International Journal of Scientific Research in Science, Engineering and Technology
Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)
doi : https://doi.org/10.32628/IJSRSET

A Client Server Crypto System Based on Elliptic Curve Cryptography and Mapping Technique

Prof. Prachi Parwar, Anjana Singh
Takshshila Institute of Engineering and Technology, Jabalpur, Madhya Pradesh, India

Article Info
Volume 8 Issue 1
Page Number: 170-175

Publication Issue :
January-February-2021

Article History
Accepted : 01 Feb 2021
Published : 10 Feb 2021

ABSTRACT

The efficiency and effectiveness of the information systems, in many ways, depend on its architecture and how data are transmitted among different parties. Similarly, a very crucial aspect in the software development is the security of data that flows through open communication channels.
One of the most popular architecture is client/server architecture that makes the centralization of data storage and processing enable, and provides flexibility for applying authentication methods and encryption algorithms within information systems. While the number of clients increase, its require increasing the authentication and encryption level as high as possible. Client/server is a technology that allows to open an interactive session between the user's browser and the server. In this study, we used client/server architecture to accomplish secure messaging/chat between clients without the server being able to decrypt the message by applying two layer security: one layer of encryption between the clients and the server, and the second layer of encryption between the clients in the chat room. In this manner, a Client / Server Crypto system Based on elliptic curve cryptography and mapping technique a Secure Messaging System is proposed .Elliptic curve cryptography is a widely used public-key cryptography and authentication system for data encryption of digital messaging transactions such as email over the intranet, extranet and Internet, to encode and decode messages in a terminal window is developed.

Elliptic Curve Cryptography (ECC) is a public-key crypto system which can be used for message encryption, key agreement protocols and digital signature applications. ECC offers high level of security with smaller key sizes makes it ideal for applications which run on small devices that have power and memory constraints such as smart cards and cell phones. Encoding (converting a plaintext message to a point) and Decoding (converting a point to a plaintext message) are important functions in encryption and decryption schemes using ECC before transmission over public networks and unsecured channels. In this paper, we proposed a text message encoding scheme which is based on computational operations on points that lie on a predefined elliptic curve (EC). For any ECC-based encryption scheme, the mapping methodology of a plaintext message onto a coordinate on an affine curve is a mandatory prerequisite. ASCII character codes are considered for the mapping method to convert a plaintext message into coordinates of the predefined EC-points. Discussing the mapping methodology, creating the mapping table and the converting process are given in detail along with their implementations.

Keywords : ECC, EC, Cryptosystem, Python, Cryptography, Keys.

I. INTRODUCTION

In today's world, computer networking has become a n integral part of life. There are many different netwo rks available to share information between groups of devices through a shared communication medium. Th ey are mainly differentiated by the physical medium a nd protocol standards. Ethernet is a prime wired netw orking standard which is an obvious choice for many network applications due to reliability, efficiency, and speed. Ethernet standard is used in various applicatio n segments. Figure 1 shows the Client/Server model a rchitecture that has been used in most network syste ms and in this study specially. The client side could be any type of smart devices (desktop, laptop, smart pho ne, etc.). The server part is one device that control an d pass messages and opining the connections among cl ients and/or between clients and server. The Internet part could be one device to isolate the network overal l into two main parts: client(s) and server, it could be a switch or hub or router or just a cable. A very impor tant aspect in the world of software development is th e security of data that flows through open communica tion channels. In our web applications, there is an int ensive exchange of data via different protocols, like ht tp, between client applications which presented as br owser, mobile and desktop applications and server sid e applications. The importance and confidentiality of data may be different depending on the specifics of th e web application, and the possibility of interception by a third party increases with perfection of hacking t echniques in the world of IT. What can be done to pr event access to the data by your traffic listener? If we exchange with data between the client applications an d server we don't want the information to be stored as open text on the server, which will be accessible in c ase of server crack . Every day people used chat area, t hrough the users (clients) scan chat or send messages t o selected users. However, the security components in chat area application are to make sure all information from clients is protected from hackers. The chat mess ages from users can easily transform by expert hackers, without a good enough security components. In this way, a chat area interface (CAI) is required technique to secure a chat message from hackers. The cryptogra phy is significant to keep private data secure and to av oid unauthorised access.

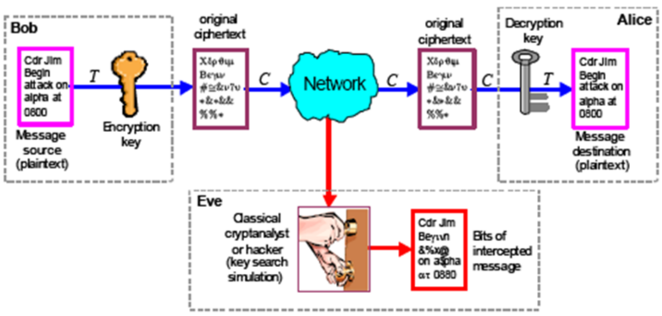

Fig. 1 client server architecture

II. LITRATURE REVIEW

Cryptography is a practical means for protecting priva te and sensitive information.

Elliptic curve cryptography (ECC) is a public-key cry pto system first introduced in 1985 by Miller [1] and Koblitz. Since then, many researchers tried to employ ECC on different data types and improve it's efficienc y by proposing various encryption techniques.

The most attractive advantage that motivated cryptog raphers to use ECC was the well suitability of it in the constrained environments where processing power, s torage, bandwidth or power consumption is of primar y interest. These characteristics of ECC motivated us t o study the potential of using it for encoding the Ame rican Standard Code for Information Interchange (AS CII) character codes for any ECC-based encryption sc heme. The fundamental issue of protecting the confid entiality, integrity as well as authenticity of plaintext messages through various communication entities has become a major concern especially with the increasin g use of digital techniques for transmitting and storing these messages. In most cryptographic systems, we m ust have a method for mapping our plaintext, message into a numerical value upon which we can perform mathematical operations. In order to use elliptic curve s, we need a method for mapping a plaintext message onto a point on an elliptic curve. Elliptic curve crypto systems then use elliptic curve operations (Add, Doub le, Multiply) on that point to yield a new point that w ill serve as the ciphertext. We proposed a secure plain text message encoding scheme using EC-points operat ions. The encoding process of the ASCII character cod e is done and implemented by using the proposed ma pping methodology. The decoding process is accompli shed by using the mapping methodology to obtain the plaintext messages. The simulation analysis demonstr ated that the proposed plaintext message encoding sch eme has large key space and can satisfy the performan ce requirements for the confidentiality of digital mess ages.

ECC Background: ECC is one of the most accomplishe d and widely used, however least understood, cryptog raphy tools. It is the future generation of public key c ryptography. It provides significantly more security t han first-generation public key cryptography systems like RSA. ECC is a technique in public key cryptograp hy set on the algebraic arrangement of elliptic curves over finite fields. Compared to non-ECC cryptograph y, ECC provides equivalent security with smaller keys. The elliptic curve cryptosystem was initially propose d as a basis for public key cryptosystems, and it has pr oven to be an important unit of current cryptography. ECC utilizes the mathematics of elliptic curves. The s ecurity of ECC lies in the complexity of working the e lliptic curve discrete logarithm problem. An analysis of ECC theory and its computational problems are stat ed below.

elliptic curves ($E_q(a, b)$) are a set of points defined by the solutions to the equation $y^2 \equiv x^3 + ax + b \pmod q$, where a and b are elements of the field k together with a point at infinity O [24]. There is also a conditio n such that $4a^3 + 27b^3$ 6= 0 (mod q) where q is a pri me number. This equation must be satisfied for the ell iptic curve to have a well-defined group structure. Th is forms an additive cyclic group $E = \{(x, y) \in E_q(a, b)\} \cup \{O\}$, where O serves as an additive identity element of the group . If P is a point in E and k is a positive in teger, then the point multiplication is computed by re peated addition, such as $k \cdot P = P + P \cdots + P$, where k i s a large integer and P is added to itself k times.

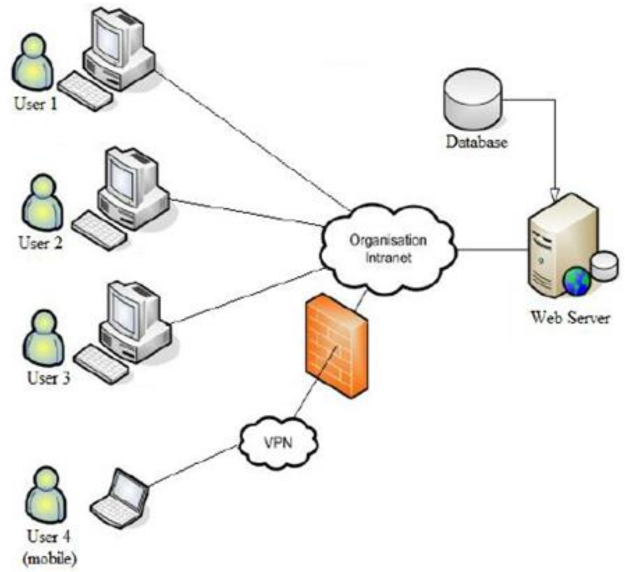

Fig.2 ECC cryptography

Computational Nature of ECC: ECC is a computation ally-intensive operation. Its scalar multiplication is on e-way, making it computationally infeasible to trace t he original number. For example: let P be a point in E, and let Q be a point such that Q = kP. The elliptic cur ve discrete log problem is the following: knowing the values of P and Q, determine the value of k. If the mo dulus q is large, the ECDLP (For elliptic-curve-based protocols, it is assumed that finding the discrete logari thm of a random elliptic curve element with respect t o a publicly known base point is infeasible: this is the “elliptic curve discrete logarithm problem" (ECDLP).) is computationally infeasible. ECC is based on this pro blem. Even if P and Q are known, determining k such that Q = kP (kP and k · P have the same meaning in E CC multiplication) is computationally infeasible. Hen ce, the elliptic curve discrete log problem makes k diff icult to compute.

Elliptic Curve over Finite Prime Field: Let E be an elli ptic curve over Fp, p > 3, given by an affine Weierstra ss equation of the form : E : y 2 = x 3 +ax+b
Where a and b are coefficients belonging to Fp such t hat 4a 3 + 27b 2 6= 0 (this last condition ensures that E has no singular point over Fp). The set E(Fp) of Fp-r ational points is simply defined as E(Fp) = {O} ∪ {P = (x,y);x,y ∈ Fp;y 2 = x 3 +ax+b}, (2) where O represents the point at infinity. Such an elliptic curve E admits a n addition law. Equipped with this addition law, E(Fp) becomes a finite abelian group, where O is the neutra l element. To encrypt a message, Alice and Bob pick a n elliptic curve E and select an affine point G ∈ E(Fp). Plaintext m is encoded into a point Pm. Alice choose a random prime integer x and Bob choose a random p rime integer y. Alice and Bob’s private keys are x and y respectively. To generate the public key, Alice comp utes PA = [x]G and Bob computes PB = [y]G. To encry pt a message point Pm for Bob, Alice chooses another random integer k and computes the encrypted messag e PC using Bob’s public key PB. Then, PC is a pair of points given by the following equation: PC = [([k]G), (Pm + [k]PB)]. (3) Alice sends the encrypted message PC to Bob. Bob receives the ciphered message and mu ltiplying his private key, y, with [k]G and subtract it f rom the second point in the encrypted message to co mpute Pm. The result is the plaintext message m indic ated by the following equation: Pm = [(Pm + [k]PB)– ([yk]G)].

Points addition and points doubling are the basic EC o perations . Assume that P1 = (x1,y1) and P2 = (x2,y2) are two points of E, then their sum which is P3 = (x3, y3) can be obtained as follows: P3 = P1 +P2 = (O if P1 = –P2 (x3,y3) if P1 6= –P2 (5) where (in the latter cas e) (x3 = λ 2 –x1 –x2 y3 = (x1 –x3)λ –y1 (6) with λ = (y 2–y1 x2–x1 if x1 6= x2 3x 2 1+a 2y1 if x1 = x2 and y1 6 = 0 (7) It turns out that point P3 belongs to the curve E, and even is an element of E(Fp) if both P1 and P2 a re. Recall that the computations of the algebraic quan tities above are done (mod p) at each step in practice. Using this addition law, one can compute, like in any abelian group, any multiple [k]G for any G ∈ E(Fp).T herefore, multiplication on EC requires a scalar multi plication operation [k]G, defined for a point G = (x,y) on EC and a positive integer k as k times addition of G to itself. This scalar multiplication can be done by a s eries of addition and doubling operations of G. The str ength of an ECC-based cryptosystem depends on the difficulty of finding the number k of times G is added to itself to get [k]G (PA). This reverse operation is kno wn as the Elliptic Curve Discrete Logarithm Problem (ECDLP) and is considered the core hardness of ECC.

III. PROPOSED SYSTEM

Basically, the proposed messaging/chat system is expe cted to provide a communication channel between cli ents via a server using encryption based on ECC in a Client/Server environment. The goal for this study is t o use client/server architecture to accomplish secure c hat between clients without the server being able to d ecrypt the message by using one layer of encryption b etween the clients and the server, and then a second l ayer of encryption between the clients in a chat room. All the used encryption processes based on ECC algor ithm. The implementation of this study is held in Pyt hon Google Colab environment.

The very term client-server was initially applied to th e software architecture, which described the distribut ion of the execution process by the principle of interaction of two software processes, one of which in this model was called the client and the other the server. The client process requested some services, and the server process ensured their execution. It was assumed that one server process can serve a lot of client processes. One of the client/server application is that “chatting”.

Chatting alludes to one kind of correspondence over the Internet that offers a continuous transmission of instant messages from sender to beneficiary or over a server that is control and deal with the gatherings (customers) to convey.

A. Client/Server

The used client/server model describes how a server provides resources and services to one or more clients. Examples of servers including web servers, chat servers, and file servers. Each of these servers provides resources to client devices. Most servers have a one-to-many relationship with clients, meaning a single server can provide resources to m Computers. In order to meet the main requirements of businesses, networks themselves are becoming quite complex multiple clients at one time. B. Chat Service A secure chat service provides the ability to have real time secure discussions among users electronically, one-to-one or in groups session . A public network accumulates information slightly, rather than on a user’s individual computer that is used to keep in touch with people. A secure chatting between client and server to make a safe and reliable communication, the benefits are: · Allows for instant communications between users. · Uses real time chat over the network that can eliminate costly long distance charges. · Allows for rapid query and rapid responses. While the negative points of chat service can be listed as following: · Security problems of instant messaging program · Secure chats in most cases are routed through a server system, where the service is provided and that is a single point where all messages can be intercepted. Chat programs can provide an open avenue of attack for hackers, crackers, spies and thieves.

B. Chat Service

A secure chat service provides the ability to have real time secure discussions among users electronically, one-to-one origin groups session. A public network accumulates information slightly, rather than on a user’s individual computer that is used to keep in touch with people. A secure chatting between client and server to make a safe and reliable communication, the benefits are:

- Allows for instant communications between users
- Uses real time chat over the network that can eliminate costly long distance charges.
- Allows for rapid query and rapid responses.

While the negative points of chat service can be listed as following:

- Security problems of instant messaging program
- Secure chats in most cases are routed through a server system, where the service is provided and that is a single point where all messages can be intercepted.
- Chat programs can provide an open avenue of attack for hackers, crackers, spies and thieves.

Encryption algorithm is deployed to encrypt messages exchanged with the proposed chat gateway. This study is about developing a new model to create private messaging network to transmit message contents over the network / intranet between client terminals. The chat messaging environment showed a great potential to host realtime interactive interaction system which is supported by ECC encryption methodology to preserve the security of the message stream. Choosing the key size in ECC encryption is of great importance. As the size of the key increases, the security level of the system, the complexity and the resistance of encrypted text increases. These advantages make it difficult to decrypt ciphertexts and break passwords. However, in addition to these advantages, the encryption key creation time, text encryption time, and mobile device RAM consumption increase. These disadvantages are factors that will influence the effective use of the application. For this reason, the advantages and disadvantages of key dimensions should be determined and the most suitable key size should be preferred. To accomplish the chatting and meet the goals of this study in client/server architecture, the need for authentication methods and encryption algorithms will be urgent RSA Algorithm for cryptography consists of three main stages: Key Generation Stage, Encryption Stage and Decryption Stage. Key Generation Stage is the process of generating keys for cryptography. Keys, generated in this stage, are used to encrypt the plaintext in Encryption Stage and used to decrypt the cipher-text in Decryption Stage. Encryption Stage is the process of encoding messages in such a way that only authorized people can understand it . By encryption, the message is converted into cipher-text. Decryption Stage is the process of decoding the cipher-text to get the original message. These three stages are followed both of the layers (first and second encryption layers). The flowchart of the secure chat system is presented.

Here, we used one authentication level and two encryption levels. We used ECC algorithm to encrypt messages between clients and the server as the first encryption level and then encrypt messages between clients and chat room. By means of this model, secure messaging in corporation environments might be provided with the help of a two level authentication scheme.

Text Message Encoding Scheme: The problem of encoding plaintext messages as points on an EC is not as simple as it was in the conventional case. In particular, there is no known polynomial time, deterministic algorithm for writing down points on an arbitrary elliptic curve E (mod p). However, there are fast probabilistic methods for finding points, and these can be used for encoding messages. The proposed encoding scheme uses a mapping table to encode plaintext message characters to an elliptic curve points. The aim of the method is to provide an additional level of security in the elliptic curve encryption schemes by making use of the hardness nature of the ECDLP. The characters in the plaintext message m are first represented as numbers k and these numbers are then encoded to different points on the curve using the mapping table. These points can be converted to cipher points by using the EC point operations. The letter frequencies in the plaintext are not preserved in the ciphertext and thus the crypt analysis based on letter frequency can be defeated. This method is more suitable for encrypting short messages such as Short Message Service (SMS) and Multimedia Messaging Service (MMS) which are used in mobile phones for non-voice communications.

The Mapping Methodology :To encode a plaintext message m that consists of a number of characters and each character is represented by ASCII character code, which used a 7-bit character code of between 0 and 127 according to the standard ASCII table, we need to encode k = 128 numbers. In this case, each character should be considered as a text message and mapped to a point on a predefined EC. The mapping method proposed in this section is based on a map table. To create this table, an elliptic curve E with at least 128 points, which is all possible points on the finite field, is generated first. Then, we find point G of order ℓ equal at least 129 and as close to 129 as possible on E. The order of point G is $\ell = k + 1$, that is we have different points $\{G,[2]G,[3]G,\ldots,[k]G\}$ (9) with $[\ell]G = O$ is infinity point and k is integer. The row indexes start from 0 and end with 127 where each row stands for a character code value as listed in Table 1.

ASCII Code Implementation: In our experiment, in order to define the implementation process clearly, we used the following EC equation: $E : y^2 = x^3 + 4x + 1$ (10) over F503, where the order of E is N = #E(Fp) = 516. We also select generator point G = (283,315) of order $\ell = 129$ for our mapping method. Starting from the first character in the plaintext message, the corresponding point with the intensity value in the table is mapped to this character and continues to the last character.

So, we encode plaintext message characters as points of E assigning all character codes to all points as the fo llowing: 0 =⇒ G,1 =⇒ [2]G,2 =⇒ [3]G, ··· ,127 =⇒ [128] G. (11) In Table 1 are presented results of the mappin g method for ASCII character codes. The first column represent ASCII character values as {m = 0,...,127} and the second column shows ASCII corresponding symb ols. The third column shows how ASCII values are ma pped according to [k]G with {k = 1,...,128}. In the four th column, the EC mapped points are resulted for all ASCII character values with successful iteration of k.

IV. CONCLUSION

Demonstrating of appropriate client/server applicatio ns is a basic figure for planning, sending, and later ada ptability. The demonstrating advances required in this exertion are not for the most part accessible, and not prepared for wide dispersion to application originator s and organisers. This system highlights the usefulness requirements for client/server models and depicts co nfiguration inquiries to be tended to. We developed a client/server encrypted chat based on ECC by using P ython Google Colab software encryption polices. The result will give one authentication level and two encr yption levels by secure chat data based on ECC algorit hm. We have implemented the system in client/serve r architecture and in real-time network. We believe t hat the system provides high level in encryption and more flexibility in implementation. However, as a fut ure work other encryption algorithm might be used a nd a hybrid algorithm can be developed for further pu rposes such as faster or wider messaging needs.

V. REFERENCES

[1]. Bibinagar, N., Kim, W. J. (2013). Switched Ethernet based real-time networked control system with multiple client–server architecture. IEEE/ASME transactions on Mechatronics, 18(1), pp.104-112.

[2]. Honda, K., Hu, R., Neykova, R., Chen, T. C.,Demangeon, R., Deniélou, P. M., Yoshida, N. (2014). Structuring communication with session types. In Concurrent Objects and Beyond, pp. 105-127, Springer BerlinHeidelberg.

[3]. Lin, T., Zhou, K., Wang, S. (2013). Cloudlet–screen computing: a client–server architecture with top graphics performance. International Journal of Ad Hoc and Ubiquitous Computing, 13(2) , pp.96-108.

[4]. Iwamoto, M., Omino, T., Komano, Y., Ohta, K. A new model of Client-Server Communications under information theoretic security. In Information Theory Workshop (ITW), pp. 511-515, 2014.

Cite this article as :

Prof. Prachi Parwar, Anjana Singh, "A Client Server Crypto System Based on Elliptic Curve Cryptography and Mapping Technique", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 8 Issue 1, pp. 170-175, January-February 2021.
Journal URL : https://ijsrset.com/IJSRSET218134