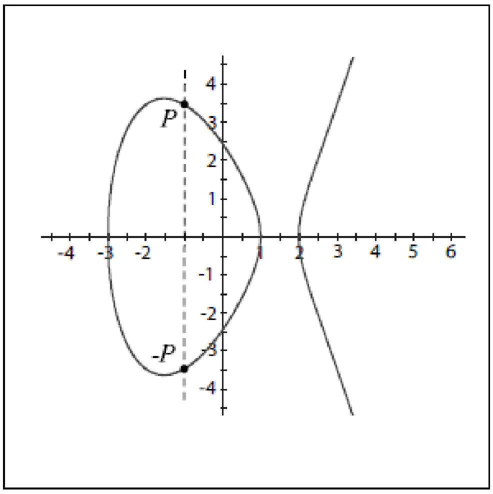


Fig 3.Point doubling

2.5.3 Adding the points P and –P:

The addition of the points P and −P poses a unique situation. The line through the points P and -P is a vertical line will not intersect the elliptic curve at any third point. Therefore addition of P and –P is defined as the point at infinity. I.e. P + (−P) =∞. Figure 3 illustrates this case.



$P + (-P) = \infty$ at $P = (-1, 3.464)$ on $y^2 = x^3 - 7x + 6$

Fig 4.Adding the points P and −P

Point multiplication:

Point multiplication, which is a basic component of every elliptic curve crypto-system, is defined by using point additions as follows:

$$Q = kP = P + P + P + \cdots k\ times$$

Where, Q, P∈ $E(F_p)$ and k is an integer. P is called the base point and Q is the result point. Security of elliptic curve cryptosystems is based on the difficulty of solving the inverse operation of point multiplication called elliptic curve discrete logarithm problem (ECDLP), i.e., the problem of finding k if P and Q are given. Point multiplication decomposes into three levels of hierarchy from top to bottom as follows:

3. PROPOSED ALGORITHM FOR INFORMATION SECURITY:

Here the given plain text will be encrypted using OTP. Then encrypted text will be represented as points on elliptic curve using Koblitz encoding method. These points will be sent to the receiver.

At the receiver side receiver will convert the points back to cipher text and then cipher text to plain text using OTP.

In spite of being strong cipher, OTP has key exchange problem. This key exchange problem can be solved using Elliptic curve ElGamal cryptosystem. The proposed algorithm is explained with the flowchart given in figure 1 and 2.

Part I. Encryption with One Time Pad

Let P be plaintext letter.
Let K be key letter
Let C be the cipher text letter.

$$\boxed{C_i = P_i \oplus K_i}$$

Where P_i = i^{th} bit of P

K_i= i^{th} bit of K

C_i= i^{th} t of C

Now C will be plain text letter to Koblitz method.

Part II. Koblitz's Method for encoding plaintext.

Step1: Pick an elliptic curve Ep(a,b) i.e.
$y^2=x^3+ax+b$ (mod p)

Step2: Convert the plain text character into integer corresponding to its ASCII value.

Step 3: Choose a large integer Q, such that failure rate ($1/2^Q$) is acceptable.

Step 4: C will be represented by a number x=CQ+ j, where $0 \le j < Q$.

Step 5: For j=0,1,2,….,Q-1 compute x^3+ax+b and try to calculate the square root of x^3+ax+b(mod p)

Step 6: If there is a square root y, then take point corresponding to C as (x, y).

Step 7: otherwise increment j by 1 and repeat the step 5.

Step 8: Repeat steps 5-7 until a square root is found or j=Q.

Step 9: Repeat steps 2-8 for all the characters of the cipher text resulting from one time pad encryption.

Part III: Encrypt the One time key using Elgamal elliptic curve cryptosystem.

Elliptic Curve ElGamal Cryptosystem

Let Alice wants to send a message x to Bob.

1. Bob chooses an elliptic curve E(Fp).
2. He chooses a point α on E and a secrete integer a
3. He computes

$$\beta=a\,\alpha(\alpha+\alpha+\alpha+\cdots+\alpha)$$

4. The points α and β made public while a is kept secret
5. Alice expresses her message as a point x on E.
6. she chooses a random number k and computes

$$y_1 = k\alpha$$
$$y_2 = x + k\beta$$

7. Alice sends $y_1, y_2$to Bob.
8. Bob decrypts by calculating

$$x = y_2 - ay_1$$

Decoding:

Part I: Decrypt the OTP key using ElGamal cryptosystem.

Part II: Consider each point (*x*, *y*) and set C to be the greatest integer less than (*x*-1)/*k*. Then the point (*x*, *y*) decodes as the symbol *C*.

Part III: Decrypt cipher text to plain text using decrypted OTP key

.

$$\boxed{P_i = C_i \oplus K_i}$$

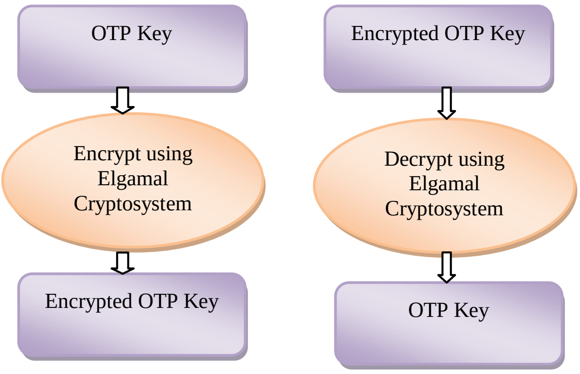

OTP Key
Encrypt using Elgamal Cryptosystem
Encrypted OTP Key
Encrypted OTP Key
Decrypt using Elgamal Cryptosystem
OTP Key

Fig 5.Encryption and decryption of OTP key

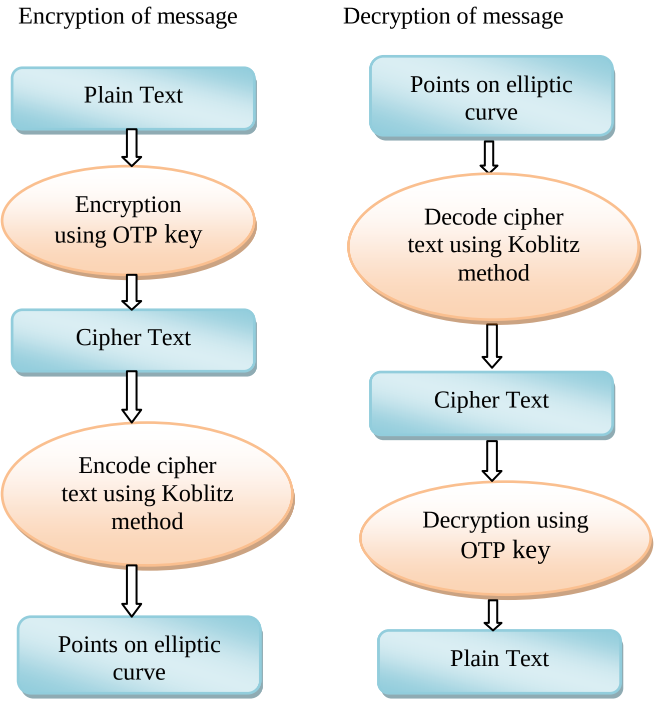


Fig 6 Encryption and decryption of message:

4. RESULTS

Following graph shows the experimental results of encryption and decryption of text files of different sizes, using proposed method.

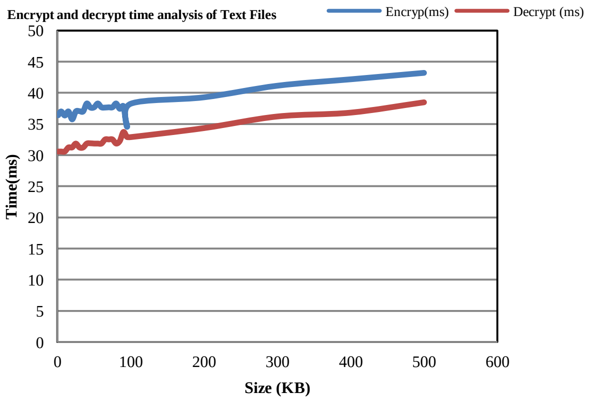


Fig 7Analysis of encryption and decryption time

5. CONCLUSION

In this paper, an overview of Koblitz method of encoding is provided and a hybrid security mechanism based on OTP has been developed. OTP is the only unbreakable cipher till date, which has been proved mathematically. Being a symmetric cipher OTP has key exchange problem. This has been solved with ElGamal cryptosystem.

This technique provides improved security compared to OTP as the given plaintext gets encrypted twice. A method to improve the performance of this technique shall be the subject of future communication.

6. REFERENCES

[1] Nithin Nagaraj, "Short communicationOne-Time Pad as a nonlinear dynamical system"Amrita Vishwa

Vidyapeetham, Amritapuri Campus, India,Elsevier, http://dx.doi.org/10.1016/j.cnsns.2012.03.020

[2] Shannon CE. Communication theory of secrecysystems. Bell Syst Tech J 1949;28:656–715

[3] Shannon CE. A mathematicaltheory of communication. Bell Syst Tech J 1948; 27:379–423

[4] Tarun Narayan Shankar, G. Sahoo, “Cryptography with Elliptic Curves”, International Journal Of Computer Science And Applications Vol. 2, No. 1, April / May 2009,ISSN: 0974-1003

[5] Menezes A, van Oorschot PC, Vanstone S. Handbook of applied cryptography. Boca Raton, FL: CRC Press; 1996

[6] Nithin Nagaraj and Vivek Vaidya “Re-visiting the One-Time Pad”, International Journal of Network Security, Vol.6, No.1, PP.94–102, Jan. 2008

[7] Kimmo Jarvinen and Jorma Skytta, “Fast point multiplication on Komblitz curves: Parallelization method and implementations”, Elsevier, Microprocessors and Microsystems, Volume 33, Issue 2, March 2009, Pages 106-116, doi:10.1016/j.micpro.2008.08.002

[8] Shukla, R. and Prakash, H.O., “Sampurna Suraksha: Unconditionally Secure and Authenticated One Time Pad Cryptosystem”, *IEEE Conference:* International Conference on Machine Intelligence and Research Advancement , 2013 ,Pages: 174 - 178, DOI: 10.1109/ICMIRA.2013.40

[9] Borowski, M., Lesniewicz, M.,“Modern usage of old one-time pad”, IEEE Conference :Communications and Information Systems 2012,Pages: 1 – 5, ISBN: 978-***1***-4673-1422-0.

[10] Songsheng Tang and Fuqiang Liu,“A one time pad encryption algorithm based on one-way hash and conventional block cipher”, *IEEE Conference*: 2nd International Conference on Consumer Electronics, Communications and Networks , 2012 Pages: 72 - 74, DOI: 10.1109/CECNet.2012.6201917

[11] Boruah, D.; Saikia, M., “Implementation of ElGamal Elliptic Curve Cryptography over prime field using C”, *IEEE Conference:* International Conference on Information Communication and Embedded Systems , 2014, Pages: 1 - 7, DOI: 10.1109/ICICES.2014.7033751