Issue 1 vol 4 ISSN: 2321-8134

IJFEAT

INTERNATIONAL JOURNAL FOR ENGINEERING APPLICATIONS AND TECHNOLOGY

E-COMMERCE TRANSACTION USING HYBRID ENCRYPTION

Mr. Shankar V. Chavhan[1], Miss. Mayuri P. Solanke[2], Miss. Pooja B. Pund[3], Miss. Rutuja S. Lonkhande[4]

Prof. Satish L. Thombare[5]

[1]*Student, Information Technology Department, J.D.I.E.T. Yavatmal, Maharashtra, India,*
nilchavhan1996@gmail.com
[2]*Student, Information Technology Department, J.D.I.E.T Yavatmal, Maharashtra, India,*
mahisolankepatil99@gmail.com
[3]*Student, Information Technology Department, J.D.I.E.T Yavatmal, Maharashtra, India,*
poojap3398@gmail.com
[4]*Student, Information Technology Department, J.D.I.E.T Yavatmal, Maharashtra, India,*
ruttuja8308@gmail.com
[5]*Prof, Information Technology Department, J.D.I.E.T. Yavatmal, Maharashtra, India,*
satishthombare@gmail.com

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 shank algorithm and AES is symmetric key algorithm.

Index Terms: *Key exchange, Secure e-commerce transaction.*

---------- *** ----------

1. Introduction

E-commerce is an important topic in dealing with the security issues. Its core research area is its way of protecting the security of e-commerce system and data. Transaction records, commercial transactions, user account, market scheme and others are the sensitive financial data and assets in the e-commerce database. The parties involved in e-commerce are needed to be assured of security of their data transactions completely. As in the transactions there is always a threat of third party hack. So we need a secure transaction with maintaining speed and efficiency. However a simple encryption technology, such as symmetrical encryption or asymmetrical encryption, is very difficult to guarantee the security of network transactions. We must combine both of these and through hybrid encryption we can create a safe, efficient ecommerce transaction mechanism.

Communication or computer networks are undergoing a fast development in various fields of applications like Information technology, business, e-commerce, medical applications etc. Even more, wireless sensor networks targets the applications

like temperature sensing, destruction estimation, military and many others where human support is required only at remote console. Whatever is the communication scenario, wired locally or wireless geographically, or sensor nodes at remote location, it involves the source, receiver and a channel.

2. Literature survey

The proposed work ensures high security level of ATM banking transaction. We chose ATM network as an example of communication networks as this involves the ATM banking machine as client which communicates to the banking server through high optic communication link. RSA algorithm involves mathematical function which adds on the security access in the process . Symmetric cryptography technique is easy to implement, less computation steps involved, mathematical complexity is less and is a fast in processing. For applications where not a high security measure is involved, we can select symmetric cryptography method of encryption and decryption. But, this method involves simple mathematical operation, same key is used at both encryption and decryption process. So there is every chance for a brute force or trial out attack to receive the key and thereby the encryption and decryption step. This makes the security of the communication network in threat of fraudulent attack. In asymmetric or public key cryptography, such as RSA algorithm, there is a high security check mechanism involved as it involves mathematical foundations and number theory and field facto to decide the corresponding encryption and decryption process. It involves two keys, both public and private key to get the plaintext or message from source to receiver. Even though an intruder tried for a brute force or other cryptanalysis method, it is very difficult to receive the public and private keys and also secondary keys generated which send to the customer mobile phone to complete the transactions.

In the research work, we combine both symmetric and asymmetric methods. It is not just two security level checks. It involves secondary key generations at each level. When, ATM card inserted, ATM Pin number entered and that follows a first level security check by entering the customer specific pin provided by the bank to the customer. Then, proceed to the second level RSA security check using secondary pin. Again, final security code generated and sends to the mobile after successful completion of RSA algorithm security level check point. If all the three steps completed successfully then only the user will get an access into the ATM communication network transactions.

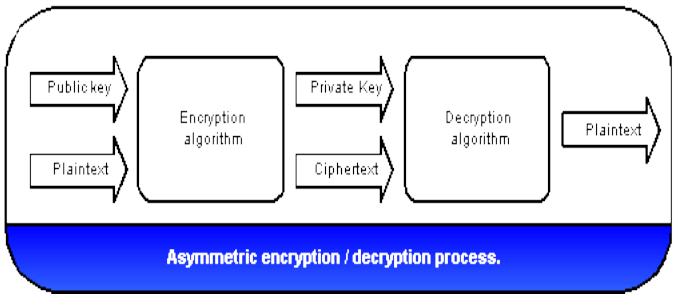
The future scope of this research work is to investigate and establishes other public cryptography techniques and porting this Mat lab based tool into hardware. Research on existing security attacks and the reliability of this tool can be measured.

3. Encryption Technique

Encryption is the process of converting a plaintext message into ciphertext which can be decoded back into the original message. An encryption algorithm along with a shank is used in the encryption and decryption of data. There are various types of data encryptions which form the basis of network security. Encryption schemes are based on block or blow ciphers.

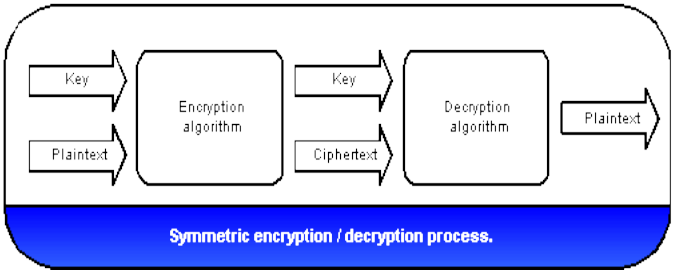
3.1 Asymmetric Encryption Technique

A modern sector of cryptography. also known as public-key cryptography in which the algorithms employ a combination of keys (a public key and a private key) and use a different component of the pair for different steps of the algorithm.



3.2 Symmetric Encryption Technique

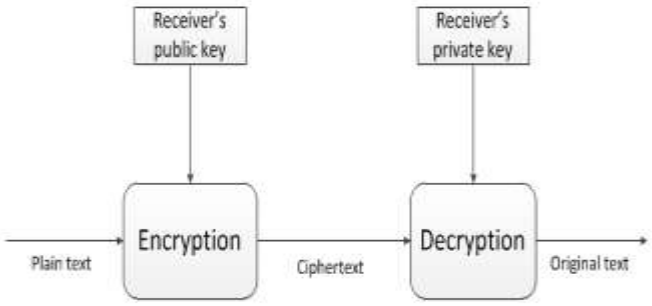
The encryption key and the decryption shank are interrelated and may even be the same.



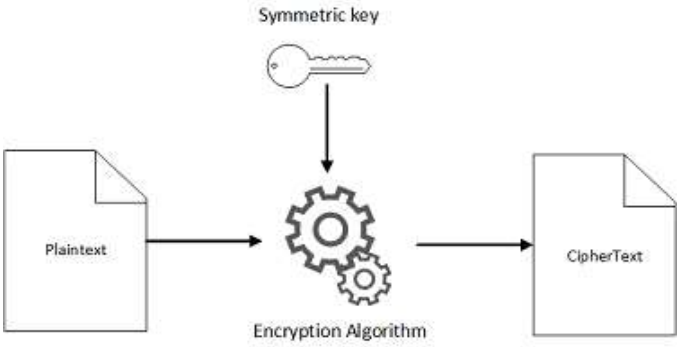
4. Cryptography Technique

Cryptography involves creating written or generated codes that allow information to be kept secret. Cryptography deals with the actual securing of digital datum. It refers to the design of go ahead based on mathematical algorithms that provide fundamental information security services. You can think of cryptography as the installation of a large toolkit containing different techniques in security applications.

4.1 Asymmetric Cryptography Technique



4.2 Symmetric Cryptography Technique



5. Algorithm

5.1 RSA

The two most widely used public key algorithms are RAS and Diffie-Hellman. In 1978, a group at MIT discovered a strong method for public key encryption it is known as RSA, the derived from the initials of three discovers Ron Rivest, Adi Shamir, Leonard Adleman.

RSA cryptosystem is the most widely accepted asymmetric key algorithm in fact most of the practically implemented security systems are based on RSA.

The algorithm requires keys of at least 1024 bits for good security. This algorithm is based on some principles from number theory, which states that determining the prime factors of a large number is extremely difficult.

Steps of RSA Algorithm

Step 1: Consider the two large prime number said as p and q these for security purpose reason.

Step 2: Calculate n=p*q

Step 3: Calculate $\Phi(n) = (p-1)(q-1)$

Step 4: Assume e such that $\gcd(\Phi(n), e) = 1; 1 < e < \Phi(n)$

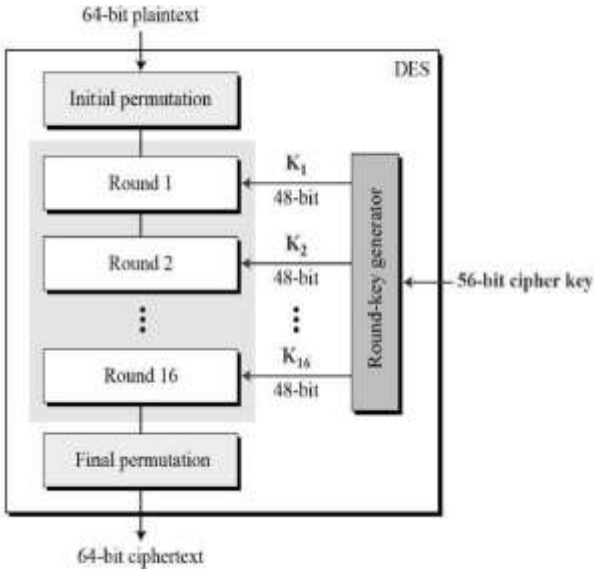
Step 5: Assume d such that $de \bmod \Phi(n) = 1$

Step 6: Public key KU = {e,n}

Step 7: Private key KR = {d,n}

5.2 DES

The Data Encryption Standard (DES) is a symmetric-shank block cipher published by the National Institute of Standards and Technology (NIST). DES is an implementation of a Feistel Cipher. It uses 16 round Feistel structure. The block size is 64-bit. Though, key length is 64-bit, DES has an effective key length of 56 bits, since 8 of the 64 bits of the key are not used by the encryption algorithm (function as check bits only). Common Structure of DES is depicted in the following illustration.



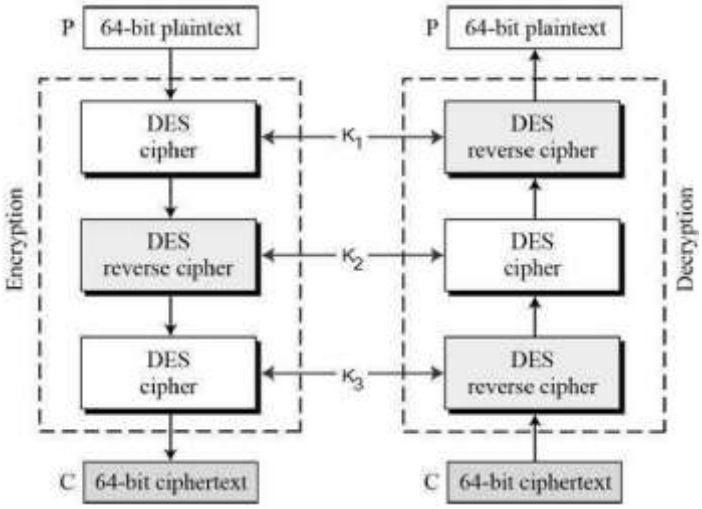
5.3 Triple DES

The speed of exhaustive shank searches against DES after 1990 began to cause discomfort amongst users of DES. However, users did not want to prepare DES as it takes an enormous amount of time and money to change encryption algorithms that are widely adopted and embedded in large security architectures.

The pragmatic approach was not to abandon the DES completely, but to change the manner in which DES used. This led to the modified schemes of Triple DES (sometimes known as 3DES). Incidentally, there are two variants of Triple DES known as 3-shankTriple DES (3TDES) and 2-key Triple DES (2TDES).

3-KEY Triple DES

Before using 3TDES, user first generate and distribute a 3TDES key K, which consists of three different DES keys K_1, K_2 and K_3. This means that the real 3TDES key has length 3×56 = 168 bits. The encryption scheme is illustrated as follows.



The encryption-decryption process is as follows

- Encrypt the plaintext blocks using single DES with key K_1.
- Now decrypt the output of step 1 using single DES with key K_2.
- Finally, encrypt the output of step 2 using single DES with key K_3.
- The output of step 3 is the cyphertext.
- Decryption of a cyphertext is a reverse process. User first decrypt using K_3, then encrypt with K_2, and finally decrypt with K_1.

Due to this design of Triple DES as an encrypt–decrypt–encrypt process, it is possible to use a 3TDES (hardware) implementation for single DES by setting K_1, K_2, and K_3 to be the same value. This provides backwards compatibility with DES.

Second variant of Triple DES (2TDES) is similar to 3TDES except that $K_3$is replaced by K_1. In other words, user encrypt plaintext blocks with shank K_1, then decrypt with key K_2, and finally encrypt with K_1 again. Therefore, 2TDES has a shank length of 112 bits.

Triple DES systems are significantly reliable than single DES, but these are emphatically a much slower process than encryption using single DES.

6. Future Scope

Every organization has a huge amount of confidential data. This security of this data is the primary concern for the existence of any organization. No organization can afford the loss of even a small part of its data. It may result in a loss of millions or billions of money. Nearly 80% budget of IT companies is spent on Information security. Data can never be said to be 100% secure. Each time a new security mechanism is developed, its cracks also get developed after some time. So the security mechanisms can be compared to passwords which need to be changed time to time. Security Mechanisms must be upgraded after a short span of time in order to avoid loss of confidential data and harsh consequences thereafter.

References

[1] Ziff Davis, "E-Commerce." Software World, 2003, vol. 30, pp. 207212.

[2]https://academic.csuohio.edu/yuc/security/Chapter_06_Data_Encription_Standard.pdf

[3]https://www.google.com/search?q=ecoomerce+transaction+using+hybrid+encryption+abstract&rlz=1C1CHBF_enIN723IN728&oq=ecoomerce+transaction+using+hybrid+encryption+abstract&aqs=chrome..69i57.23471j1j7&sourceid=chrome&ie=UTF-8

[4]http://ijcset.net/docs/Volumes/volume5issue7/ijcset20150507 10.pdf