Secure Tranmission of Data by Elliptic Curve Cryptography

Nirbhay Sibal
Dept. of Computer Science & Engineering
HMRITM, New Delhi

Tanvi Hasija
Dept. of Computer Science & Engineering
HMRITM, New Delhi

Shally Gupta
Assistant Professor
Dept. of Computer Science &Engineering
HMRITM, New Delhi

***Abstract*—The most important factor of today's businesses is data. Top organizations spend millions of dollars to save their networks and to protect their data. Imagine the situation when all the precious research data on which millions of dollars had been invested by the organization over the years. We are highly dependent today on computers for doing huge money transfers between banks, markets, insurance etc. We cannot take security in this critical area for granted. As the networks and systems complexity are increasing, vulnerabilities have also increased and so network's security is becoming lot more difficult and complex.This makes security of data or precisely security of network, an important factor in today's era. This paper focus on the use of video just like the cover to protect or for data hiding and also insistingon security encryption using steganography with ECC.**

Keywords— Security; steganography; ECC.

I. INTRODUCTION

Data is continuously exchanged over different types of computer networks. It is obviously correct to say that a huge part of the data is private or confidential which demandstronger techniques of encryption. There are two commonly used techniques for securing the data that is transmitted over the network, these are encryption and steganography[2]. Therefore, there are a lot many encryption-decryption systems to encrypt and decrypt the transmitted information. The technique of hiding data in a medium that can be called as a cover or carrier such that the actual existence of the complete message is made hidden or concealed, this method is called as Steganography.Elliptic curve cryptography (ECC) is a technique to public-key cryptography, and it is based on the elliptic curve's algebraic structure over finite fields. ECC do not require large keys rather use keys that are smaller as compared to non-ECCtechnique of cryptography, which are based on plain Galois fields, that provide securityequivalent to ECC. To ensure that the access to information is reliable, ECC offers considerable security, that too with smaller size of keys, with faster computation, and also lower power consumption. Besides all this, there is memory and band width saving .This is especially useful for mobile devices orwireless pagers which are limited in bandwidth,memory and low Power and network connectivity[4].

II. LITERATURE SURVEY

ECC has been used over many years for security purpose. In 2008 Mohammad Ali BaniYounes and AmanJantan[2] talked about hiding the data within the encrypted image data using Least Significant Bits (LSB) insertion. They have even managed to maintain correlation and entropy even after the data hiding. They hid the data in the images by modifying some pixels' color codes so that the image, when reformed, would look identical to the original one. Later, An Liu and Peng Ling of North Carolina State University [7] proposed a configurable library of ECC operations in wireless sensor networks. This package was called TinyECC which provided a number of optimization switches, which could turn specific optimizations on or off depending developers' needs. In 2009, Tarun Narayan Shankar and G. Sahoo[8] described the basic idea of ECC and its implementation through coordinate geometry for data encryption. They reviewed the generation of public key on the elliptic curve and used the same for encryption, and then, further, reviewed the generation of private key and used it for decryption. MrithaRamalingam, [9] in 2011, proposed a machine named as astego machine to develop a steganographic application to hide data that contain the text in a video file and then, further, retrieve the hidden information. This was done in such a way that the video wouldn't lose its functionality. Hence, Least Significant Bit (LSB) modification method was used. When considering the Manet networks, Ertaul L [10] in 2005 proposed a new approach to provide reliable data transmission in MANET, uses combination of ECC and Threshold Cryptosystem and compares the performances of ECC and RSA. Though elliptic curves have known many years ago and V.S. Miller in 1986 [11] have used the concept of elliptic curves for cryptosystems but still due to many formulas n calculations it came out to be only 20% faster than the Diffie-Hellmann. But in 2005, K Lauter [12] in his paper proposed the use of elliptic curves in cryptography, as the wireless industry is growing tremendously in every field so there was a need to have a public key infrastructure.

ECC has been around since mid-1980s, but it has not been implemented extensively.It is a system in which we have a public key with which we encrypt data and a private key with

which we decrypt data.[3]. When we talk about it, we talk about the notion of a Trapdoor function. This is the math function that underpins the public key crypto-system [6].
We can use a value, let's call it 'A' and use the trapdoor function to get to another value, let's call it 'B'. It could be done very easily. But if we try to go the other direction i.e. going from B to A, it is very difficult. This difficulty is the only thing that makes the implementation of such things useful.
Currently, RSA algorithm is widely used, which is essentially the base for ECC. RSA is based on prime number factorisation. In RSA, we take two random prime numbers and we multiply those to get a large prime number, which is the process A to B. Then, we have to factor those out, which is the other way, B to A, which is very difficult.
The keys are the base of these algorithms. Here is a little study about the keys in both RSA & ECC:

ECC Vs. RSA

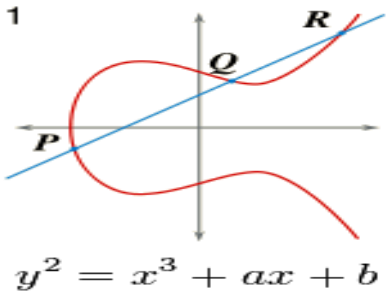
ECC	RSA
256 bits	3072 bits
384 bits	7680 bits

The table reflects that a key of size 256 bits in ECC provides a same level of security as a key of size 3072 bits in RSA [13] [14] [15].
In fact, 384 bits of ECC is strong enough to hold America's top secret level information.
Elliptical equation used:

$$y^2 = x^3 + ax + b$$

The curve is symmetric about the x-axis. It works on a principle that if we draw astraight line through the curve, it will intersect the curve in no more than three points.
Let's name these three points are 'P', 'Q' and 'R'. The 'dot' function is basically used in mathematical calculations, as:

P dot Q -> R

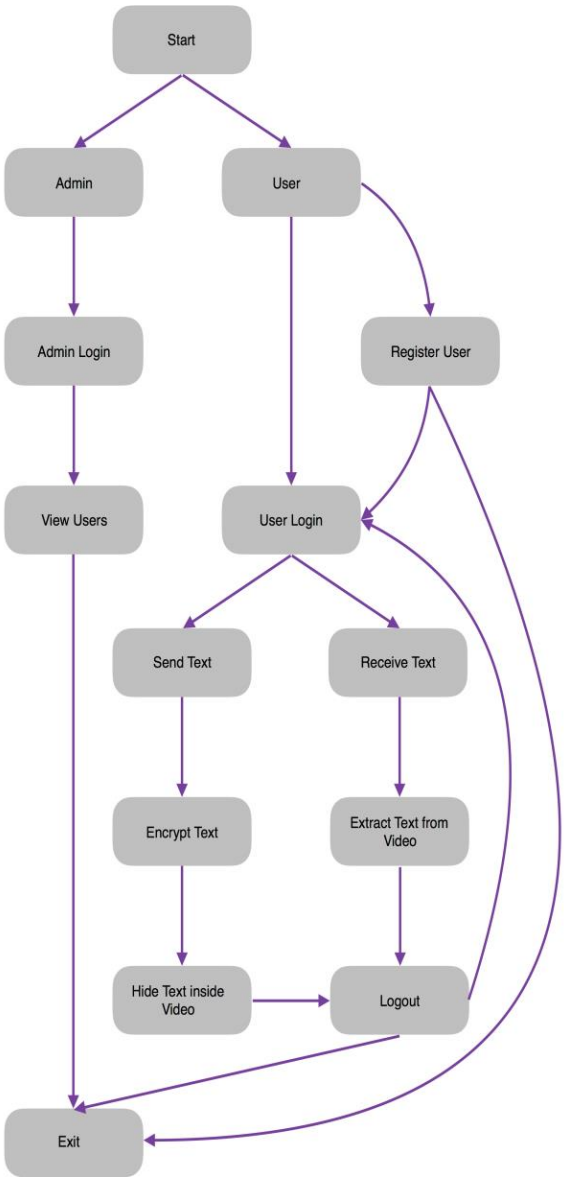


Now, if we again wish to do this dot function, we need to drop the value of R in symmetry to themirror image of the curve i.e. on the opposite side of x-axis. Let's call that point 'S'. Now if we draw a line from P to S, (that is, dot it essentially) we will find that there are again 3 points on this line which intersect the curve. Let's call the third point on this line 'T'. Now we can again drop the value of T to the mirror image of the curve on the other side of the x-axis. Let's call this point 'U'. Now we can dot P to U. We can dot this a certain number of times.
Another important term is the max value. It is essentially the key size. The larger the max value, the more space is we have to work with the keys. If any value crosses the max value, we have to start all over again. So, as max value increases, we get more values to work with, thus increasing the complexity of cracking this system.
Private Keyin this whole crypto-system, is the 'n', that is the number of times thatthe system dot the number 'n' with itself.

III. PROPOSED SYSTEM

In short, the existing system has overhead of choosing the key, more time consumption in encoding and decoding and not good in user interface. Though some of them are appropriate in every aspect, but some have too many bugs and there is a possibility that program is not available for other operating systems. The proposed system will consider the above shortcomings and since we will be using java so the problem of operating on different operating systems and even on different hardware will no longer be an issue. The basic idea behind all this is to hide the data from intruders and send to the receiver securely. The secure data transmission is based on an algorithm i.e. ECC.

A. Structure Modal:



At the Sender's end:

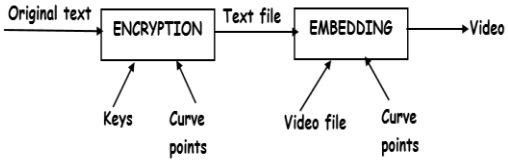
- User inputs the video that can be broken down into frames.
- User enters the data that he needs to send.
- User enters the prime number that will be used for ECC.This data is encrypted with the help of ECC.
- The prime number entered by the user is used to locate elliptic curve points on the frames of video.
- Now on these points, we can alter the pixel value of the frames in order to hide our data.
- Data is stored in multiple consecutive frames.
- Frames are recombined to form a video.

At the receiver's end:

- Video received is broken down into frames.
- Points are located using the prime number that was initially used.
- Data is recovered from the frames.

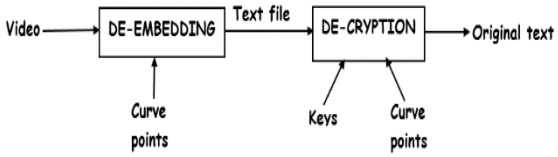
1) Embedding:

a) Firstly, the user will enter the message, i.e. the information, he wants to hide.
b) Then, the user will enter a key and two points of the curve and will encrypt the information by just a press of a button.
c) The cipher text is displayed. The user will save it to a text file.
d) Then, the user will select a video file from the local storage of his computer and the text file which houses the cipher text.
e) Then, he will enter another two points of the curve, which ought to be prime numbers and embed the text in the video. These points will be stored in the database for later authentication at the de-embedding stage.
f) The new video is overwritten in place of the original video.



2) De-embedding:

- The user will select a video from the local storage.
- Then, the user will enter the two points of the curve which will be matched from the database.
- If the points are matched, the data from the video will be extracted and be stored in a text file. This is in the cipher form.
- The user will select this text file and input the values of key and the other curve points for decryption.
- The algorithms will convert the cipher text to the plain text and display it.



IV. CONCLUSION

With every independent execution of the system, it could easily be observed that the cipher text becomes bigger and better with the increase in the values of the keys and the curve points, making it even harder for the intruder to decode or make a wild guess of the original information out of the encrypted one, without knowing proper key values. Moreover, using a 10-second video of a full high definition resolution was more than enough to hide a whole lot of information, making it next to impossible for an intruder to even guess if there's anything unusual with the video just by watching it.

V. FUTURE SCOPE

Elliptic Curve Cryptography (ECC) is absolutely the next-generation technique to cryptography as it make use of a mathematical formula and use of relatively smaller keys for cryptography that provide either the same or even greater level of security than the larger RSA keys. Thus, ECC is of great use to the highly secured agencies and government databases as well as information sharing methods. In 2010, NIST has recommended moving from RSA 1024-bit to RSA 2048-bit keys. ECC, someday or the other, is for sure going to outsmart RSA for not just testing purpose, but real time applications.For making it even better, a research could be conducted where the keyswill create automatically from the elliptical curve rather than applying the time consuming method that is mentioned above.

REFERENCES

[1] http://www.omnisecu.com/ccna-security/what-is-network-security-and-why-we-need-network-security.php
[2] Mohammad Ali BaniYounes 1 and AmanJantan 2, "A New Steganography Approach for Image Encryption Exchange by Using the Least Significant Bit Insertion,"IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.6, June 2008.
[3] Wikipedia, "Elliptic Curve Cryptography", January 2017. https://en.wikipedia.org/wiki/Elliptic_curve_cryptography
[4] Ravneet Kaur and Tanupreet Singh, "Hiding Data in Video Sequences using LSB with Elliptic Curve Cryptography," International Journal of Computer Applications (0975 – 8887) Volume 117 – No. 18, May 2015.
[5] L Vegh and L Miclea, "Improving the Security of a Cyber-Physical System using Cryptography, Steganography and Digital Signatures," International Journal of Computer and Information Technology (ISSN: 2279 – 0764) Volume 04 – Issue 02, March 2015.
[6] http://www.cs.virginia.edu/~kam6zx/invention/trapdoor-one-way-functions/
[7] An Liu and PengNing, "TinyECC: A Configurable Library for Elliptic Curve Cryptography in Wireless Sensor Networks."Proceeding: IPSN '08 Proceedings of the 7th international conference on Information processing in sensor

networks April 22 - 24, 2008, IEEE Computer Society Washington, DC, USA ©2008

[8] Tarun Narayan Shankar and G. Sahoo, "CRYPTOGRAPHY WITH ELLIPTIC CURVES," International Journal Of Computer Science And Applications Vol. 2, No. 1, April / May 2009.

[9] MrithaRamalingam, "Stego Machine – Video Steganography using Modified LSB Algorithm," World Academy of Science, Engineering and Technology 50 2011.

[10] Ertaul L., Lu W. (2005), "ECC Based Threshold Cryptography for Secure Data Forwarding and Secure Key Exchange in MANET (I)". In: Boutaba R., Almeroth K., Puigjaner R., Shen S., Black J.P. (eds) NETWORKING 2005. Networking Technologies, Services, and Protocols; Performance of Computer and Communication Networks; Mobile and Wireless Communications Systems.NETWORKING 2005. Lecture Notes in Computer Science, vol 3462. Springer, Berlin, Heidelberg.

[11] V.S. Miller, "Use of Elliptic Curves in Cryptography", Advances in Cryptology - Proceedings of CRYFTO '85 Springer Verlag Lecture Notes in Computer Science 218, pp. 417-426, 1986.

[12] K. Lauter, "The advantages of elliptic curve cryptography for wireless security," **Published in:** IEEE Wireless Communications (Volume: 11, Issue: 1, Feb 2004).

[13] N. Gura, A .Patel, A. Wander, H. Eberle, and S. C. Shantz, "Comparing elliptic curve cryptography and rsa on 8-bit CPUs," In CHES, Boston, Aug. 2004.

[14] Nicholas Jansma and Brandon Arrendondo, "Performance Comparison of Elliptic Curves and RSA Signatures,"

[15] Rounak Sinha, Hemant Kumar Srivastava, Sumita Gupta, "Performance Based Comparison Study of RSA and Elliptic Curve Cryptography," International Journal of Scientific & Engineering Research, Volume 4, Issue 5, May-2013 ISSN 2229-5518.

[16] David Dunning, "What Are the Advantages & Disadvantages of Elliptic Curve Cryptography for Wireless Security?", March 2015. https://www.techwalla.com/articles/what-are-the-advantages disadvantages-of- elliptic-curve-cryptography-for-wireless-security