HYBRID MODEL FOR SECURING E-COMMERCE TRANSACTION

Sidraah Matte, Anoop Dubey, Nilkanth shirsat, Prof. Dr. Anil Kale

Abstract- in today's world the requirement for securing e-commerce is on a great demand. It includes the e-commerce transaction's privacy, authentication, maintenance of its integrity and non-repudiation. These are very critical issues in today's time for trade which is taken over the internet through the means called e-commerce. This paper contains of various methods called as the Cipher method that improves the Diffie-Hellman key exchange by using truncated polynomial in discrete logarithm problem (DLP) that increases the security of the e-commerce transaction that takes over the internet. It also contains algorithms such as the MD5, and AES. MD5 is the asymmetric key algorithm and AES is symmetric key algorithm.

Index Terms — key exchange, securing e-commerce transaction.

1 INTRODUCTION

In today's highly digital world the use of e-commerce and its trade occurring on e-commerce has highly increased. This has made an exponential growth in trade and the number of transactions and participants are highly increased. Since all this occur over an open network there is a high risk of sensitive information to be leaked. In order to avoid such circumstances these three algorithms are used to encrypt the sensitive information of the users which cannot be easily or we can say impossible to access.

Over the internet there are various malicious attacks taking place over e-commerce trading site against the government policies. So in order to avoid such situations these powerful algorithms such as AES, MD5 and Diffie- Hellman are used for encryption.

Communication security requires a period of time to exchange information and no one can break this communication during this period.

2 PURPOSES, SCOPE AND APPLICABILIY

2.1 Purpose

In the following review, different methods were used in order to increase the e-commerce security:

Sung W. T., Yuggung L., proposed this research as an adaptive secure protocol to support and secure e-commerce transactions. This adaptive secure protocol dynamically adapts the security levels based on the nature and sensitivity of the interactions among the participants. The security class incorporates the security level of cryptographic techniques with a degree of information sensitivity. It forms and implements adaptive secure protocol and measure the performance of adaptive secure protocol. The experimental results show that the adaptive secure protocol provides e-commerce transaction with high quality of security.

Using truncated polynomial in discrete logarithmic problem (DLP) to increase the complexity of this method over unsecured channel.

Also Ganesan R proposed software implementations of digital envelope for a secure e-commerce channel that combines the hashing algorithm of MD5 for integrity.

Also H. K. Pathak, Manju Sanghi proposed a new public key cryptosystem and a key exchange protocol based on the generalization logarithmic problem.

2.2 Scope

We present both the symmetric and asymmetric encryption techniques. The data plain text that is to be transmitted is encrypted using the AES algorithm. The data that is to be transmitted, secondly to easy generate secret key that is used in AES algorithm.

2.3 APPLICABILITY

Key Generation: There are two publicly known numbers: Irreducible polynomial f(p) and a polynomial value F(a) that is primitive root of F(p).

Client side: The client side select a random polynomial value f(xc) < f(p) and computer.

f(yc) = (f(a) mod f(P).

Server side:

The server side select a random polynomial value.f(xs)<f(p) and computes: F(ys)=(f(a) mod f(p)Each side makes the f(x) value private and makes the f(y) value available publicly to the other side.

3 EQUATIONS

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.

Modifications of Diffie-Hellman (MDF)

The idea is to improve the Diffie-Hellman key exchange by using truncated polynomial in discrete logarithmic problem (DLP) to increase the complexity of this method over unsecured channel.

Sections

We present both the symmetric and asymmetric encryption

techniques. The data plain text that is to be transmitted is encrypted using the AES algorithm. The data that is to be transmitted, secondly to easy generate secret key that is used in AES algorithm.
Key Generation: There are two publicly known numbers: Irreducible polynomial f(p) and a polynomial value F(a) that is primitive root of F(p).
Client side: The client side select a random polynomial value f(xc)<f(p) and computer.
f(yc)=(f(a) mod f(P).
Server side:
The server side select a random polynomial value.f(xs)<f(p) and computes:
F(ys)=(f(a) mod f(p)
Each side makes the f(x) value private and makes the f(y) value available publicly to the other side.

.

4 Objectives

AES Algorithm: The Advanced Encrytion Algorithm 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-bits. The actual key size depends on the desired security level.
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.
Modifications of Diffie-Hellman(MDF)
The idea is to improve the Diffie-Hellman key exchange by using truncated polynomial in discrete logarithmic problem (DLP) to increase the complexity of this method over unsecured channel.

5 End Sections

5.1 Appendices

With any cryptographic system dealing with 128 bit key, the total no. of combination is 2*128. The minimum required to check the possible combinations at the rate of 50 billion key/second is approximately (5*10) years thus AES is very atrong and efficient to use in e-commerce.

5.2 Acknowledgments

Sung W. T., Yuggung L., proposed this research as an adptive secure protocol to support and secure e-commerce transactions. This adaptive secure protocol dynamically adapts the security levels based on the nature and sensitivity of the interactions among the participants. The security class incorporates the security level of cryptographic techniques with a degree of information sensitivity. It forms and implements adaptive secure protocol and measure the performance of adaptive secure protocol. The experimental results show that the adaptive secure protocol provides e-commerce transaction with high quality of security.
Also Ganesan R proposed software implementations of digital envelope for a secure e-commerce channel that combines the hashing algorithm of MD5 for integrity.
Also H. K. Pathak, Manju Sanghi proposed a new public key cryptosystem and a key exchange protocol based on the generalization logarithmic problem.

6 Conclusion

Although a conclusion may review the main points of the paper, do not replicate the abstract as the conclusion. A conclusion might elaborate on the importance of the work or suggest applications and extensions. Authors are strongly encouraged not to call out multiple figures or tables in the conclusion—these should be referenced in the body of the paper.

Acknowledgment

The authors wish to thank A, B, C. This work was supported in part by a grant from XYZ.

References

[1] Sung. W. T., Yuggung L., Eun K. P., and Jerry S., designed and evolution of Adaptive Secure Protocol for e-commerce.
[2] Ganesan R., Dr. Vivekannada K.,"A Novel Hybrid Security Model for e-commerce channel.
[3] Pathak H.K., Manju S., "Public key cryptosystem and a key exchange protocol.