SHORT COMMUNICATION

APPLICATION OF ELLIPTIC CURVE CRYPTOGRAPHY ON DATA ENCRYPTION OVER A NETWORK

*BIBU, G. D. & ANGAI, S.

Department of Mathematics
University of Jos, Nigeria
*(Corresponding author)
gidadik@yahoo.com

Network security refers to all hardware and software functions, characteristics, features, operational procedures, accountability measures, access controls, and administrative and management policy required to provide an acceptable level of protection for hardware, software, and information in a network (Shaffer *et al.,* 1994). The need to ensure data security on University campuses all over Nigeria is necessary as very important documents and sensitive information are transmitted from one point to another, like examination questions, students' results, very important circulars, and even financial transactions of the university. Most networks today, especially in Nigeria and particularly in the University of Jos, do not have a comprehensive way of securely transmitting data over their networks. The most common means of providing data security over these networks is the use of passwords, which over time has proven to be quite unreliable as they can easily be breached. Encryption algorithms applied on these networks are based on symmetric or private key cryptography which do not provide a high level of security. So the need to provide a highly efficient method of securely transmitting data over a network cannot be over emphasized.

Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. The use of elliptic curves in cryptography was suggested independently by Neal Koblitz and Victor Miller in 1985. Their security is based on the hardness of the elliptic curve discrete logarithm problem (ECDLP) (Hankerson *et al.,* 2004). Elliptic curve cryptography is an effective tool for ensuring data security that could be applied to a network to enhance secure data transfer over the network. This is due to the fact that elliptic curve cryptography provides security based on the hardness of the elliptic curve discrete logarithm problem. Also, elliptic curve encryption has a high implementation rate, and it does not require a lot of bandwidth like other public cryptosystem. It is also very robust making it a viable encryption tool to be used on networks that desire to achieve maximum security (Robshaw & Yin 1997).

In this work, elliptic curve cryptography was used to provide a much shorter key length, with the same level of security as other public key cryptosystems such as Rivest-Shamir-Adleman (RSA). Thus it is an ideal method for securely transmitting data over a network to achieve the following:

- Provide high confidentiality by ensuring that messages sent from a source to a destination would not be readable by a third party.
- Detect any modifications that might have been made on the data during transmission over the network.

The destination should be able to authenticate the origin of the data, and verify indeed that the data originated from the claimed source.

The destination should be convinced of the identity of the other communicating entities. When the destination receives a message from the source, not only is the destination convinced that the message originated from the source, but the destination can convince a neutral third party of this; thus the source cannot deny having sent the message to the destination.

THE PROPOSED SYSTEM

The proposed network security system is graphically described by the following data flow diagram:

The cryptosystem distributes public and private keys to each user, these keys are used by the user to encrypt and decrypt plain texts and files. The server generates addition points using an elliptic curve over a specified field. The public key (encryption key) is usually a point on the elliptic curve while the private key (decryption key) is us used to decrypt data in elliptic curve cryptography. The private and public keys used by each user at any instance are stored in the database to avoid public and private key conflicts.

OPERATION OF THE PROPOSED SYSTEM

Elliptic Curve Cryptography schemes use an elliptic curve E over a finite field such as Z_p, where p is a very large prime, and involves both encryption and decryption operation. This project uses the ElGamel public-key cryptosystem based on the Discrete Logarithm problem in Z_p, the set of integers $1, 2, ..., {}_p - 1$, under the multiplication modulo ${}_p$

The scheme will be demonstrated using Alice and Bob as sender and receiver of a secret message respectively. The coordinates of the points on the elliptic curve itself serves as a pool of numbers to choose from.

The Encryption Operation

To encrypt plaintext messages M, into cipher text, the plaintext message is encoded into a point P_M from the finite set of points in the elliptic group $E_p(a, b)$.

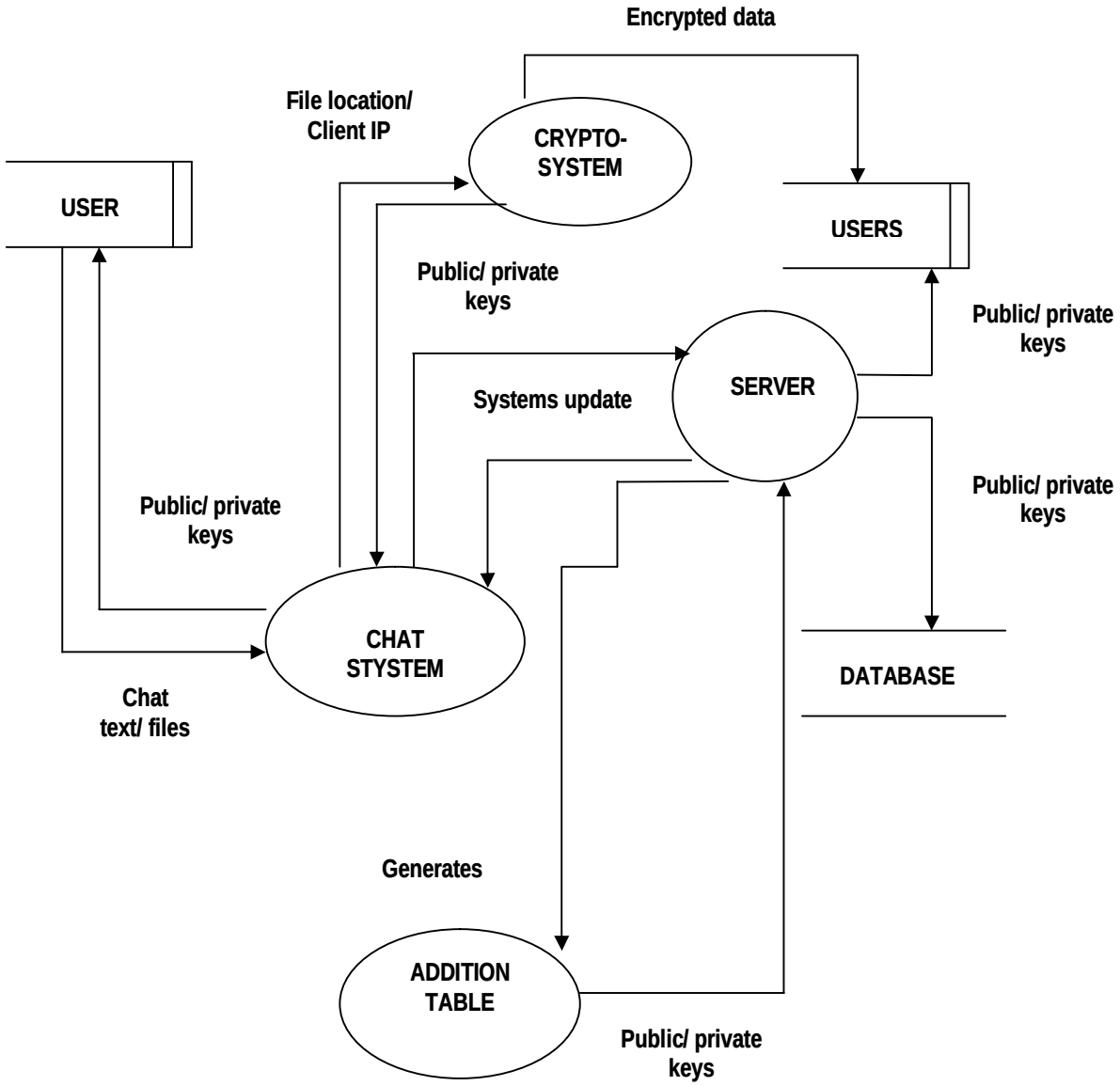

FIG. 1. THE CRYPTOSYSTEM DATA FLOW DIAGRAM

The first step consists of choosing a generator point $G \in Ep(a,b)$ such that the smallest value of n for which $nG = 0$ is a very large prime number. The elliptic group $E_p(a,b)$ and the generator point G are made public.

Each user selects a private key $n_A < n$ and computes the public key P_A as: $P_A = n_A G$. To encrypt the message point P_M for Bob (B), Alice (A) chooses a random integer k and computes the cipher text pair of points P_C using Bob's public key P_B:

$$P_C = \left[(kG), (P_M + kP_B) \right]$$

The Decryption Operation

After receiving the cipher text pair of points, P_C, Bob multiplies the first point, (kG) with his private key n_B, and then adds the result to the second point in the cipher text pair of points, $(P_M + kP_B)$:

$$\left(P_M + kP_B - \left[n_B(kG)\right]\right) = (P_M + kn_B G) - \left[n_B(kG)\right]$$
$$= P_M$$

Which is the plain text corresponding to the plain text message M, only Bob knowing the private key n_B can remove $n_B(kG)$ from

the second point of the cipher text pair of points, that is ($P_M + kP_B$), and hence retrieve the plain text information P_M .

IMPLEMENTATION OF NEW SYSTEM

The system was implemented and tested using a simple chat scenario. The messenger server (Fig. 2) coordinates all users that login to the messenger and most importantly, it generates quadratic residues, which is used to compute an elliptic group, and performs addition and multiplication of points over the elliptic group. These points are used by the cryptosystem which generates the public and privates keys for each logged on user to encrypt (at the source) and decrypt (when it arrives at the destination) data as they travel over the network.

FIG 2. SERVER INTERFACE

Each user is required to provide an E-mail address and a password in order to gain access to the messenger.

After login, the messenger interface pops-up as shown in Fig. 3, this interface enables users to send plain text and files which get encrypted as they are being transmitted over the network.

FIG 3. MESSENGER INTERFACE

Figs. 4 and 5 show two users chatting in real time over a network. This system only permits real time communication. Although each user sees their message in plain texts, the message is actually enciphered at the source as it travels through the network and deciphered at the destination as it is displayed on the two chat interfaces below. This therefore makes it difficult for any third party that may want to listen in on any conversation between users to make any sense out of the messages while on transit between the users.

FIG 4. CHAT

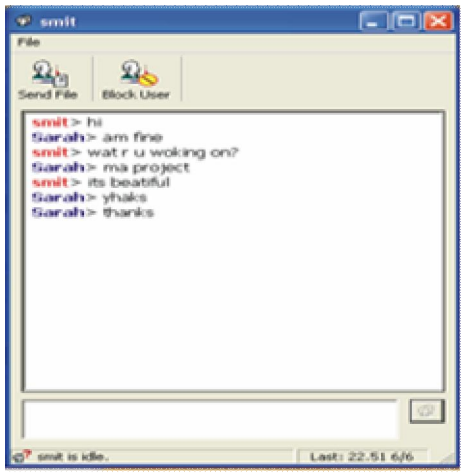

FIG 5. CHAT

The system not only permits transmission of plain texts, but also allows transmission of files over a network. However, the user at the source who wishes to send a file must receive acknowledgement from the user at the destination (the receiver) before the transmission can be affected. The receiver therefore has the choice to accept or reject. These files are also encrypted using elliptic key cryptography as they make their transit across the network. This method of encryption ensures that the source cannot deny that the file(s) originated from it and also ensures that no modifications can be made on the file as it moves through the network. It is imperative to mention that when encrypting data over a network, the cipher texts are not visible or can not be seen with

the human eye, this is because data is encrypted only while in transit, existing as plaintext on the originating and receiving hosts.

CONCLUSION

The climax of the work is the design and implementation of data security over a network through the use of elliptic curve cryptography, which is a very strong tool that can be implored to achieve high level of security over a network.

REFERENCES

Hankerson D., Menezes A., Vanstone S. (2004). *Guide to Elliptic Curve Cryptography*, Springer-Verlag Inc, New York.

Robshaw, M.J.B. & Yin, Y.L. (2008). Overview of elliptic curve crptosystems. Technical reports. RSA Laboratories.

Shaffer, S. L. & Simon A. (1994). *Network security*. Academic press.