IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 4, April 2016

A New Approach of Cryptographic Technique using RSA & ECC

Vaibhav V. Bhujade[1], Deepak Chaudhary[2]

Assistant Professor, Computer Science & Engineering, DMIETR, Wardha, Maharashtra, India[1]

Assistant Professor, Computer Science & Engineering, IET, Alwar, Rajasthan, India [2]

Abstract: Cryptography is the technique in which usually a file is converted into unreadable format by using public key and private key system called as public key cryptosystem. Then as per the user requirement that file is send to another user for secure data transmission. In this transmission file of unreadable format is send, after receiving this file receiver used the same algorithm and key to get the original file data. In this procedure various algorithms are used as a processing function and depending on that algorithm we used the key. The strength of any algorithm is depending on the key used in sender and receiver side. For this secure transmission we traditionally used RSA algorithm which is more secure for use so most of the system used the same algorithm for secure communication. Even most of the financial transaction is done by the use of this algorithm as it used the strong key while encryption and decryption. But In today's digital world there is a tremendous growth in the usage of the Internet. Behind one software generator there are hundreds of hackers. So, a fraction of second will be enough to destroy the security. Hence we require more strong algorithms, which secure the Internet work of sending and receiving. So this proposed system enhanced the security of existing RSA algorithm by using elliptical curve cryptography (ECC) algorithm. This algorithm is also stronger and has less key length as compared to RSA. The resultant system will be more secure than the previous system by enhancing the security of existing algorithm. Also proposed system provide good authentication for the user.

Keywords: Cryptography, Authentication, Plain Text, cipher text, RSA, ECC

I. INTRODUCTION

Cryptography has a long and fascinating history. The most complete non-technical account of the subject is Kahn's The Code breakers. This book traces cryptography from its initial and limited use by the Egyptians some 4000 years ago, to the twentieth century where it played a crucial role in the outcome of both world wars. Completed in 1963, Kahn's book covers those aspects of the history which were most significant (up to that time) to the development of the subject. The predominant practitioners of the art were those associated with the military, the diplomatic service and government in general. Cryptography was used as a tool to protect national secrets and strategies.
The proliferation of computers and communications systems in the 1960s brought with it a demand from the private sector for means to protect information in digital form and to provide security services. Beginning with the work of Feistel at IBM in the early 1970s and culminating in 1977 with the adoption as a U.S. Federal Information Processing Standard for encrypting unclassified information, DES, the Data Encryption Standard, is the most well-known cryptographic mechanism in history. It remains the standard means for securing electronic commerce for many financial institutions around the world.

The most striking development in the history of cryptography came in 1976 when Diffie and Hellman published New Directions in Cryptography. This paper introduced the revolutionary concept of public-key cryptography and also provided a new and ingenious method for key exchange, the security of which is based on the intractability of the discrete logarithm problem. Although the authors had no practical realization of a public-key encryption scheme at the time, the idea was clear and it generated extensive interest and activity in the cryptographic community. In 1978 Rivest, Shamir, and Adleman discovered the first practical public-key encryption and signature scheme, now referred to as RSA. The RSA scheme is based on another hard mathematical problem, the intractability of factoring large integers. This application of a hard mathematical problem to cryptography revitalized efforts to find more efficient methods to factor. The 1980s saw major advances in this area but none which rendered the RSA system insecure. Another class of powerful and practical public-key schemes was found by ElGamal in 1985. These are also based on the discrete logarithm problem.

One of the most significant contributions provided by public-key cryptography is the digital signature. In 1991 the first international standard for digital signatures (ISO/IEC 9796) was adopted. It is based on the RSA public-key scheme. In 1994 the U.S. Government adopted the Digital Signature Standard, a mechanism based on the ElGamal public key scheme.

The search for new public-key schemes, improvements to existing cryptographic mechanisms, and proofs of security continues at a rapid pace. Various standards and infrastructures involving cryptography are being put in

DOI 10.17148/IJARCCE.2016.54254

place. Security products are being developed to address the security needs of an information intensive society. [8]

Basics of Cryptography

Cryptography is the science of information security. The word is derived from the Greek kryptos, meaning hidden. Cryptography is closely related to the disciplines of cryptology and cryptanalysis. Cryptography includes techniques such as microdots, merging words with images, and other ways to hide information in storage or transit. However, in today's computer-centric world, cryptography is most often associated with scrambling plaintext (ordinary text, sometimes referred to as clear text) into cipher text (a process called encryption), then back again (known as decryption). Individuals who practice this field are known as cryptographers.

Modern cryptography concerns itself with the following four objectives:

- Confidentiality (the information cannot be understood by anyone for whom it was unintended)
- Integrity (the information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected)
- Non-repudiation (the creator/sender of the information cannot deny at a later stage his or her intentions in the creation or transmission of the information)
- Authentication (the sender and receiver can confirm each other’s identity and the origin/destination of the information)

In recent times, cryptography has turned into a battleground of some of the world's best mathematicians and computer scientists. The ability to securely store and transfer sensitive information has proved a critical factor in success in war and business.

2. RELATED WORKS

Cryptosystem

Encryption is a method of transforming original data, called plaintext or clear text, into a form that appears to be random and unreadable, which is called cipher text. Plain text is either in a form that can be understood by a person (a document) or by a computer (executable code). Once it is transformed into cipher text, neither human nor machine can properly process it until it is decrypted. This enables the transmission of confidential information over insecure channels without unauthorized disclosure. When data is stored on a computer, it is usually protected by logical and physical access controls. When this same sensitive information is sent over a network, it can no longer take these controls for granted, and the information is in a much more vulnerable state.

The algorithm, the set of mathematical rules, dictates how enciphering and deciphering take place. Many algorithms are publicly known and are not the secret part of the encryption process. The way that encryption algorithms work can be kept secret from the public, but many of them are publicly known and well understood. If the internal mechanisms of the algorithm are not a secret, then something must be. The secret piece of using a well-known encryption algorithm is the key. The key can be any value that is made up of a large sequence of random bits. Is it just any random number of bits crammed together? Not really. An algorithm contains a key space, which is a range of values that can be used to construct a key. The key is made up of random values within the key space range. The larger the key space, the more available values can be used to represent different keys, and the more random the keys are, the harder it is for intruders to figure them out

3. PROPOSED SYSTEM

The proposed system is a combine approach of two most secure algorithms that are globally accepted for the security and accuracy in work. These are RSA and elliptical curve cryptography. RSA is well known algorithm used globally. RSA implements a public-key cryptosystem, as well as digital signatures. RSA is motivated by the published works of Diffee and Hellman from several years before, who described the idea of such an algorithm, but never truly developed it. Introduced at the time when the era of electronic email was expected to soon arise, RSA implemented two important ideas:

1. Public-key encryption. This idea omits the need for a \courier" to deliver keys to recipients over another secure channel before transmitting the originally-intended message. In RSA, encryption keys are public, while the decryption keys are not, so only the person with the correct decryption key can decipher an encrypted message. Everyone has their own encryption and decryption keys. The keys must be made in such a way that the decryption key may not be easily deduced from the public encryption key.

2. Digital signatures. The receiver may need to verify that a transmitted message actually originated from the sender (signature), and didn't just come from there (authentication). This is done using the sender's decryption key, and the signature can later be verified by anyone, using the corresponding public encryption key. Signatures therefore cannot be forged. Also, no signer can later deny having signed the message.

This is not only useful for electronic mail, but for other electronic transactions and transmissions, such as fund transfers. The security of the RSA algorithm has so far been validated, since no known attempts to break it have yet been successful, mostly due to the difficulty of factoring large numbers n = pq, where p and q are large prime numbers. [9]

Another algorithm in this approach is Elliptical curve cryptography. Elliptic Curve Cryptography (ECC) is emerging as an attractive public-key cryptosystem for mobile/wireless environments. Compared to traditional cryptosystems like RSA, ECC offers equivalent security

DOI 10.17148/IJARCCE.2016.54254

with smaller key sizes, which results in faster computation, lower power consumption, as well as memory and bandwidth savings. This is especially useful for mobile devices which are typically limited in terms of their CPU, power and network connectivity. However, the true impact of any public-key cryptosystem can only be evaluated in the context of a security protocol. This paper presents a first estimate of the performance improvements that can be expected in SSL (Secure Socket Layer), the dominant security protocol on the Web today, by adding ECC support. Today, the scientific efforts are looking for a smaller and a very faster public key cryptosystem, at the same time the approach should be practical and very secure, even for the most constrained environments. For any cryptographic technique, there is an analogue for Elliptic Curve. One of these systems is Diffie – Hellman key exchange system. This paper proposed methods to encrypt and decrypt the message, and we will encrypt and decrypt the message by using the Diffie–Hellman Exchanging key. And this is a secrete point in the proposed methods (M1) and (M2). In the first method (M1), the sender compute the multiplication between the coordinates of the key in the encryption algorithm, and the receiver compute the multiplication between the coordinates of the key in the decryption algorithm.

In the second method (M2), we support the system more security of the first method, because the sender compute the exponentiation function between the coordinates of the key in the encryption algorithm (use fast exponentiation method), and the receiver compute the inverse of the exponentiation function between the coordinates of the key in the decryption algorithm. The rapid progress in wireless mobile communication technology and personal communication systems has prompted new security questions. Since open air is used as the communication channel, the content of the communication may be exposed to an eavesdropper, or system services can be used fraudulently. In order to have reliable proper security over the wireless communication channel, certain security measures need to be provided .The mobile environment aggravates some of the security concerns and threats. Mobile users will use resources at various locations and may be provided by different service providers. Integrity and confidentiality of information stored on the mobile appliance is another important concern. ATM machines and storage of medical records require an efficient encryption algorithm, which uses low processing power. The vast majority of the products and standards that use public-key cryptography for encryption and digital signatures use RSA [1]. As we have seen, the bit length for secure RSA use has increased over recent years, and this has put a heavier processing load on applications using RSA. This burden has ramifications, especially for electronic commerce sites that conduct large numbers of secure transactions. Recently, a competing system that has emerged is elliptic curve cryptosystem (ECC) [3,4].

The resultant system we get is most secure as compare to previous developed system as we are using the power of both the algorithm. In this system first of all the file is encrypted by RSA algorithm and that encrypted data is again encrypted by elliptical curve cryptography algorithm so the resultant output is most secure data in unreadable form. After getting this output the system decrypt it on the client side by using the elliptical curve cryptography algorithm and then by the algorithm in the combined approach. In between this process of encrypting and decrypting the system permit the user who have access of that file and this permission is given by the server. Before giving the permission server verify the user about his identity from his information which is entered by that user at the time of registration. After verifying that user server allow and send a secret key to that user to allow the download for the same file. This system maintains the database of the entire registered user. So any one can registered on to this system but only allowed user can access the secure files of the server. This system provides the uploading option to the server only and that uploaded file can be access by any registered user who is allowed by the server. This all means that this system is secure in terms of security as we are using the power of both the algorithm and also provide a better authentication mechanism for the registered user for file accessing.

The process latest several months during which Rivest proposed approaches, Adleman attacked them and Shamir recalls doing some of each. In cryptography, RSA is an algorithm for public-key cryptography which was given by Rivest, Shamir and Adleman. According to Mathematically. The RSA algorithm is based on the mathematical part that is easy to find and multiple two large prime numbers together, but it is extremely difficult to factor their product. There are some important steps are involved in a RSA algorithm to solve a problem as given below:

Step 1: Assume two large prime numbers p & q.
Step 2: Compute:

$$N = p*q$$

Where N is the factor of two large prime number.

Step 3: Select an Encryption key (E) such that it is not a factor of (p-1)*(q-1)

$$\text{i.e. } Ø(n)= (p-1)*(q-1)$$

for calculating encryption exponents E, should be 1< E < Ø(n) such that

$$gcd(E, Ø(n)=1$$

The main purpose of calculating gcd is that E & Ø(n) should be relative prime. Where Ø (n) is the Euler Totient Function & E is the Encryption Key.

Step 4: Select the Decryption key (D), which satisfy the Equation

$$D*E \bmod (p-1)*(q-1) = 1$$

Step 5: For Encryption:
Cipher Text= (Plain Text)E mod N
CT = (PT) E mod N
Or
CT=ME mod N
Step 6: For Decryption:
Plain Text= (Cipher Text)E mod N
PT= (CT) E mod N

DOI 10.17148/IJARCCE.2016.54254

Elliptic Curve Cryptography

Elliptic Curve Cryptography (ECC) is emerging as an attractive public-key cryptosystem for mobile/wireless environments. Compared to traditional cryptosystems like RSA, ECC offers equivalent security with smaller key sizes, which results in faster computation; lower power consumption, as well as memory and bandwidth savings. This is especially useful for mobile devices which are typically limited in terms of their CPU, power and network connectivity. However, the true impact of any public-key cryptosystem can only be evaluated in the context of a security protocol. This paper presents a first estimate of the performance improvements that can be expected in SSL (Secure Socket Layer), the dominant security protocol on the Web today, by adding ECC support.

Today, the scientific efforts are looking for a smaller and a very faster public key cryptosystem, at the same time the approach should be practical and very secure, even for the most constrained environments. For any cryptographic technique, there is an analogue for Elliptic Curve. One of these systems is Diffie – Hellman key exchange system. This paper proposed methods to encrypt and decrypt the message, and we will encrypt and decrypt the message by using the Diffie–Hellman Exchanging key. And this is a secrete point in the proposed methods (M1) and (M2).

In the first method (M1), the sender compute the multiplication between the coordinates of the key in the encryption algorithm, and the receiver compute the multiplication between the coordinates of the key in the decryption algorithm. In the second method (M2), we support the system more security of the first method, because the sender compute the exponentiation function between the coordinates of the key in the encryption algorithm (use fast exponentiation method), and the receiver compute the inverse of the exponentiation function between the coordinates of the key in the decryption algorithm.

The rapid progress in wireless mobile communication technology and personal communication systems has prompted new security questions. Since open air is used as the communication channel, the content of the communication may be exposed to an eavesdropper, or system services can be used fraudulently. In order to have reliable proper security over the wireless communication channel, certain security measures need to be provided .The mobile environment aggravates some of the security concerns and threats. Mobile users will use resources at various locations and may be provided by different service providers. Integrity and confidentiality of information stored on the mobile appliance is another important concern. ATM machines and storage of medical records require an efficient encryption algorithm, which uses low processing power.

The vast majority of the products and standards that use public-key cryptography for encryption and digital signatures use RSA[1]. As we have seen, the bit length for secure RSA use has increased over recent years, and this has put a heavier processing load on applications using RSA. This burden has ramifications, especially for electronic commerce sites that conduct large numbers of secure transactions. Recently, a competing system that has emerged is elliptic curve cryptosystem (ECC)[3,4].

4. OBJECTIVES

Before initiating this project, substantial amount of time has been spent to study algorithms related to cryptography and coming to a conclusion that there exists an ample scope to simplify/ improve/ enhance/ redevelop/ redesign/ rearrange these methods.

Objectives of this work are:

i. To arrange the algorithm which provide more security to the stored data on server side.
ii. To provide the enhanced security to the image file also as this system protect the document files.
iii. To provide better authentication technique for the each registered user more individual level security.

The basic cryptographic algorithm RSA is known to everywhere, it is efficient and reliable too. But as it is used in everywhere so there may issue of cracking this algorithm. So our system is using the advantages of RSA but also this system enhanced this security by using elliptical curve cryptography. This combined approach of both algorithms provides better security mechanism.

Also this system provide the server client mechanism in which the file uploaded on the server side can be downloaded by the client who is successfully register on this system. So when any client needs to access any file on server side, client will request to download that file. If server finds that requested client is authorized and permit table then server gives the access of that file by providing the secret key to the requested client. Then client can easily download the required file by using the server generated secret key. The previous system are developed for the document file of image file with single algorithm who is not that much secure. But this system is based on the combined approach on both algorithm and also provides the service for document as well as image file.

5. CONCLUSION AND FUTURE WORK

We have presented a novel software-based scheme to prevent the attack from the unauthorized person and provide more enhanced security for data communication and data transfer.

Cryptographic support is an important mechanism of securing important data. In this work, we introduce combined approach of two well-known and secured algorithms RSA and ECC. This algorithm is simple and fast enough for most applications. RSA is already in use in most of the application globally, we add the more secured

DOI 10.17148/IJARCCE.2016.54254

technique call elliptical curve cryptography to enhance its security.

In future, we are interested to extend the proposed system for every possible format of files by which everyone is capable to use this system for secure data transmission and sharing of various files through this secure channel.

REFERENCES

[1] William Stallings :Cryptography and Network Security Principles and Practice, 5th Edition

[2] Giuseppe Ateniese & Stefan Mangard : A New Approach to DNS Security (DNSSEC) , CCS'01, November 5-8, 2001, Philadelphia, Pennsylvania, USA.

[3] M. Junaid Arshad and M. Abrar "Securing DNS Using Elliptical Curve Cryptography: An Overview"

[4] Ram Ratan Ahirwal, Manoj Ahke, "Elliptic Curve Diffie-Hellman Key Exchange Algorithm for Securing Hypertext Information on Wide Area Network ", IJCSIT volume 4 (2) 2013

[5] Anoop MS : Elliptic Curve Cryptography An Implementation Guide

[6] G.V.S. Raju and Rehan Akbani, Department of Computer Science The University of Texas at San Antonio. San Antonio, TX 78249-0669 "Elliptic Curve Cryptosystem and its Applications"

[7] S. Maria Celestin Vigila1, K. Muneeswaran2, "Elliptic Curve based Key Generation for Symmetric Encryption", IEEE 2011

[8] Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone, HANDBOOK of APPLIED CRYPTOGRAPHY

[9] Burt Kaliski RSA Laboratories, The Mathematics of the RSA Public-Key Cryptosystem

[10] Vishwa gupta,2. Gajendra Singh ,3 .Ravindra Gupta, "Advance cryptography algorithm for improving data security" IJARCSSE 2012

[11] William Stalling ,Network security and cryptography by PHI publications.

[12] Atul Kahate, Cryptography and network security ,second edition ,TataMcGraw-Hill

DOI 10.17148/IJARCCE.2016.54254