SECURITY AND COMMUNICATION NETWORKS
Security Comm. Networks 2016; **9**:4242–4254
Published online 7 September 2016 in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/sec.1601

RESEARCH ARTICLE

Elliptic curve coding technique application for digital signature

Kazim Yildiz[1]*, Ali Buldu[1] and Hasan Saritas[2]

[1] Marmara University Technology Faculty, Computer Engineering, Istanbul, Turkey
[2] Marmara University Technical Education Faculty, Electronic-Computer Education, Istanbul, Turkey

ABSTRACT

An elliptic curve coding technique application is proposed in this study. It is one of the asymmetric coding techniques and so crucial in today's world. The application codes messages between two different console screens by using elliptical curve coding technique. It is created by using C# with the class of Crypto Next Generation (CNG) which brings into consideration the messaging system as four different security levels. The aim is to use the necessary additional security precautions when using asymmetric techniques. Cryptography techniques are not used for connection, and messaging occurs in security level 1. Security level 2 describes the public channel for the connection between two console screens which is used for sending and receiving key pair; then messaging occurs. Public channel for the connection between two console screens is used for sending and receiving signed key pair and encrypted data; then messaging occurs in security level 3. Security level 4 is the safest one. A private channel for the connection between two console screens is used for sending and receiving a signed key pair and encrypted data, and then messaging occurs. In addition, Advanced Encryption Standard (AES) technique is used in applications which is one of the symmetric cryptographic techniques for encrypting data. Copyright © 2016 John Wiley & Sons, Ltd.

KEYWORDS

cryptology; elliptic curve coding; digital signature; security

***Correspondence**

Kazim Yildiz, Faculty of Technology, Computer Engineering, Marmara University, Istanbul, Turkey.
E-mail: kazim.yildiz@marmara.edu.tr

1. INTRODUCTION

The cryptography forms and confirms the digital signatures. In appearance, the class of applied mathematics convert messages into incomprehensible forms and turn original form again. The public key cryptography is used by digital signatures which operates an algorithm using two completely dissimilar keys that are mathematically connected. One of these keys is composing a digital signature or reducing information into an apparently obscure type, the opposite of key for confirming a digital signature. It is also reverting the message to its straight type. For advanced signatures, the supplementary keys of an asymmetric cryptosystem are randomly called as a private key. It is known as a signer; the digital signature is created by it and is more widely known. Public key is used by a trusting party for verifying the digital signature. The general public key should be obtainable or distributed to verify the signer's advanced signatures by the people. In spite of the keys are mathematically related and asymmetric crypto system has been processed and implemented securely, then it is computationally unfeasible to reproduce the non public key from the information of the general public key.

In this way, the general public key of a dedicated signer could be recognize by the people and used for confirming that signer's mark. The signer's non-public key cannot be found by them, and they use it to form digital marks. It is called as the standard of irreversibility. The other method is called as a hash function which is used in making and confirming a digital signature. This algorithm forms a digital acting or fingerprint like a hash value or hash result of a standard length. Typically, it is smaller than the message, but primarily original to that. If the message changes, then it produces a unique hash result once an identical hash operation is used. Under a secure hash function, it is called as a one-way hash function which is computationally unfeasible to breed the first message from data of its hash price. The computer codes are changed by hash functions

for making digital signatures. The people run on smaller and foreseeable amounts of knowledge which provides powerful apparent correlation to the initial message content. In this way, there has been no alteration of the information because it absolutely was digitally signed [1–10].

Digital signatures typically have two processes which every of them implemented by the signer and alternatively by the receiver of the digital signature. The first one is digital signature creation which uses a hash result that is reproduced from. It is original to both given private key and the signed message. To make secure hash result, there must be only an insignificant probability. The same digital signature can be created with the mixture of the other message and personal key. And the second one is digital signature verification which controls the digital signature. It uses inventive information and a given public key as reference. Because of the proposed digital signature, the non public key which follows to the documented public key has same message exploitation [11].

Elliptic curve E, Fq get on the surface and the elliptic curve point P as a point of order to get N primes. Each user [1, N − 1] range selects a random integer x. This user's public key q = xP point; x is the secret key. Hashing value of M message, H, $1 < H < N - 1$ can be an elliptic curve which uses digital signature algorithm for signing, which is as follows [12];

- A random integer k is chosen between [1, N − 1],
- $kP = (x_1, y_1)$ is calculated and $r = x_1 \ mod \ N$ assigned values. P point where the component is defined x_1 on *finite* object element; integer must be converted. If $r = 0$, go back to the first step then the process should begin again.
- k^{-1} mod N is calculated $s = k^{-1} \times (H + xr) \ mod \ N$ value is found. If s = 0, turn back to step one.

Messages can be created together using the elliptic curve signature (r, s). The following actions should be performed for verifying the digital signature which is created.

- The public Q key of a person who signs and sends messages is taken,
- Numbers r and s are confirmed to be in the range of [1, N − 1] and H hash value is calculated.
- $u_1 = s^{-1}$ H mod N and $u_2 = s^{-1}$ r mod N are calculated.
- $u_1 P + u_2 Q = (x_0 + y_0)$ is calculated and $v = x_0 \ mod \ N$ is found
- If v = r, then the signature is verified. Otherwise the message did not come from that client [13].

In this paper, section 2 defines the elliptic curve theory deeply. The method of the application is described in section 3. The development of the algorithm is described in section 4, and section 5 serves the working principle of the designed system. Finally, conclusion part is presented.

2. ELLIPTIC CURVE THEORY

Elliptical curves are not ellipse. The elliptical curves should be shown with the cubical equalities which is used by the calculations of the ellipse circles. If K is a selected object, and K should be defined as an object, R is as real numbers, Q is as rational numbers, C is as a complex number or P is accepted as a prime number, the Fq finite objects can be composed of elements. The finite object of GF (2) of the characteristic is 2; the characteristics of real and complex numbers are infinite.

For any object K, the general equation of the elliptic curve is as in below [14]:

$$y^2 + axy + by = x^3 + cx^2 + dx + e. \tag{1}$$

If the characteristic of K object Char $(K) = 2$, then equation (1) is transformed to equations (2) and (3),

$$y^2 + ay = x^3 + bx + c \tag{2}$$

$$y^2 + xy = x^3 + 2ax + b \tag{3}$$

The characteristic of K object Char (K) = 3; equation (1) can turn into equation (4);

$$y^2 = x^3 + 2ax + bx + c \tag{4}$$

If the characteristic of K object Char (K) = 2 or 3, equation (1) is converted to equation (5);

$$y^2 = x^3 + ax + b \tag{5}$$

Figure 1 shows the example of the form $y^2 = x^3 - 3x + 3$.

The affine transformations are used for each equation, and the values x, y, a, b, c, d and e are in the top of the K object in equations. The elliptic curve equation is called as an E which occurred from (x, y) points and in the field of K, even any of the requirements has to be in equations defined above. Elliptic curve coding technique has many advantages such as public key, uses small key sizes and is efficient for both private and public operations, such as signing and verifying.

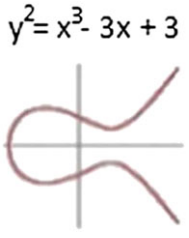

Figure 1. Example of the elliptic curve plain.

2.1. Elliptic curves

In general, the elliptic curve equation will be used in equation (5). In this equation a and b are real numbers and x^3+ax+b equation should be $4a^3+27b^2\neq 0$ to avoid the multiple roots. If $y^2=x^3+ax+b$ satisfies these conditions, it is called elliptic curve. Moreover, the elliptic curve in the infinite, or zero point is called an O notation. Because the greatest degree is over 3, so the equations of this type are called cubic.

Figure 2. Local network server and client connection.

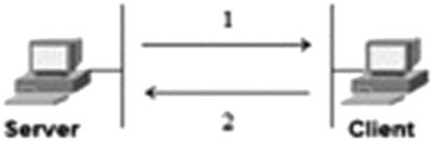

Figure 3. Basic messaging.

- For any point P on elliptic curve, P + O = P,
- A vertical line, the x value of an elliptic curve P1 = (x, y) and P2 = (x, −y). If it cuts two points, this line also cuts the eternity point of the elliptic curve at the same time. Therefore P1 + P2 + O = O and P1 = −P2. Thus, negative value of a point is a point having the same value on x axis. The value of that point in y axis equals to its negative value [15].
- The x coordinate of the intersection of the different Q and R is selected from a straight line drawn from the last two points; the third point of intersection is found as P1. P1 is only one point (If passed right tangents drawn from one of the Q or R point in this case then P1 or P2 = Q = Q is taken) [9,16]. In this case: P1 + Q + R = O and so Q + R = −P1 will be.
- For P point to make double, a tangent line intersecting the other point of the curve is drawn. If this point is called as −R, then P + P = 2P = R equality is provided.

3. ELLIPTIC CURVE ENCRYPTION TECHNICAL APPLICATION

3.1. General properties of elliptic curve cryptography application

Elliptic curve encryption implementation was carried out which is called simply Crypto Next Generation (CNG) crypto-class next generation in MS Visual Studio 2008.

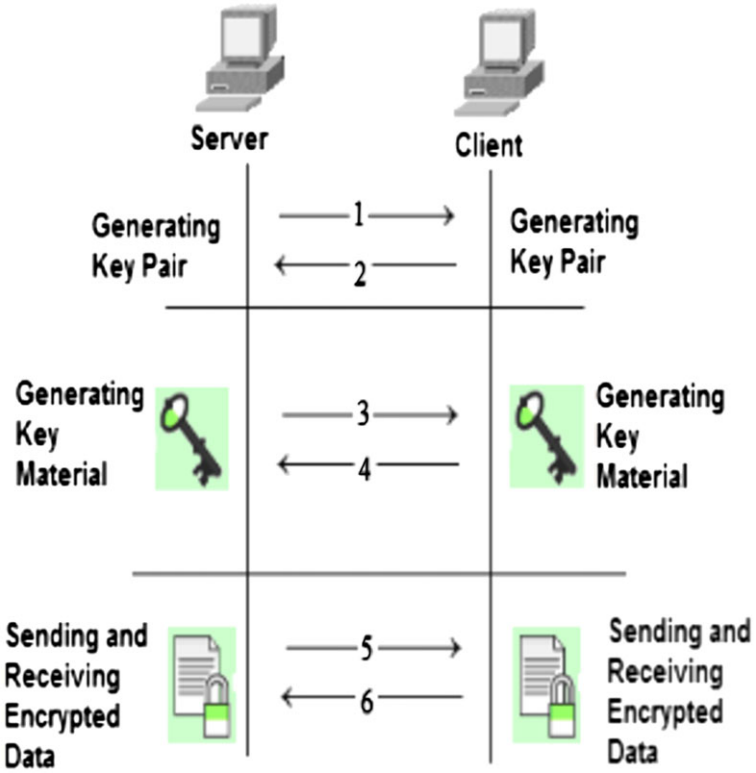

Figure 4. Public and private key pair.

Security Comm. Networks 2016; **9**:4242–4254 © 2016 John Wiley & Sons, Ltd.
DOI: 10.1002/sec

The application on the local network between server and client computers by using elliptic curve encryption technique was revived for different security levels. Public and private key pairs are created by using cryptographic security environments, eavesdropping, denial and displacement that take place through methods such as the attacks. It is difficult to decode with the technology to Elliptic Curve Cryptography Technique so some attacks are taken into account. The application of elliptic curve encryption technique, 256, 384 and 512-bit length, is achieved by using public and private key pairs [17]. Figure 2 shows the connection between the server and client computers over a local network.

3.1.1. Security levels

This application is created using the Elliptic Curve encryption method that works in four different security levels which are basic messaging, using public and private key pair messaging, using a digital signature messaging and using a digital signature messaging through a private channel is called.

3.1.2. Basic messaging

The server computer and client computer are connected to each other via a local network. This communication takes place over the connection without any security level. Figure 3 shows at security level 1 the realization of the exchange of information without a safety precaution.

3.1.3. Use of public and private key pair

The server and client computers over a local network connected to each other through the open channel. Server computer creates a public and private key pair that the public key is sent to the client. The client computer also performs the reverse operations. Server generates a shared secret key by using the client's public key and its private key. Similarly, the client computer generates a secret key which is shared. Server, using the generated shared secret key, generates the key materials. Similarly, the client computer generates key materials. Server encrypts the message using the key materials and sends it to the client. The encrypted message is received by the client and decrypts it with key materials; a similar situation occurs directly to the server to the client. One to one connection between server and client will be established according to the security level 2. Figure 4 shows the security level 2 according to the connection between the server and the client is streaming.

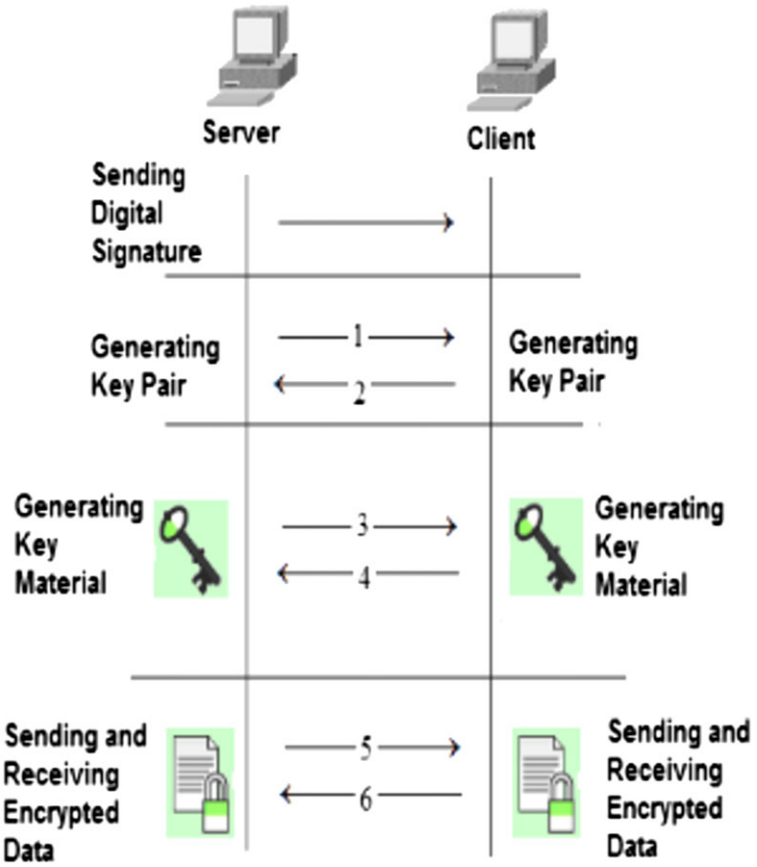

Figure 5. Using digital signature.

3.1.4. Digital signature usage

In addition to security level 2, key pairs and messages are encrypted with a digital signature. Before producing the key pairs, the digital signature is sent from the server to the client over a public channel shown in Figure 5.

3.1.5. Using the digital signature over a private channel

Security level 4 provides a fully implemented level of elliptic curve encryption method. According to a previous level of security, digital signature from the computer server to the client computer is sent through a private channel. Public channels are sent over the digital signature for deception. The connection between the server computer and client computer created two different channels as shown in Figure 6. The first channel with a '0' is shown. Invalid digital signature for deception was sent through this channel. The second channel of the '0' is shown. Real digital signature is sent to a private channel on the server computer to the client computer which is sent via private channel.

4. ALGORITHMS IN THE APPLICATION

The Elliptic Curve Diffie–Hellman (ECDH) and Advanced Encryption Standard (AES) algorithms are used in the application. When a connection is established between the server and client computer, the ECDH algorithm is used for the security of the connection as well as the AES algorithm, and hash function is used for the data encryption. ECDH algorithm is preferred in terms of reliability and performance among other asymmetric algorithms. The AES is a kind of symmetric algorithm which has better performance at encryption and decryption process of communication between server and client computers.

4.1. ECDH algorithm

ECDH algorithm is created based on two open parameters [18]. These parameters are P and G. The parameter P is

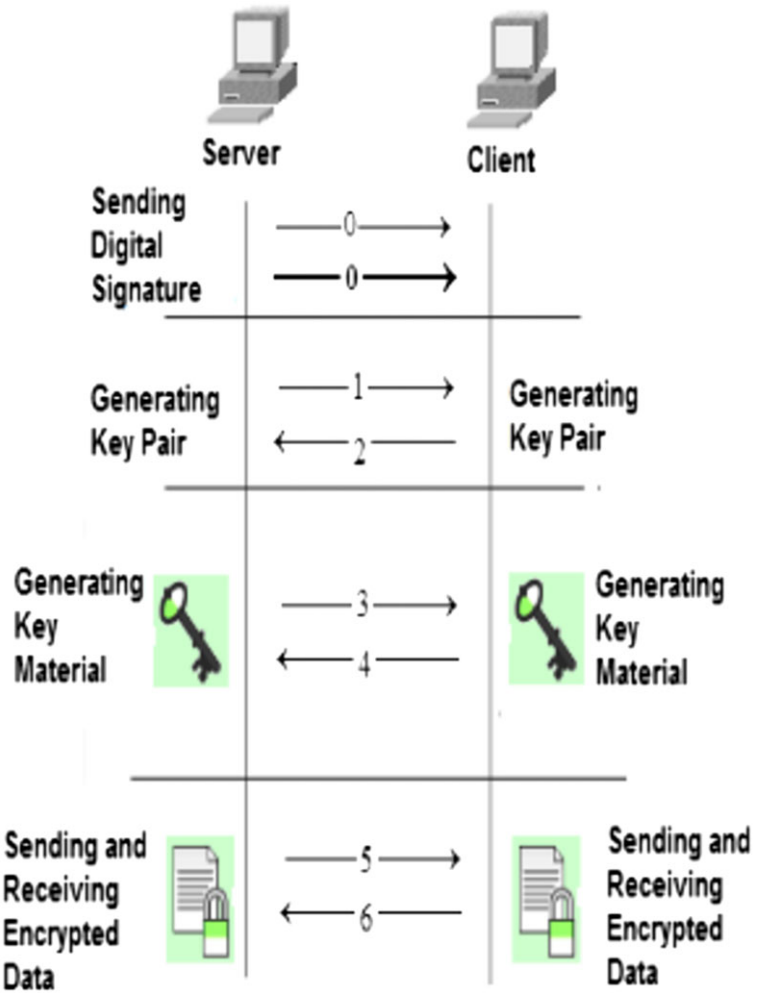

Figure 6. Using the digital signature over a private channel.

Security Comm. Networks 2016; **9**:4242–4254 © 2016 John Wiley & Sons, Ltd.
DOI: 10.1002/sec

the big prime number, and the other parameter is an integer which is smaller than P. These are exchanged between the server computer and client computer. The private keys are generated by server and client computer after receiving two parameters. Server computer (A) and client computer (B) produce their own public keys using the own private keys and parameters. The equation of (g^a) mod p is used by server computer, and also the equation of (g^b) mod p is used by client computer. These are asymmetric keys which are not the same with one another. The public keys of server (A) and client (B) computers are obtained by using the shared secret key. ECDH algorithm provides that server and client computer produce the same shared secret keys.

a, b and g^ab = g^ ba is open to everyone.

The shared secret key cannot be reproduced without knowing the private keys which are generated by server and client computer. In order to establish secure connection between server and client computer with the help of ECDH algorithm, it must be a very well-known source of the open parameters. To ensure this, there are two methods:

- Server and client computers encrypt their own public keys with their own digital signatures. Then the encrypted public key is sent to the other computer in a secure channel.
- The digital signature keys which have certification authority (CA) are used. For both methods, the validity of the public keys is checked.

4.2. AES algorithm

In the elliptic curve application, AES [19] symmetric algorithm is used for encrypting and decrypting the data which belongs to server or client computers. After sending and receiving the public keys for server and client computers, the method of the ECDH derives a key material that is generated from secret agreement between server and client computers. The key material is used by AES symmetric algorithm to encrypt or to decrypt the data which is produced by server or client computers. The algorithm consists of two main blocks: encryptor/decryptor and key generator.

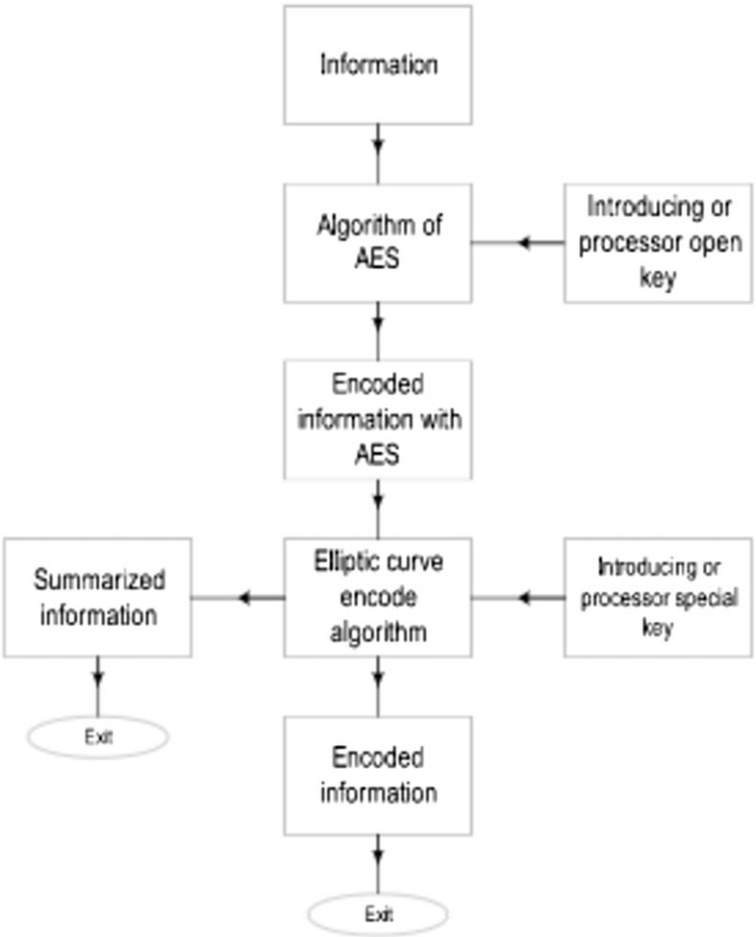

Figure 7. Elliptic curve algorithm, AES algorithm and hash function relationship.

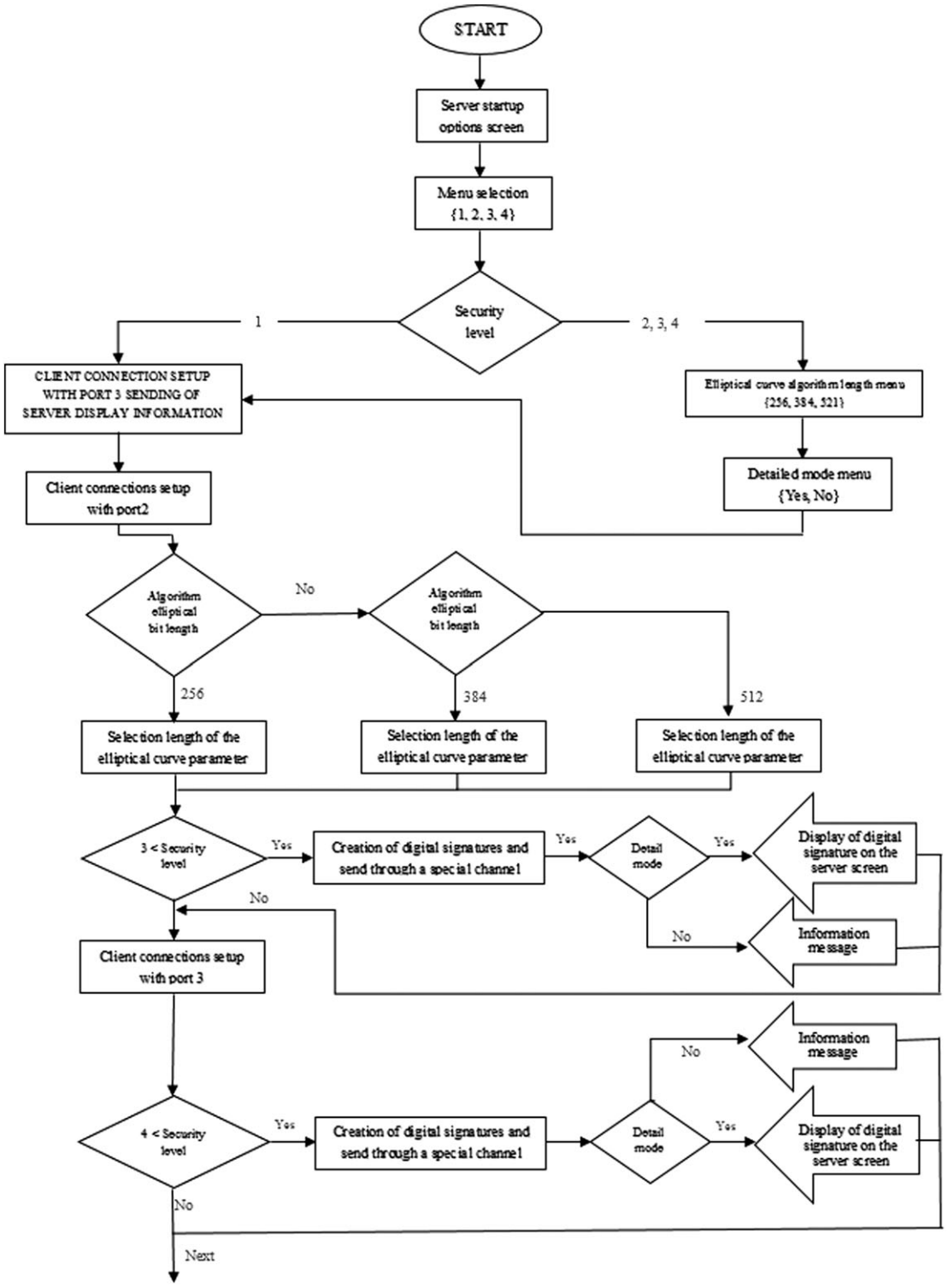

Figure 8. The elliptic curve encryption flow diagram.

4.3. Hash function

Hashing is very useful in computer applications for example in special public key cryptography counts on cryptographic functions [20]. A cryptographic hash function has the following properties which are pre image resistance, second pre image resistance and collision resistance [21]. At security level 2 for server and client sides, the hash

function of the communication class is executed for verifying if the data is reliable or not. The key length of algorithms and the hash function are determined at the same time. As a result of this, the integrity of the elliptic curve application is being realized. Figure 7 shows that the relationship between the AES algorithm and the hash function and the ECDH algorithm in the application.

Figures 8 and 9 show the whole process in the section of the elliptic curve encryption flow together. From startup to end of the stage, it describes all the phase of designed algorithms. The all encryption and decoding process are defined there.

5. THE WORKING PRINCIPLE OF THE APPLICATION OF ELLIPTIC CURVE ENCRYPTION

In the application stage on local network, server and client computers use the encryption keys which have 256, 384 or 521 bit length. Figure 10 shows the connection of the server and client computers on the local network via switch. Figure 11 shows the opening of the server and client console screens.

5.1. Server and client work

The Class of TcpListener which is on server computer is used for listening to demand the connection from a port which is connected to the client computer. On the other hand, the class of TcpIstemci which is on the client computer is used for sending the IP address of the server computer from a port which is connected to the server computer. The server computer listens on the port and accepts incoming connection requests. After that, the connection between the server computer and the client computer will be realized. In elliptic curve encryption, encrypted messaging that is from the main menu, when the second security level is selected from the main menu, respectively,

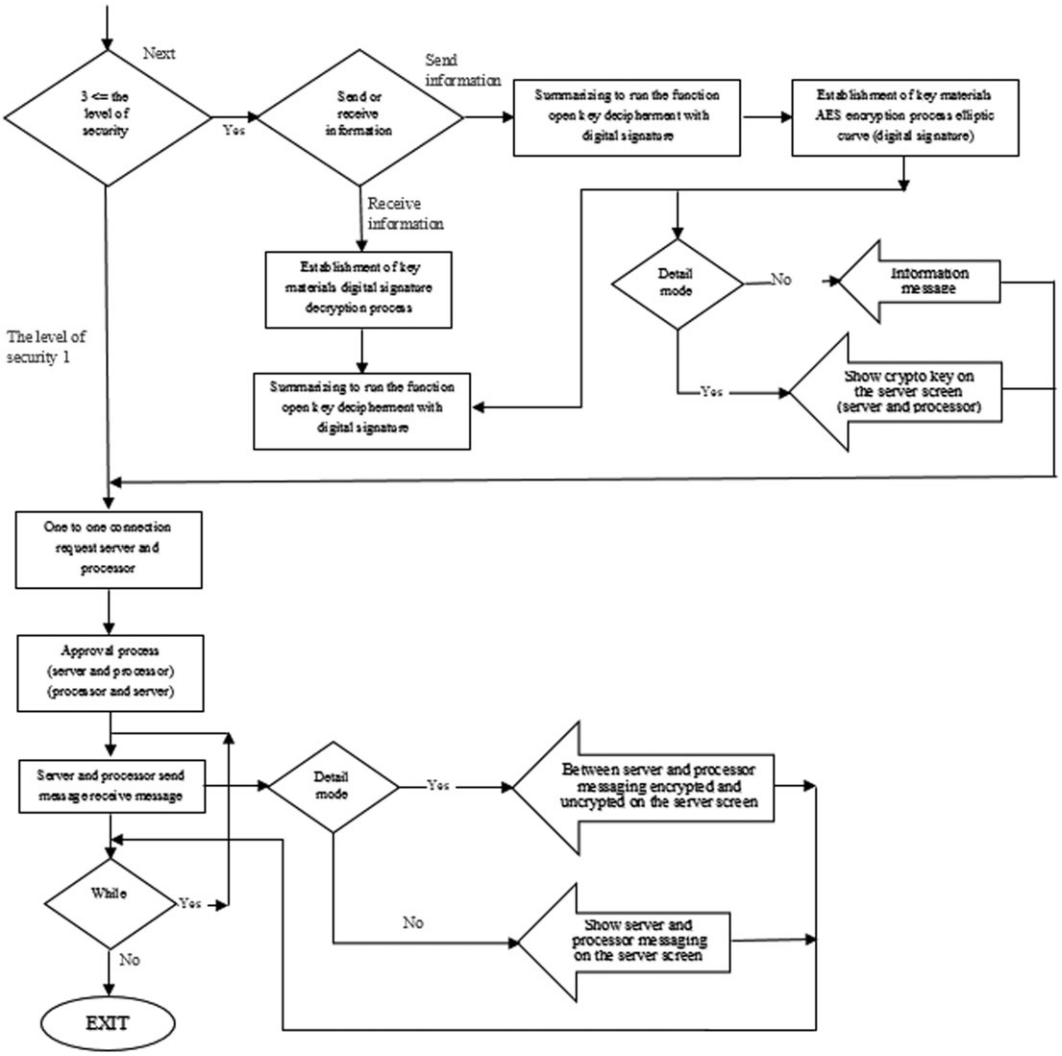

Figure 9. The elliptic curve encryption flow diagram second part.

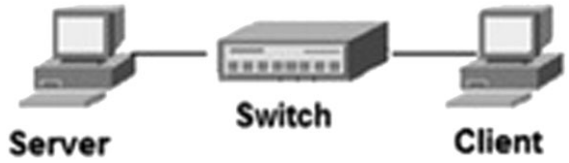

Figure 10. Server and client connectivity.

key generation, public key creation, sending and receiving the keys, encryption and decryption operations are realized. These processes use the elliptic curve coding algorithm for 256,384 and 521 bit while they are getting connected. In addition, the length of the hash function is described, according to the length of the keys. Figure 12 shows the server level of security in the opening screen; elliptic algorithms are part of the length and detail mode. Between the security levels, security without creating a server and client connectivity is established.

5.2. Key creation

First, the option of cryptic messaging screen of the server computer is chosen from the Console. Then, the key bit

Figure 11. Server main screen and client connection pre-screen display.

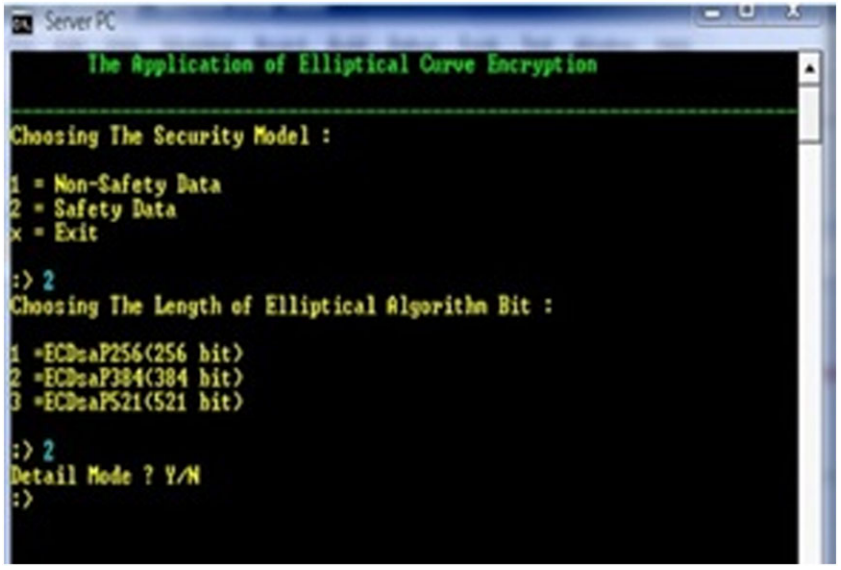

Figure 12. Server main screen menus.

DOI: 10.1002/sec

length is selected from the menu. After you specify the length of the key, the key is generated using Microsoft Visual Studio2008 in the CngKey class. The following command line will produce the object identified with the key. CngKey creates a class method that takes three parameters. X parameter is the length of the algorithm entered via the screen. KeyCreateParms according to the standards is added to the properties of the key to create. The obtained key is assigned on dsKeyBlob object in byte structure. Figure 13 shows the version 4 of the security at the console screen B. A digital signature is sent to the console screen display seen over a private channel. The console of the B is from the console screen A. Digital signature is taken over a private channel.

5.3. Public and private key creation

Elliptic curve encryption asymmetric encryption method and public and private key generation is an important step. Random generated public keys are exchanged between server and client computers. Public key exchange between them is provided for security level 2. Public and private

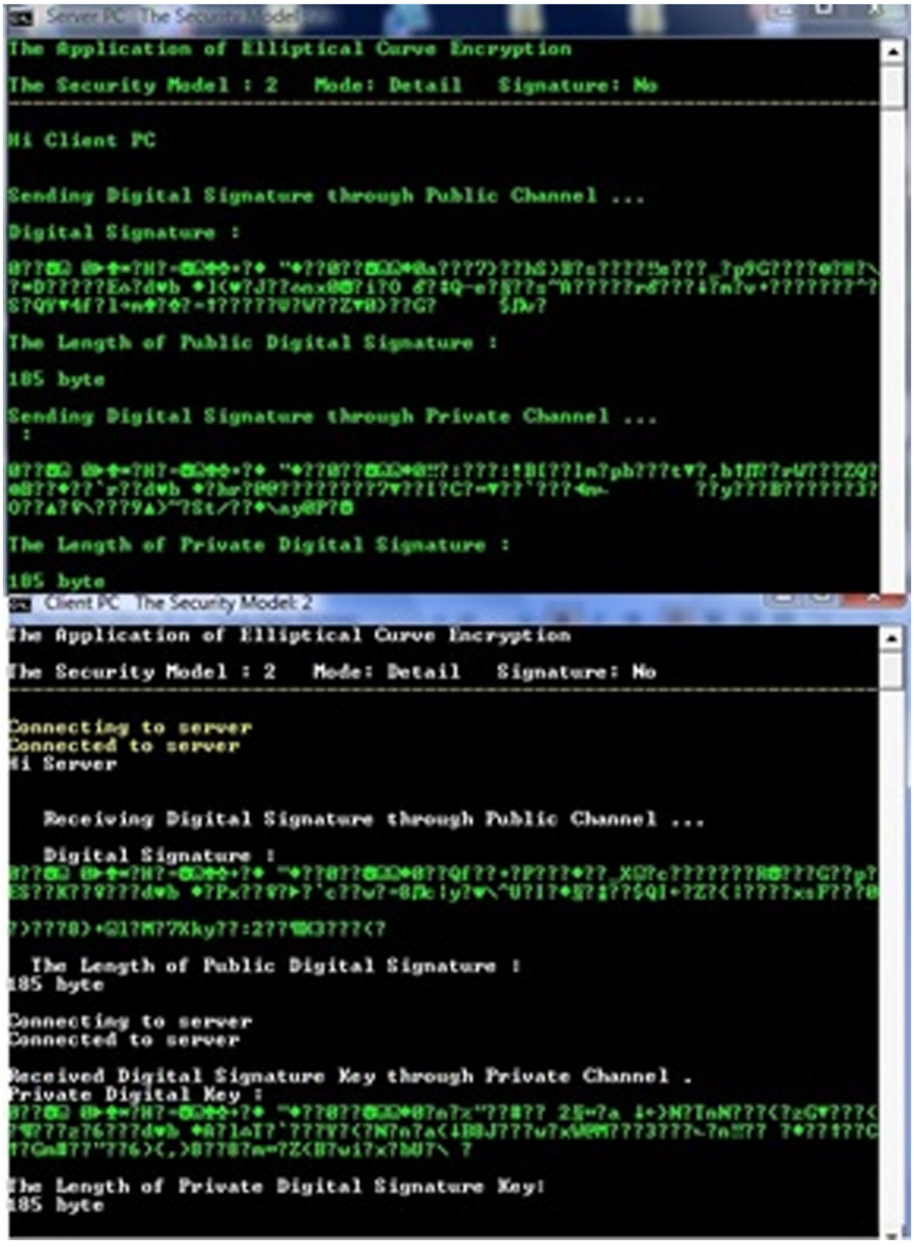

Figure 13. Submitting digital signature screen from the custom channels and the console of the B from the console screen A, digital signature is taken over a private channel.

keys are created randomly by ECDiffieHellmanCng class. From the main menu, key bit length is selected as a parameter. This parameter is determined by the length of public and private key bits. Public key has been translated into XML format. Figure 14 shows that the public key is in xml format both for server and client model. Exchange of public keys between server and client computers is the first step for encrypted messaging.

5.4. Key exchange and channel creation

Communication is a safe way to accomplish the second step to exchange public keys with private channels between server and client computers. In order to create a private channel, the server computer sends the digital signature to the client computer. The server computer sends the digital signature to the client computer by using a private channel and a private port. This point is the most important point in terms of security.

Before exchanging of public keys between server and client computers, the security of digital signature must be provided. This can only be achieved by authorizing certification. It guarantees the security of public keys for server and client computers. The private channel in application is used like authorizing certification, because it is only known by server and client computers. When elliptic curve

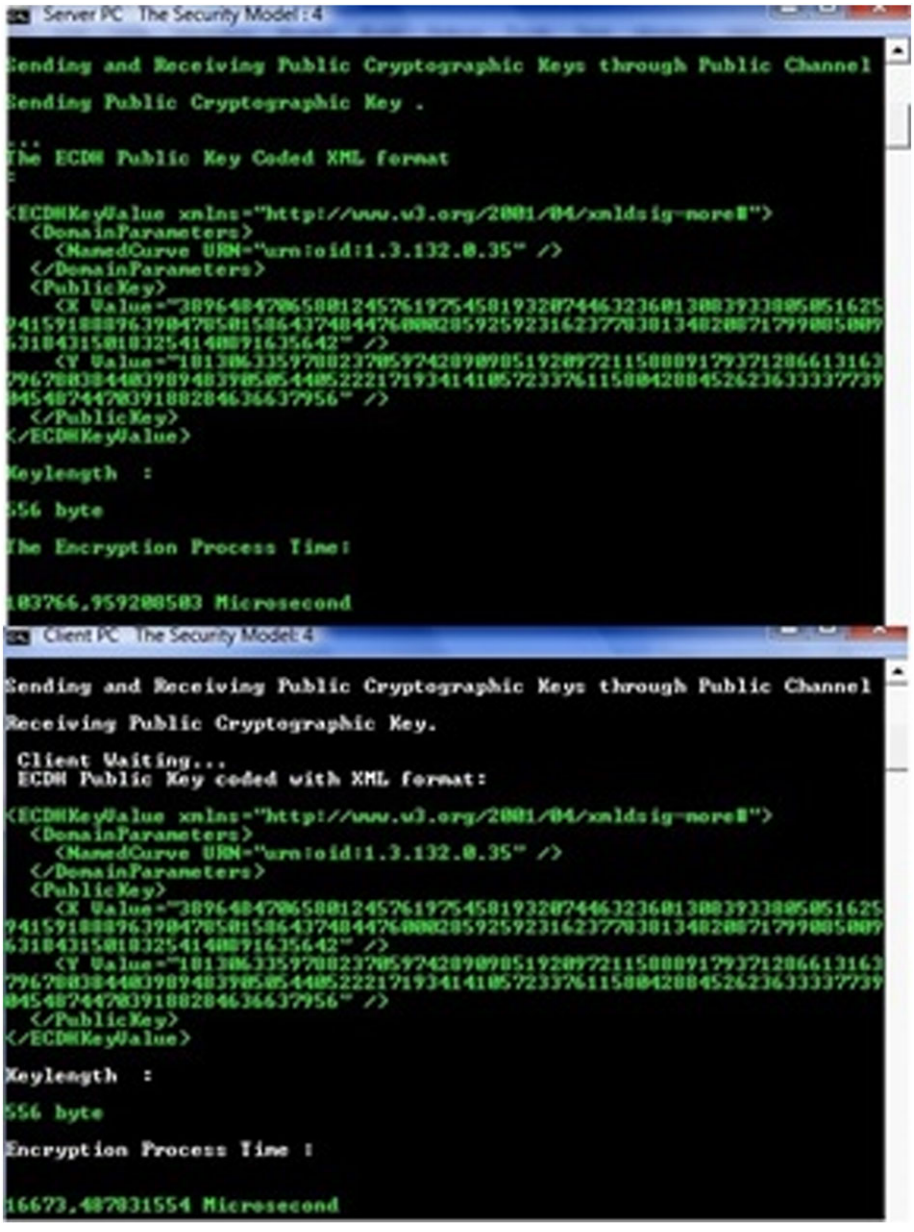

Figure 14. A contact for the public key to send B's blog and considered from key on A Switch B's Blog.

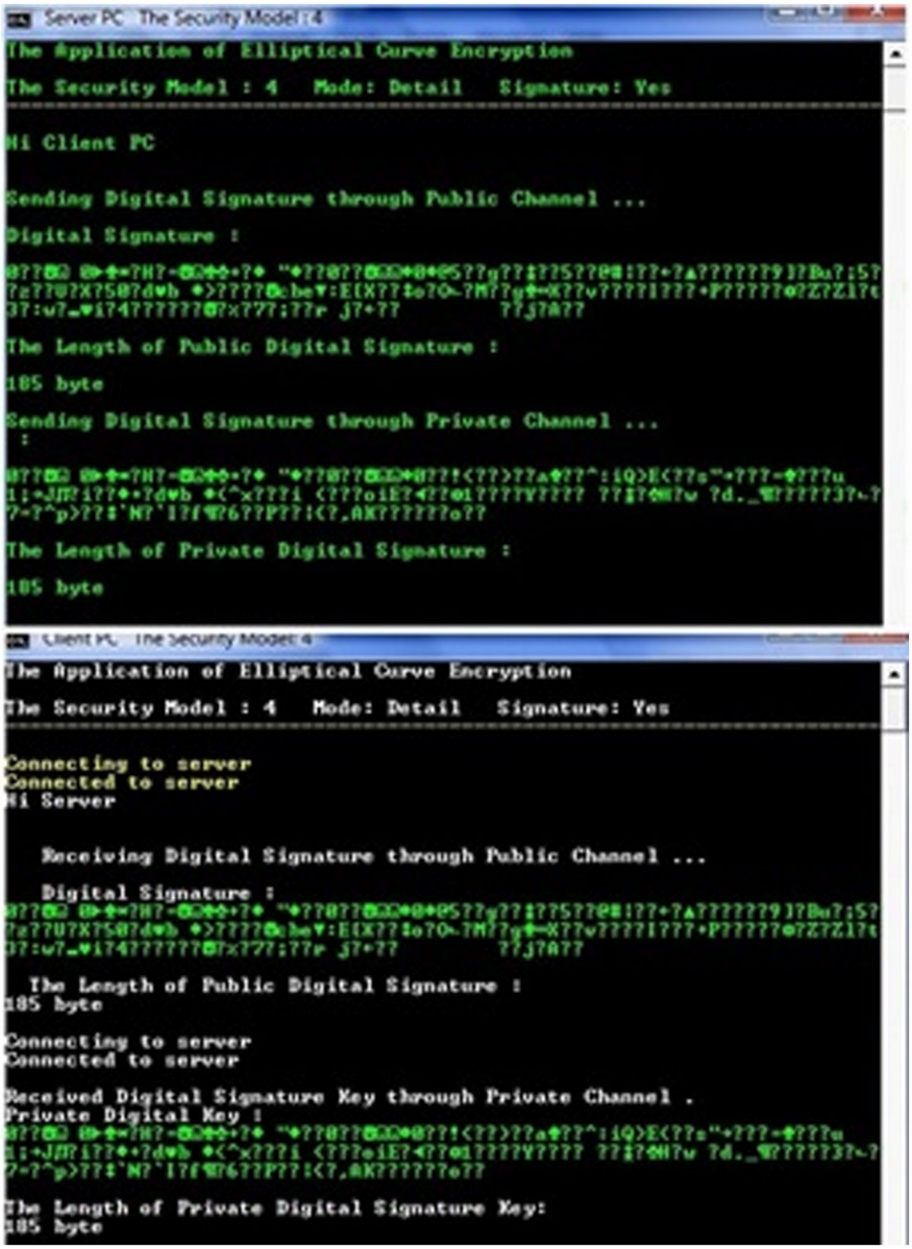

Figure 15. Digital signature which is sent over a private channel and getting over a private channel.

encryption techniques are used for communication between server and client computers, the exchange of public keys is realized in the security level 2 of the application. The digital signature which is sent and obtained from private channel is shown in Figure 15.

6. CONCLUSION

Elliptic curve encryption techniques which are one of the asymmetric encryption techniques were used for the secured communication between server and client computers over a local network. With the help of this technique, the processes of encryption or decryption are extremely fast and secure for the communication on a network. In this application, besides the importance of elliptical curve encryption technique, the importance of the certification authorization (CA) was emphasized for the security of public keys of elliptical curve encryption technique. It guarantees their reliability and prevents being intercepted by a third party. The application can be used for e-government, banking and trade.

Elliptic curve encryption techniques have better security level than the mathematical model for irregular topologies which is mathematical performance model for wormhole-switched irregular networks [22]. The advanced

version of the application of elliptic curve cryptography for bank can be performed as a remote connection through internet in a secure way.

REFERENCES

1. Andreeva E, Mennink B, Preneel B. Open problems in hash function security. *Designs, Codes and Cryptography* 2015; **77**(2–3):611–631.
2. Cramer R, Damgård IB, Döttling N, Fehr S, Spini G. Linear secret sharing schemes from error correcting codes and universal hash functions. in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*.2015.
3. Elmadani AB. Digital signature forming and keys protection based on person's characteristics. in *2012 International Conference on Information Technology and e-Services* (*ICITeS*).2012.
4. Hansche S. *Official (ISC)2 Guide to the CISSP-ISSEP CBK*. CRC Press, Auerbach Publications: Boca Raton, FL, 2006.
5. Katz J, Lucks S, Thiruvengadam A. Hash functions from defective ideal ciphers. in *Cryptographers' Track at the RSA Conference*.2015.
6. Qi C, Cui S, Hao L. A new threshold signature scheme based on ECC and factoring. in *2009 ISECS International Colloquium on Computing*, *Communication*, *Control*, *and Management*.2009.
7. Saini S, Ahmad F. Java model of DSA (digital signature algorithm). *IETE Technical Review* 2002; **19** (4):189–194.
8. Softpanorama. Available from:http://www.softpanorama.org/Algorithms/Crypto/public_key_cryptography.shtml [Accessed on 15 November 2015].
9. Sun X, Xia M. An improved proxy signature scheme based on elliptic curve cryptography. in *International Conference on Computer and Communications Security*.2009.
10. Vacca JR. *Public Key Infrastructure: Building Trusted Applications and Web Services*. CRC Press, Auerbach Publications: Boca Raton, FL, 2004.
11. Association, A.B. Available from:http://www.americanbar.org/groups/science_technology/digital_signatures.html [Accessed on 10 November 2015].
12. Cetin O. Elliptic curve cryptography. *Gazi University*. Master Thesis. 2006
13. Menezes AJ, Van Oorschot PC, Vanstone SA. *Handbook of Applied Cryptography*. CRC press, Auerbach Publications: Boca Raton, FL, 1996.
14. Koblitz N. Elliptic curve cryptosystems. *Mathematics of Computation* 1987; **48**(177):203–209.
15. Akben SB, Subasi A. Comparison of the RSA and elliptic curve algorithms performances. *KSÜ Science and Engineering Journal* 2005; **8**(1):35–40.
16. Sayegh AA, El-Hadidi MT. A modified secure remote password (SRP) protocol for key initialization and exchange in bluetooth systems. in *First International Conference on Security and Privacy for Emerging Areas in Communications Networks* (*SECURECOMM'05*).2005.
17. Microsoft. Available from:http://msdn.microsoft.com/en-us/library/cc488018.aspx [Accessed on 19 October 2009].
18. Zhang X, Ma S, Han D, Shi W. Implementation of elliptic curve Diffie–Hellman key agreement scheme on IRIS nodes. in *Intelligent Computing and Internet of Things* (*ICIT*), *2014 International Conference on*.2015.
19. Masoumi M, Rezayati MH. Novel approach to protect advanced encryption standard algorithm implementation against differential electromagnetic and power analysis. *IEEE Transactions on Information Forensics and Security* 2015; **10**(2):256–265.
20. Ablayev F, Vasiliev A. Cryptographic quantum hashing. *Laser Physics Letters* 2013; **11**(2):025202.
21. Rogaway P, Shrimpton T. Cryptographic hash-function basics: definitions, implications, and separations for preimage resistance, second-preimage resistance, and collision resistance. in *International Workshop on Fast Software Encryption*.2004.
22. Moraveji R, Moinzadeh P, Sarbazi-Azad H. A general mathematical performance model for wormhole-switched irregular networks. *Cluster Computing* 2009; **12**(3):285–297.