HYBRID MODEL FOR SECURING E-COMMERCE TRANSACTION

Abdul Monem S. Rahma[1], Rabah N. Farhan[2], Hussam J. Mohammad[3]
[1]Computer science Dept. University of Technology, Iraq
[2 &3]Computer science Dept., College of Computer, Al-Anbar University, Iraq

ABSTRACT

The requirements for securing e-commerce transaction are privacy, authentication, integrity maintenance and non-repudiation. These are the crucial and significant issues in recent times for trade which are transacted over the internet through e-commerce channels. In this paper suggest cipher method that is improves the Diffie-Hellman key exchange by using truncated polynomial in discrete logarithm problem (DLP) to increases the complexity of this method over unsecured channel, also combines the hashing algorithm of MD5, the symmetric key algorithm of AES and the asymmetric key algorithm of Modification of Diffie-Hellman (MDH).

KEYWORDS: *key exchange, Securing E-commerce Transaction, Irreducible Polynomial*

I. INTRODUCTION

As an electronic commerce exponentially grows, the number of transactions and participants who use e-commerce applications has been rapidly increased. Since all the interactions among participants occur in an open network, there is a high risk for sensitive information to be leaked to unauthorized users. Since such insecurity is mainly created by the anonymous nature of interactions in e-commerce, sensitive transactions should be secured. However, cryptographic techniques used to secure ecommerce transactions usually demand significant computational time overheads, and complex interactions among participants highly require the usage of network bandwidth beyond the manageable limit [1].

Security problems on the Internet receive public attention, and the media carry stories of high-profile malicious attacks via the Internet against government, business, and academic sites [3]. Confidentiality, integrity, and authentication are needed. People need to be sure that their Internet communication is kept confidential. When the customers shop online, they need to be sure that the vendors are authentic. When the customers send their transactions request to their banks, they want to be certain that the integrity of the message is preserved [2].

From above discussions, it is clear that we must pay careful attention to security in E-commerce. Commonly, the exchange of data and information between the customers and the vendors and the bank must rely on personal computers that are available worldwide and based on central processing units (CPU) with 16-bit or 32-bit or 64-bit and operating systems that commonly used such as (windows) that running on the same computer. Communication security requires a period of time to exchange information and data between the customers and the vendors and the bank in such a way that no one can break this communication during this period. Irreducible truncated polynomial mathematics was adopted since 2000, which was developed for use in modern encryption methods, such as AES. Irreducible truncated polynomial mathematics we can use to build the proposed system because it is highly efficient and compatible with personal computers.

As a practical matter, secure E-commerce may come to mean the use of information security mechanisms to ensure the reliability of business transactions over insecure networks [4].

II. RELATED WORKS

In the following review, different methods were used in order to increase the e-commerce security:
Sung W. T, Yugyung L., and et al (2001) this research proposed an adaptive secure protocol to support secure e-commerce transactions. This adaptive Secure Protocol dynamically adapts the security level based on the nature and sensitivity of the interactions among participants. The security class incorporates the security level of cryptographic techniques with a degree of information sensitivity. It forms implements Adaptive Secure Protocol and measures the performance of Adaptive Secure Protocol. The experimental results show that the Adaptive Secure Protocol provides ecommerce transactions with high quality of security service [9].
Also **Ganesan R and Dr. K. Vivekanandan** (2009) proposed a software implementation of a digital envelope for a secure e-commerce channel that combines the hashing algorithm of MD5 for integrity, the symmetric key algorithm of AES and the asymmetric key algorithm of Hyperelliptic Curve Cryptography (HECC). The algorithm tested for various sizes of files. The digital envelope combining AES and HECC is the better alternative security mechanism for the secure e-commerce channel to achieve Privacy, Authentication, Integrity maintenance and Non-Repudiation [5].
Also **H. K. Pathak , Manju Sanghi [2010]** proposed a new public key cryptosystem and a Key Exchange Protocol based on the generalization of discrete logarithm problem using Non-abelian group of block upper triangular matrices of higher order. The proposed cryptosystem is efficient in producing keys of large sizes without the need of large primes. The security of both the systems relies on the difficulty of discrete logarithms over finite fields [6].

III. AES ALGORITHM

The Advanced Encryption Standard AES is a symmetric block cipher. It operates on 128-bit blocks of data. The algorithm can encrypt and decrypt blocks using secret keys. The key size can either be 128-bit, 192-bit, or 256-bit. The actual key size depends on the desired security level[57].
The algorithm consists of 10 rounds (when the key has 192 bits, 12 rounds are used, and when the key has 256 bits, 14 rounds are used). Each round has a round key, derived from the original key. There is also a 0th round key, which is the original key. The round starts with an input of 128 bits and produces an output of 128 bits. There are four basic steps, called layers that are used to form the rounds [8]:
The ByteSub Transformation (SB): This non-linear layer is for resistance to differential and linear cryptanalysis attacks.
The ShiftRow Transformation (SR): This linear mixing step causes diffusion of the bits over multiple rounds.
The MixColumn Transformation (MC): This layer has a purpose similar to ShiftRow.
AddRoundKey (ARK): The round key is XORed with the result of the above layer.

IV. BASICS OF MD5

MD5 (Message-Digest algorithm 5), is an Internet standard and is one of the widely used cryptographic hash function with a 128-bit message digest. This has been employed in a wide variety of security applications. The main MD5 algorithm operates on a 128-bit, divided into four 32-bit words [5].

V. MODIFICATION OF DIFFIE-HELLMAN (MDF)

The idea is improves the Diffie-Hellman key exchange by using truncated polynomial in discrete logarithm problem (DLP) to increases the complexity of this method over unsecured channel. The DLP of our cipher method is founded on polynomial arithmetic, whereas the elements of the finite filed G are represented in polynomial representations. The original DLP implies a prime number for its module operation, and the same technique is used in proposal method but considering an irreducible (prime) polynomial instead of an integer prime number. Before offering the method, we will offer Discrete Logarithm Problem (DLP) in polynomials

i. Discrete Logarithm Problem (DLP) in polynomials

In our method (DLP) involve raising an polynomial to an polynomial power, mod irreducible polynomial .The algorithm to compute $(F(a))^{F(x)} \bmod F(g)$ offer as following :
Where:
F (a) = polynomial value, F (x) = polynomial value. F (g) = irreducible polynomial value.

ii. The solution steps for this method

Algorithm 1: Modular Exponentiation Algorithm in Polynomial.

Input: $F(a)^{F(x)} \bmod F(g)$.
Output: F (z) = Value in polynomial .

Process:

Step1: Convert the F(x) to binary and put the value in K as

Kn , Kn-1 , Kn-2 , ... k0 .

Step2: Select F (z) polynomial variable first equal to one

F (z) = 1 .

Step3: apply following

For i = n down to 0

F (z) = F (z) ⊗ F (z) mod F(g)

If Ki = 1 then

F (z) = F (z) ⊗ F (a) mod F(g)

Step4**:** return F (z)

Step5: End.

We suppose there are two sides want to exchange key (Client and Server) the Client side encrypt message and Server side decrypt its, as following:

1. Key generation

There are two publicly known numbers: irreducible polynomial *F(p)* and a polynomial value F(a) that is a primitive root of *F(p).*

Client Side

The client side select a random polynomial value F(*X*C) < *F(p)* and computes:
F(YC)= $(F(a))^{F(XC)}$ mod *F(p)*……..(1)
Server Side
The server side select a random polynomial value F(*X*S) < *F(p)* and computes:
F(YS)= $(F(a))^{F(XS)}$ mod *F(p)* …….. (2)
Each side keeps the F(*X*) value private and makes the *F(Y)* value available publicly to the other side.
Client Side
The client side compute shared key by return the *F(YS)* from server side :
Key = $(F(Ys))^{F(XC)}$ mod *F(p)* …….. (3)
Server Side
The server side compute shared key by return the *F (Yc)* from client side :
Key =$(F(YC))^{F(XS)}$ mod *F(p)* …….. (4)
Now the two sides have same Secret key (SK):
$SK = (F(a))^{F(XS) \otimes F(XC)} \bmod F(p)$ …….. (5)

2. Encryption Message

To encrypt the message firstly convert each letter from message to polynomial, secondly apply the following equation to find cipher (C):

Ci = (Mi □ Sk) mod F(*g*) …….. (6)

3. Decryption Message

To decrypt message firstly compute the multiplicative inverse for secret key (Sk'), secondly apply the following equation to find message:

Mi = (Ci □□Sk') mod F (g) …….. (7)

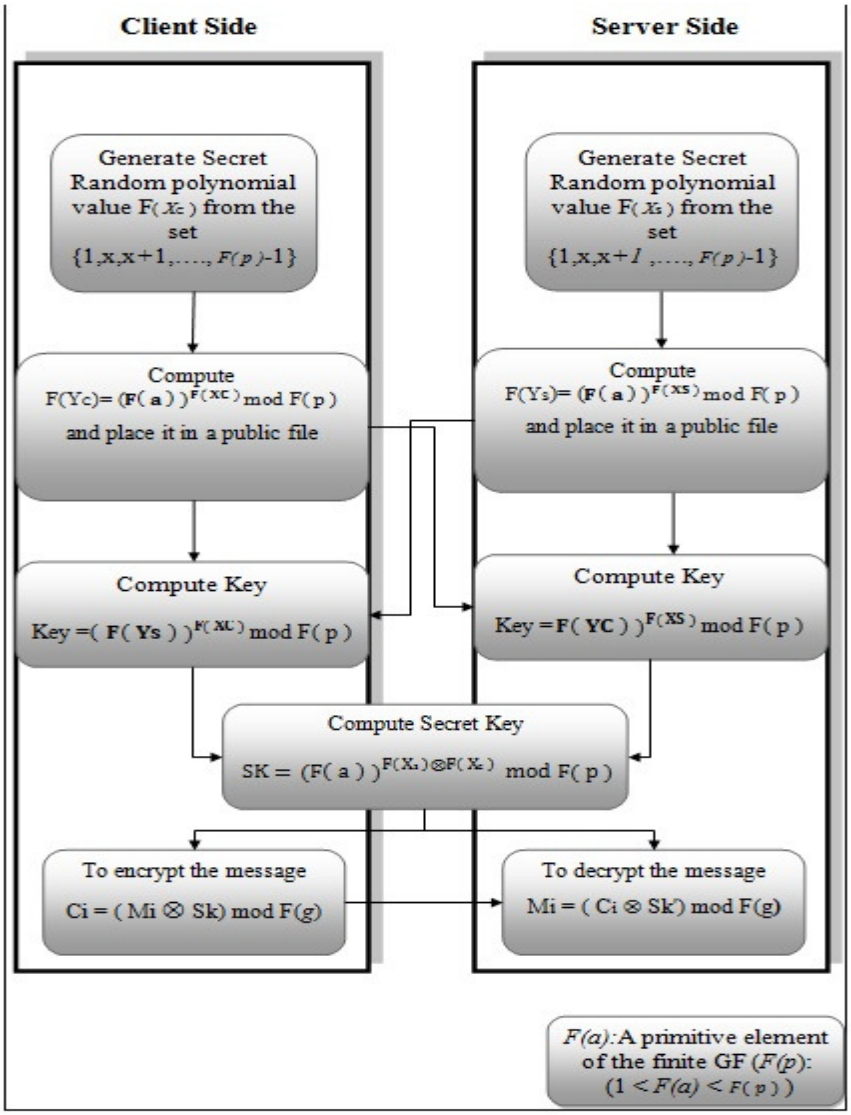

Figure (1): Modification of Diffie Hellman (MDF)

VI. IMPLEMENTATION DETAILS

We present here combines the best features of both symmetric and asymmetric encryption techniques. The data (plain text) that is to be transmitted is encrypted using the AES algorithm. The data (plain text) used input to MD5 to generate AES key. This key encrypted by using modification of diffie-hellman (MDF). The using of MD5 useful in two directions, firstly to ensure integrity of the data that is transmitted, secondly to easy generate secret key that used in AES algorithm. Thus the client sends cipher text of the message, and ciphertext of the AES key also it's represent ciphertext of the message

digest. The server upon receiving ciphertext of the message, and ciphertext of the AES key. First decrypts the Ciphertext of the AES key by (MDH) to obtain the AES key. This is then used to decrypt the cipher text of the message by AES decryption to obtain the plain text. The plaintext is again subjected to MD5 hash algorithm to compare with decrypted message digest to ensure integrity of data.

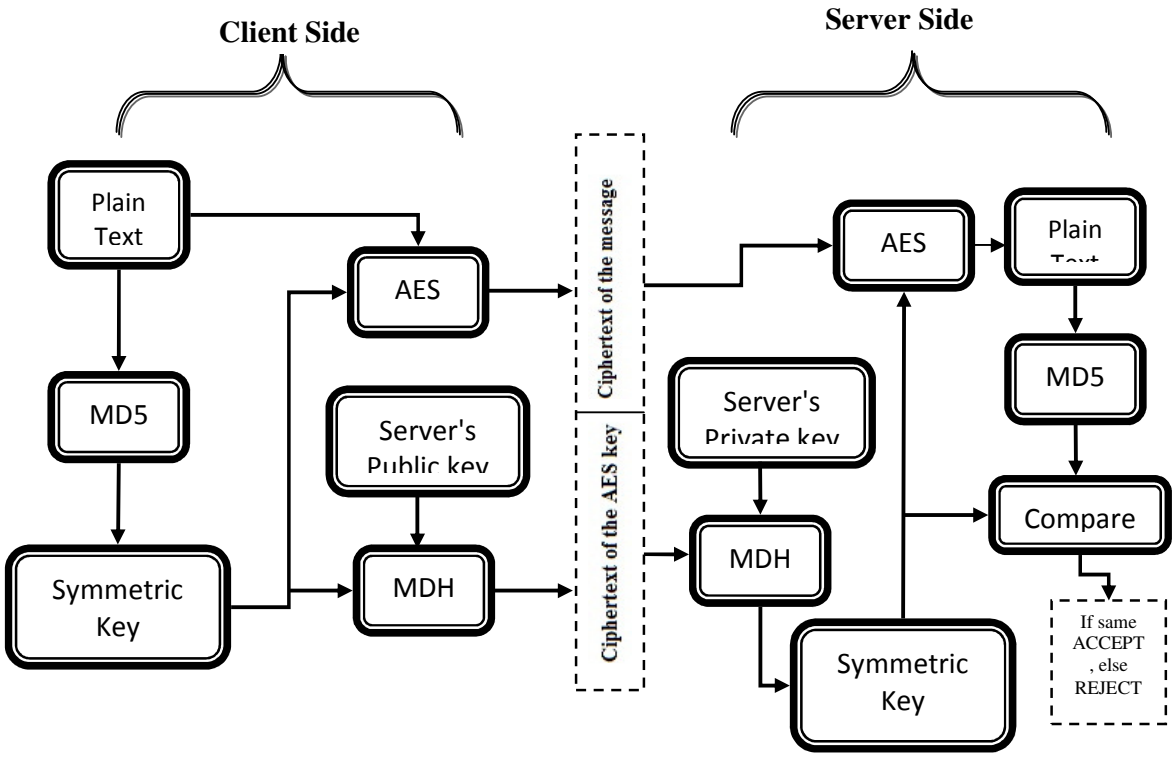

Figure (1): implementation details of model

VII. RESULTS

The hybrid algorithm execute on PC computer of CPU Intel Pentium 4 2.2 MHz Dual Core 2. The programs implemented using Microsoft Visual Studio 2008 (C#). It's tested with three messages different in length (1000 char, 3000 char, 5000 char) .The key sizes that used for AES (128 bit) .the table 1 provides details on the time taken for encryption, decryption for (AES,MDH) and Calculation of MD5 Message Digest.

Table 1: Time in (Second: Milliseconds) for AES, MDH Encryption and Decryption and Calculation of MD5 Message Digest

Message length	AES Enc	AES Dec	MDH Enc	MDH Dec	MD5
1000 char	0:30	0:17	0:700	0:500	0:20
3000 char	0:93	0:62	1: 500	1: 300	0:35
5000 char	0:187	0:109	2:800	2:400	0:52

VIII. ANALYSIS

With any cryptographic system dealing with 128 bit key, the total number of combination is 2^{128}.

The time required to check all possible combinations at the rate of rate 50 billion keys / second is approximately (5 * 10^{21}) years thus AES is very strong and efficiency to used in e-commerce .

Randomness of Modification of Diffie-Hellman (MDH) is very high whatever the irreducible polynomial because the result is always unexpected, also the complexity is always complex because it depends on irreducible truncated polynomial.

IX. CONCLUSION

Satisfying security requirements is one of the most important goals for e-commerce system security designers; in this paper we give the protocol design for securing e-commerce transaction by using hybrid encryption technique. This hybrid encryption method surely will increase the performance of cryptographic algorithms. This protocol will ensure the confidentiality, integrity and authentication. The AES algorithm provides confidentiality, the MD5 hash function provides the integrity and the modification of Diffie-Hellman will ensure the authentication. We have tested the algorithm for various sizes of messages. The experimental results showed that the model be improved the interacting performance, while providing high quality of security service for desired e-commerce transactions.

REFERENCE

[1] Sung W. T., Yugyung L., Eun K. P., and Jerry S. ," Design and Evaluation of Adaptive Secure Protocol for E-Commerce " , 0-7803-7128-3/01/$10.00 (C) | 2001 IEEE.
[2] Abeer T. Al-Obaidy , " Security Techniques for E-Commerce Websites ", Ph. Thesis, The Department of Computer Science , University of Technology, 2010.
[3] Oppliger R.,"Security Technologies for the World Wide Web, Second Edition", Library of Congress, © ARTECH HOUSE, Inc., USA, 2003.
[4] Wooseok Ham, “Design of Secure and Efficient E-commerce Protocols Using Cryptographic Primitives", MSc. Thesis , School of Engineering , Information and Communications University 2003.
[5] Ganesan R. , Dr. Vivekanandan K., " A Novel Hybrid Security Model for E-Commerce Channel" , © 2009 IEEE.
[6] Pathak H. K. , Manju S. , " Public key cryptosystem and a key exchange protocol using tools of non-abelian group" , (IJCSE) International Journal on Computer Science and Engineering , Vol. 02, No. 04, 2010 .
[7] Oswald E., " Encrypt: State of the Art in Hardware Architectures", Information Society Technologies, UK, 2005.
[8] Trappe W., Washington L.,"Introduction to Cryptography with Coding Theory, Second Edition", ©Pearson Education, Inc. Pearson Prentice Hall, USA, 2006.
[9] Sung W. T., Yugyung L., et al," Design and Evaluation of Adaptive Secure Protocol for E-Commerce”, , © IEEE, 2005.

Authors

Abdul Monem Saleh Rahma awarded his MSc from Brunel University and his PhD from Loughborough University of technology United Kingdom in 1982, 1985 respectively. He taught at Baghdad university department of computer science and the Military Collage of Engineering, computer engineering department from 1986 till 2003.He fills the position of Dean Asst. of the scientific affairs and works as a professor at the University of Technology Computer Science Department .He published 82 Papers in the field of computer science and supervised 24 PhD and 57 MSc students. His research interests include Cryptography, Computer Security, Biometrics, image processing, and Computer graphics. And he Attended and Submitted in many Scientific Global Conferences in Iraq and Many other countries.

Rabah Nory Farhan has received Bachelor Degree in Computer Science, Almustanseria University, 1993, High Diploma in Data Security/Computer Science, University of Technology, 1998. Master Degree in Computer Science, University of Technology, 2000.PHD Degree in Computer Science, University of Technology, 2006. Undergraduate

Computer Science Lecturer, University of Technology, 2002 to 2006. Undergraduate and postgraduate Computer Science Lecturer, Graduate Advisor, Computer College, University of Al-Anbar, 2006 -till now.

Hussam Jasim Mohammed Al-Fahdawi has received B.Sc in Computer Science, Al-Anbar University, Iraq, (2005-2009). M.Sc student (2010- tell now) in Computer Science Department, Al-Anabar University. Fields of interest: E-Commerce Security, cryptography and related fields. Al-Fahdawi taught many subjects such as operation system, computer vision, image processing.