www.ijsrnsc.org

Available online at www.ijsrnsc.org

IJSRNSC

Volume-2, Issue-3, Oct- 2014
Research Paper

Int. J. Sci. Res. in
Network Security
and Communication
ISSN: 2321-3256

An Innovative Digital Envelope Slant for an Unsecured Channel

Nilima Karankar[1], V. Kapoor[2], C.P. Patidar[3*]

[1,2,3*]Department of Information Technology,
Institute of Engineering & Technology, DAVV, Indore-India

Received: July/20/2014 Revised: Aug/04/2014 Accepted: Sep/20/2014 Published: Oct/31/2014

Abstract- The digital signature and digital envelope are two techniques extensively used in data communication. Both techniques have some deficiencies like digital envelope provides only confidentiality and best of both the world. Digital Signature provides confidentiality as well as integrity and non-repudiation. Symmetric key cryptography in combination with asymmetric key cryptography is used in digital envelope does not provide all security features such as integrity, authentication, and non-repudiation. Hence to fulfil all security features MD5 has to be used with a symmetric key and asymmetric key cryptography. In our work, we suggest an implementation of a novel digital envelope technique. It comprises best of both the world and digital signature to fulfil all security features integrity, confidentiality, authentication, and non-repudiation. In our project work we are using the hash generation algorithm MD5, the symmetric key algorithm (Blowfish) and the asymmetric key algorithm (Ron Rivest Shamir Adelman (RSA)). RSA is very popular and proven asymmetric key cryptography. It provides confidentiality as well as integrity and non-repudiation. So we are providing an integrated solution which will meet the above mentioned requirements. It can overcome the shortcomings of the existing digital envelope technique and it provides strength to the security of e-commerce channel.

Key Words: Encryption, Decryption, Authenticity, Confidentiality, Integrity, Message Digest-5, Blowfish, Non-repudiation, Ron Rivets Shamir Adelman (RSA)

I. INTRODUCTION

This is the internet age and the usage of internet applications over the decades are growing explicitly. That created security is the biggest challenge to secure data over network. During transfer of data over the network, it must be secure and accessible by authorized person only. During research, we found that there is requirement of such a technique which provides all key security features. Symmetric encryption provides data protection through the use of one time secret key known as encryption, whereas decryption deals with the yield at the end of communication path. Symmetric key encryption only uses single key for encryption/decryption, so there is a problem of key exchange. Asymmetric key solves the problem of key exchange.

Asymmetric key cryptography uses two keys: Private Key and Public Key. Private Key must be kept secret and public key advertised publicly as part of your certificate. Today's world needs secure transmission through cryptographic algorithm. Our main aim is to design a novel digital envelope which uses Blowfish and RSA algorithm (integrating with MD5 algorithm) for encryption and decryption of data, to secure data transmission over e-commerce channel. The performance and security issues have considered in proposed work, because in real scenario there are many security issue arises when data is transported through any network. This work is proposed to provide an efficient and secure way of data transfer according to the [1] security model.

Digital Signature

Digital signature is one of the best techniques to provide authentication and non-repudiation. Digital signature uses public key algorithm. It uses two keys, one is secret key which is used for signing purpose, referred to as private key, the other is verification key which is open, referred to as public key. Digital signature provides integrity via a process called hashing. A hash also "encrypts" a message, but in this case, the goal is not confidentiality. A hash is a "non-invertible" or one-way function, which means that once a hash is performed on a message, you cannot get the original message back .Hash algorithm defined: a one-way "encryption" algorithm that takes a message of any length and produces a fixed length, unique output message. Sender encrypts the message digest using its own private key to produce digital signature. Following diagram shows the creation of digital signature.

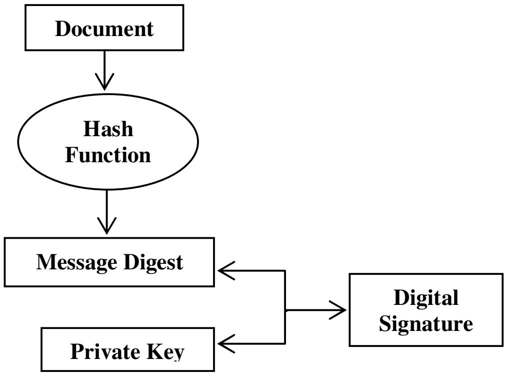

Figure 1: Creation of Digital Signature.

We have to put this digital signature on the document and then send it to receiver.

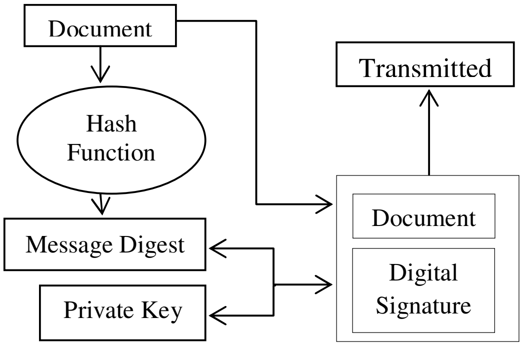

Figure 2: Transmission of Digital Signature

At receiver side the receiver then decrypt the signature using sender's public key and get the message digest. Receiver than apply hash function on document to generate the message digests. Than he will compare both the message digest, if both are same than message will be accepted otherwise rejected.

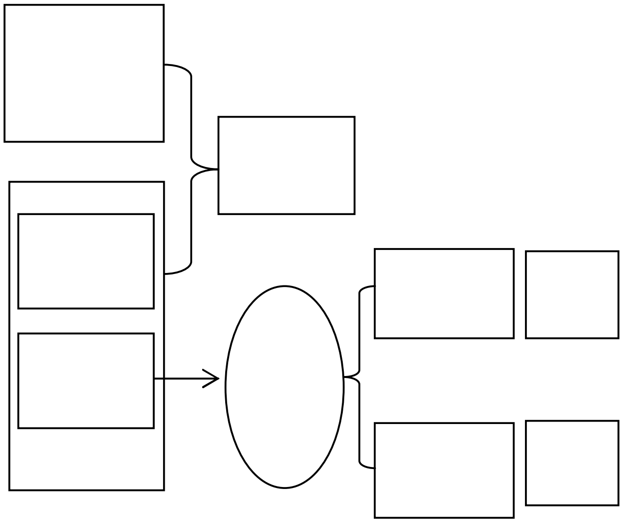

Figure 3: Decryption of Digital Signature at Receiver

The big computing workload slows down the computing speed of public key algorithm, so we can use secure one-way hash function to summarize the message so as to lessen the computing workload. Although asymmetric cryptography provides better security, but symmetric cryptography provides better performance.

Solution: use the symmetric key to encrypt and decrypt the data; use public and private keys to encrypt and decrypt the symmetric key.

Digital Envelope

Digital Envelope is a data container which is used to protect data over untrusted network. It 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. One of the problems of public-key encryption, it is slower than symmetric encryption. Here public-key encryption (RSA) is only used to encrypt the key, there is very little overhead [13].

II. RELATED WORK

In our work, we have studied 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. Digital envelope is most ensuring technique which provides key security feature like integrity, authentication, non-repudiation, privacy [1].

Wenping Guo, et al. "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.

Conventional digital envelope only ensures the confidentiality of the data, but due to the PKE it makes possible for the malicious user to destroy the data, so the integrity and non-repudiation of the data cannot be guaranteed. So the signed digital envelope is designed.

Communication data can meet the three indicators integrity, Confidentiality, Non- repudiation.

Diaa Salama, et al. "Studying the Effects of Most Common Encryption Algorithms", International Arab journal of e-Technology, Vol. 2-No. 1, Jan2011.According to author the performance of Blowfish algorithm is better than AES, DES, and 3DES, when tested on two different machines.

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].

Jawahar Thakur, et al. [9] presented a comparison between most common symmetric key cryptography algorithms: DES, AES, and Blowfish. The main concern of this work is to compare the performance of algorithms under different settings, the behaviour and the performance of the algorithm when different data loads are used. The comparison is made on the basis speed, block size, and key size.

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 smoothly works for small amount of data, blowfish uses variable length key, so that it is hard to break.

III. OBJECTIVE

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 RSA. 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 RSA 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 message.

IV. 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].

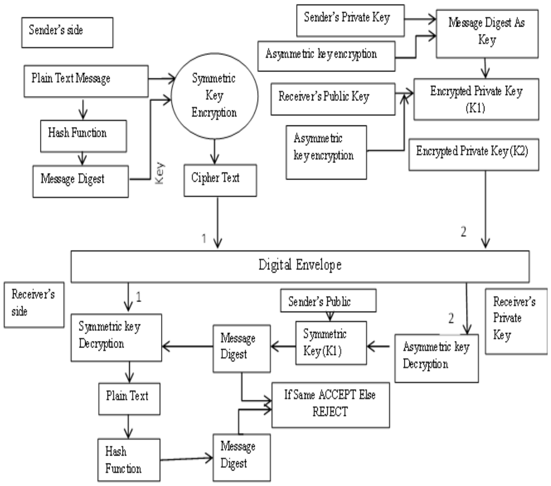

Figure 4: Digital Envelope Diagram

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. To achieve the confidentiality key is encrypted twice. Message digest is encrypted by sender's private key than we get encrypted symmetric key(K1), than K1 is encrypted by receiver's public key using RSA, than we get encrypted symmetric key K2 .

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.

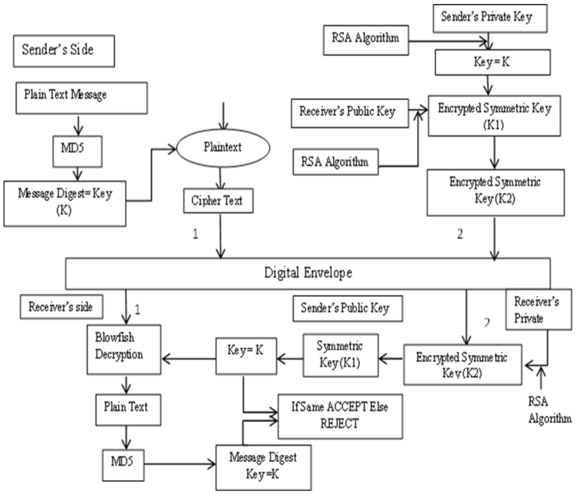

Figure 5: Digital Envelope Using Blowfish and RSA

The private key generation of the RSA, 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 RSA: First of all the system will accept Key and apply RSA encryption process on the key that will generate Symmetric key. Both cipher text and the encrypted key will send. Then on the decryption side it will get Cipher text and 128 bit key. Apply RSA 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.

VI. CONCLUSION AND FUTURE WORK

This paper purposes the digital envelope method to encrypt our data and to satisfy the rapidly growing need and to achieve security threats. Additionally, we have done comparative study of various algorithm for encrypting process, with going through many algorithms we have come up with blowfish algorithm as best among them. And then with the help of blowfish and RSA method we do the process of encryption .Now, to conclude we would say that in future much 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” International Journal of Network Security, Vol.11, No.3, PP.121 {127, Nov. 2010.

[2]. Rajasree R. S., “Generation of Dynamic Group Digital Signature” International Journal of Computer Applications (0975 - 8887) Volume 98 No.9.

[3]. Ashmi Singh, Puran Gour, Braj Bihari Soni , “Analysis of 64-bit RC5 Encryption Algorithm for Pipelined Architecture” International Journal of Computer Applications (0975 - 8887) Volume 96 No.20.

[4]. Akash Kumar Mandal, Chandra Prakash “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 (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]. Sultan Almuhammadi, “Better Privacy and Security in E-Commerce: Using Elliptic Curve- Based Zero- Knowledge Proofs”, ieeexplore.ieee.org/Xplore/home.jsp.

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

[17]. Atul Kahate (2008), “Cryptography and Network Security” McGraw Hill 2nd Edition.

[18]. M Gobi, “A New Digital Envelope Approach for Secure Electronic Medical Records”, IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.1. (January 2009).