Volume 5, Issue 11, November 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

An Inventive Digital Envelope Gradient for an Unsecured Channel

Nilima Karankar
Department of Computer Engineering,
Institute of Engineering & Technology, DAVV,
Indore, India

Abstract: ***In our daily life we are using internet for our 95% of the work. We are transferring data from one computer to other over the network, while exchanging the data there are many security issues arises. In order to achieve the key features of security i.e. integrity, authentication, non-repudiation, Digital Envelope is used. Digital Envelope is a secure electronic data container that is used to protect the message. Digital envelope allows user to encrypt data with the speed of secret key encryption and the security of public key encryption. In our work, we suggest an implementation of a digital envelope for a secure channel that combines the hashing algorithm MD5, the symmetric key algorithm (Blowfish) and the asymmetric key algorithm (Elliptic Curve Cryptography (ECC)). ECC is the unsurpassed alternative asymmetric key technique rather than RSA in the digital envelope hybrid cryptosystem.***

Keywords: Blowfish, Authenticity, Elliptic Curve Cryptosystems (ECC), Message Digest version 5 (MD5), Non-Reputability.

I. INTRODUCTION

The use of internet and network application is growing exponentially over the decades. Security is the most important and challenging aspect in internet and network application. Data which is exchanged over network or internet must be secure, must be hidden from the unauthorized user. In order to achieve the confidentiality of message, a cryptography technique is used. Cryptography is used in technologically advanced societies like; electronic commerce, where data security is more important [5]. Now –a –days cryptography techniques are used everywhere like internet banking, ATM, M-commerce etc, where data is most important. Cryptography provides a method for securing and authenticating the transmission of information across insecure communication channels. It enables us to store sensitive information or transmit it over insecure communication networks so that unauthorized persons cannot read it [12]. Cryptography techniques have two major components: Encryption algorithm and Key. We can see the simple flow of information from one system to other through diagram given:

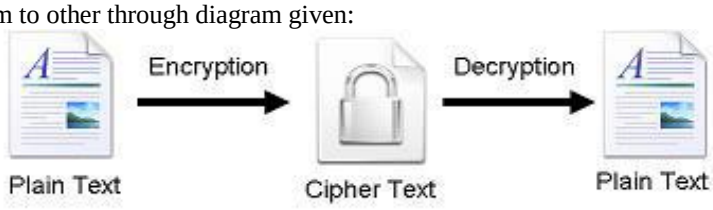

Fig.1 Encryption-Decryption Flow

Cryptographic techniques are broadly classified into symmetric key cryptographic techniques (DES, TDES, AES, Blowfish, and IDEA) and asymmetric key cryptographic techniques (RSA, ECC, HECC cryptography) [1]. In our work, we are proposing the details of a digital envelope for a secure data transfer using the Blowfish and ECC Cryptosystem. The reason behind for the adoption of ECC in this approach is that, ECC provides more security than RSA.

II. OBJECTIVES

The main objective is to achieve key security features i.e. Integrity, Authentication, and Non-repudiation by using cryptography techniques. Every communication channel which is used for data transfer must ensure security features:

1) **Confidentiality**: It must certify that the secret information can only be obtained, by the sender and the receiver, but not anyone else.
2) **Authentication:** It must certify the sender and the receiver's identities, and avoid the opponent to send a malicious message. The other hand, the scheme only allows a designate receiver to verify the signature for giving message.
3) **Non-repudiation**: It must confirm the sender's identity, and the sender could not repudiate his signature and message.

4) **Integrity**: It must be verify that message could not be change by anyone. Message should reach to the receiver which originally sends by the sender.

For these we have consider [1] as base paper, in which data is encrypted through AES and HECC to form the Digital Envelope. I have use best of both the algorithms (i.e. Symmetric and Asymmetric).
Blowfish is better than AES. Because AES is breakable, and blowfish is unbreakable. Blowfish uses variable length key, so it is hard to break the encrypted message. We are also sending the data in the form of digital envelope by encrypting the data with Blowfish and ECC. So we are using MD5 to generate the Message Digest. I have used this message digest (pseudorandom no.) as a key to encrypt the plaintext using Blowfish and ECC is used to encrypt the key. After encryption we will form a digital envelope consisting of message digest, cipher text and encrypted key in to it, and send it to receiver. Receiver will decrypt the msg.

III. DIGITAL ENVELOPE

Digital Envelope is a mechanism to send data from one location to another in secure fashion. Digital Envelope is a type of protection that uses two layers of encryption to secure a message. First, the message itself is encoded using symmetric encryption and then the key is also encrypted using public-key encryption. This technique overcomes one of the problems of public-key encryption, which is that it is slower than symmetric encryption. Because only the key is protected with public-key encryption, there is very little overhead [13].

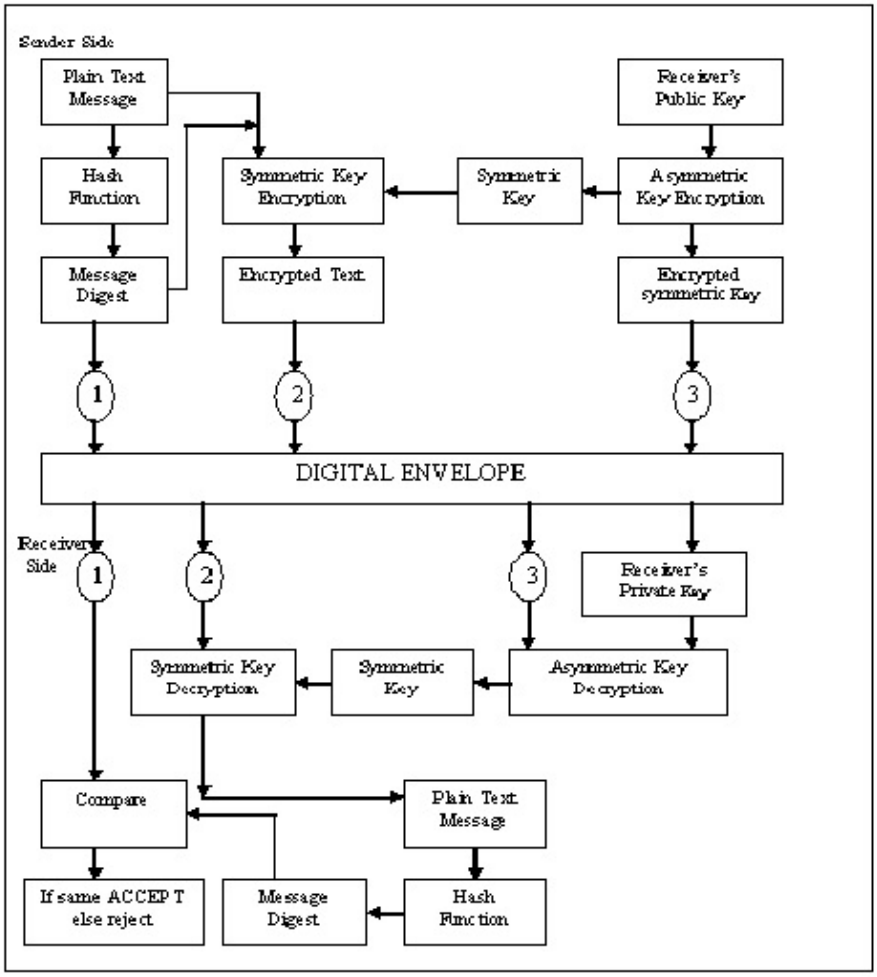

Fig 2: Digital Envelope Diagram

IV. RELATED WORK

In our research work we have studied so many papers, some authors worked on digital signature, some authors worked on digital envelope. Some authors worked on both digital signature and digital envelope in order to achieve the security of transferred data. Desponia palaka proposes a protocol using Scrip and digital envelope. In this protocol, financial institutions become partners in the e-commerce transaction, conducted by their customers over the Internet. The improvement of the proposed protocol is the reduction of the contribution of the financial institutions to ancillary support services like helping on establishing trust between the parties and at the completion of the peer-to-peer payment transaction. Moreover, the proposed system can be characterized as distributed allocation of provinces to merchants, who are responsible for locally authorizing payments. Finally, it is optimized for repeated payments to the same merchants [14].
M Gobi proposes Secure Electronic Medical Records (SEMR), which aims at providing a set of services which will

provide secure and efficient access of the EMRs to the patients, doctors, nurses and insurance agents. The set of services that are provided by SEMR include Authentication, Authorization and Secure communication. They have suggested an implementation of a digital envelope that combines the hashing algorithm of MD5, the symmetric key algorithm of AES and the asymmetric key algorithm of Hyper Elliptic Curve Cryptography (HECC). The result illustrates that the best alternative digital envelope hybrid cryptosystem for EMR [15].From this work we have influence to do the same work, by changing the symmetric key algorithm (AES) to Blowfish. Because AES is breakable blowfish uses variable length key, so that it is hard to break. We have also performed the comparative study of different algorithm:

- **DES**: DES was the first data encryption algorithm created in 1972 by IBM and was adopted by the US government as standard encryption method. DES begins the encryption process by using a 64-bit key. The NSA restricted the use of DES to a 56-bit key length, so DES discards 8-bits of the key and then uses the remaining key to encrypt data in 64-bit blocks. DES can operate in CBC, ECB, CFB and OFB modes, giving it flexibility. In 1998 the supercomputer DES cracker, assisted by 100,000 distributed PCs on the Internet, cracked DES in 22 h. The US government has not used DES since 1998[4].
- **AES:** Advanced Encryption Standard is a symmetric block cipher that can encrypt data blocks of 128 bits using symmetric keys 128, 192, or 256. AES was introduced after the DES. DES is also vulnerable, but no security algorithm is complete without DES. Brute force attack is the only successful attack known against this algorithm. It is also known as the Rijndael (pronounced as Rain Doll) algorithm [9].
- **Blowfish:** Blowfish is a symmetric block cipher. It takes a variable-length key, from 32 bits to 448 bits, making it ideal for securing data. It can be efficiently used for encryption and safety of data. It takes a variable-length key, from 32 bits to 448 bits, making it ideal for securing data. This algorithm was designed in 1993 by Bruce Schneier as a fast, free unconventional to existing encryption algorithms. Blowfish is unpatented and license-free, and is available free for all uses. Though it suffers from weak keys problem, no attack is known to be successful against it (Bruce, 1996) (Nadeem, 2005)[9].

B. Other Contributions (Tamimi, 2008) provided a performance comparison between four most common algorithms: DES, 3DES, AES, and Blowfish. The comparison had been conducted by running several different settings to process different sizes of data blocks to evaluate the algorithm's encryption/decryption speed. The simulation setup was in java programming language. The results shows that blowfish has a better performance than other common encryption algorithms. AES showed poor performance results compared to other algorithms since it requires more processing power [9].

The results shows that AES outperformed other algorithms in both the number of requests processes per second in different user loads, and in the response time in different user-load situations.

(N. Penchalaiahet.al., 2010) discussed the principal advantages of AES with respect to DES, as well as its limitations. They said that AES can be quite comfortably implemented in high level or low level languages.

(Elmina am et. al., 2010) presented a comparison of AES, DES, 3DES, RC2, Blowfish and RC6. They used different settings for each algorithm such as different sizes of data blocks, different data types, battery power consumption, different key size finally encryption/decryption speed. They concluded that in case of changing packet size Blowfish showed better performance than other algorithms followed by RC6.AES had better performance than RC2, DES, and 3DES. In case of changing key size - it was concluded that higher key size leads to clear change in the battery and time consumption.

(Singhal and Raina, 2011) presented a comparative analysis between AES and RC4 for better utilization. In this paper authors tried to find out performance comparison between block ciphers (AES) and stream cipher (RC4) algorithm. Based on the analysis and result, this paper concluded that which algorithm is better to use based on different performance metrics. The various metrics were: Encryption time, Decryption time, Throughput, CPU process time, Memory Utilization.

V. PROPOSED MODEL

Our model uses MD5 to generate message digest. Message digest is a combination of alphabets and numbers or we can say that it is a pseudorandom no. which we are using as a key to encrypt the plaintext. Plaintext is encrypted using blowfish and the receiver's public key is encrypted using Elliptic Curve Cryptography.

Blowfish is a symmetric block cipher that can be efficiently used for encryption and safeguarding of data. It takes a variable-length key, from 32 bits to 448 bits, making it ideal for securing data. Blowfish was designed in 1993 by Bruce Schneier as a fast, free alternative to existing encryption algorithms. Blowfish is unpatented and license-free, and is available free for all uses.

Blowfish Algorithm is a Feistel Network, iterating a simple encryption function 16 times. The block size is 64 bits, and the key can be any length up to 448 bits. Blowfish is a variable-length key block cipher.

The private key generation of the ECC, algorithm here accept self-generated key for encryption and that key is incorporated with the cipher for secure file exchange. In addition to that the algorithm is able to extract key from the given cipher and cross check the validity of the data.

Process of Encryption using ECC: First of all the system will accept Key and apply ECC encryption process on the key that will generate Symmetric key. Both cipher text and 128 bit key generated by MD5, and the encrypted key will send. Then on the decryption side it will get Cipher text and 128 bit key.

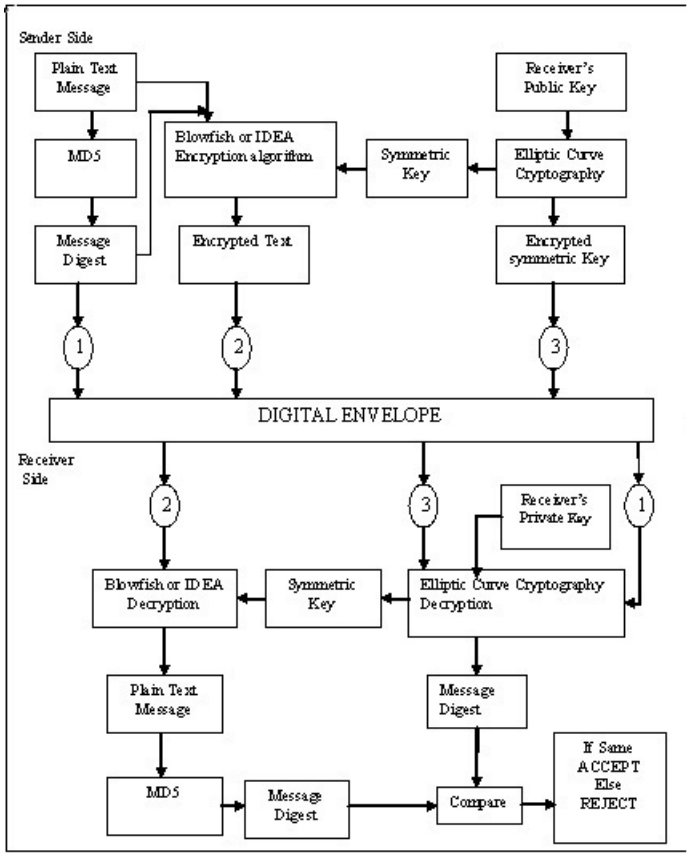

Fig 3: Digital Envelope Using Blowfish and ECC

Apply ECC decryption process on the cipher text and get original message. Now it will apply MD5 Algorithm on the message and get 128 bit key. If received 128 bit key and generated 128 bit key are same then message will accept otherwise message will discard. To understand the process of the proposed methodology, first required illustrating the traditional ECC encryption process. The traditional encryption and decryption process is given using figure 3 and 4.

If Q= Public key
P= A point on curve
d= Private key
M= Original message
K= random number

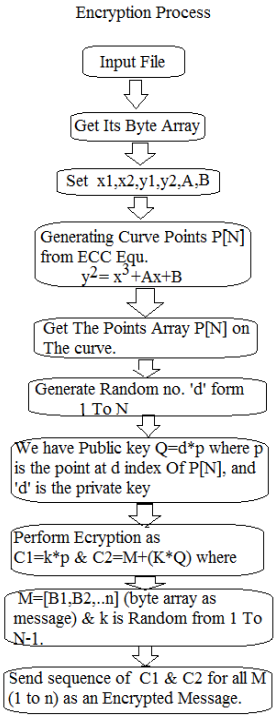

Figure 3 Encryption Process

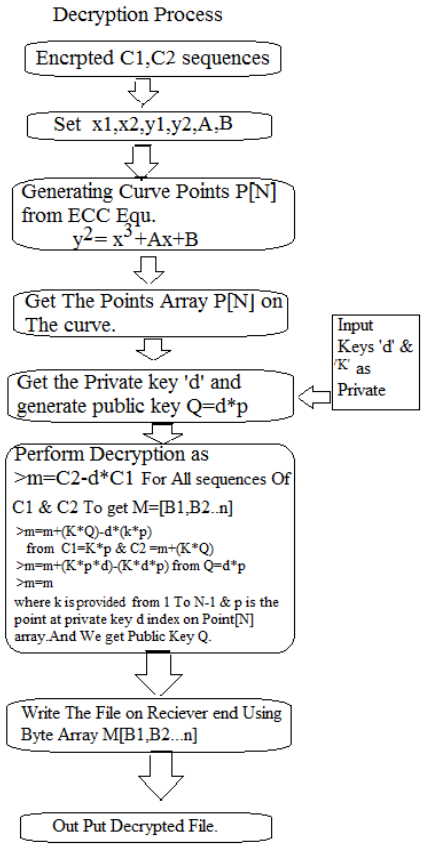

Figure 4 Decryption Process

Then using above parameters we get the two cipher texts blocks which are denoted using $C_1$and C_2

$C_1 = K.P$

$C_2 = M + KQ$

Using the above equations the message can be defined as:

$M = C_2 - d * C_1$

$M = C_2 - KQ$

At the network scenarios the cipher $C_1$and C_2 is sanded on network and the recovery of the original message can be found using the below given expression.

$M = C_2 - d * C_1$

$C_2 - d * C_1 = (M + KQ) - d * (K * p)$

In next step

$C_2 - d = M + KQ$

$C_2 = M + KQ$

$M = M$

Means the send message can be recoverable using the substitution and replacing the cypher context from the delivered messages, where the private key is utilized as the OTP (one time password). The encryption and decryption process for the transaction is given by the figure 2 and 3.

This section of the given paper includes the basic security system design methodology and simple details about the responsibilities of all communicating parties. In the next section draws the conclusion of the given work.

VI. CONCLUSION AND FUTURE WORK

This paper purposes the digital envelope method to encrypt our data to satisfy the rapidly growing need and to overcome security threats. Additionally, we have research comparative study of various algorithm for encrypt process ,with going through many algorithms we have come up with blowfish algorithm as best among them and then with the help of ECC method we do the process of encryption .Now, to conclude we would say that in future many communication technology will use this method for data encryption and decryption for secure and efficient data communication.

REFERENCE

[1] Ramachandran Ganesan, Mohan Gobi, and Kanniappan Vivekananda" A Novel Digital Envelope Approach for A Secure E-Commerce Channel".

[2] Amandeep Singh, Manu Bansal "FGPA Implementation of Optimized DES Encryption Algorithm on Spartan 3E" International Journal of Scientific & Engineering Research, Volume 1, Issue1, October-2010.

[3] Byung kwan Lee, Tai-Chi Lee, Seung Hae Yang "An ASEP (Advanced Secure Electronic Payment) Protocol Design Using 3BC and ECC(F2m) Algorithm" International Conference on e-Technology, e-Commerce and e-Service (IEEE'04).

[4] Akash Kumar Mandal, ChandraParakash "Performance Evaluation of Cryptographic Algorithms: DES and AES" 2012 IEEE Students' Conference on Electrical, Electronics and Computer Science.

[5] Ayushi "A Symmetric Key Cryptographic Algorithm" ©2010 International Journal of Computer Applications (0975 - 8887) Volume 1 - No. 15.

[6] E. Thambiraja, G.Ramesh, Dr. R. Umarani "A Survey on Various Most Common Encryption Techniques" Volume 2, Issue 7, July 2012 International Journal of Advanced Research in Computer Science and Software Engineering.

[7] Diaa Salama, Hatem Abdual Kader, and Mohiy Hadhoud "Studying the Effects of Most Common Encryption Algorithms" International Arab Journal of e-Technology, Vol. 2, No. 1, January 2011.

[8] Min-Shiang Hwang, Chi-Yu Liu "Authenticated Encryption Schemes: Current Status and Key Issues" International Journal of Network Security, Vol.1, No.2, PP.61–73, Sep. 2005

[9] Jawahar Thakur, Nagesh Kumar "DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis" Volume 1, Issue 2, December 2011 International Journal of Emerging Technology and Advanced Engineering.

[10] Stallings.W (2005), "Cryptography and Network Security 4th Ed," Prentice Hall.

[11] Abdel-Karim Al Tamimi "Performance Analysis of Data Encryption Algorithms" http://www.cse.wustl.edu/.

[12] P.Karthigaikumar, Soumiya Rasheed "Simulation of Image Encryption using AES Algorithm" IJCA Special Issue on "Computational Science - New Dimensions & Perspectives" NCCSE, 2011.

[13] Wenping Guo, Ying Chen, and Xiaoming Zhao "A Study on High-Strength Communication Scheme Based on Signed Digital Envelope" Proceedings of the Second International Symposium on Networking and Network Security (ISNNS '10) Jinggangshan, P. R. China, 2-4, April. 2010 pp. 190-192.

[14] Desponia palaka, Petros Daras "A Novel Peer-to-Peer Payment Protocol" International Journal of Network Security, Vol.4, No.1, PP.107-120, Jan.2007.

[15] Better Privacy and Security in E-Commerce: Using Elliptic Curve-Based Zero-Knowledge Proofs, Sultan Almuhammadi, ieeexplore.ieee.org/Xplore/home.jsp.

[16] A New Encryption Algorithm over Elliptic Curve, S. Han, E. Chang, W. Liu, ieeexplore.ieee.org/Xplore/home.jsp

[17] An Asymmetric Authentication Protocol for Mobile Devices Using Elliptic Curve Cryptography, Mrs. S. Prasanna Ganesan, ieeexplore.ieee.org/Xplore/home.jsp

