Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 7, July 2014, pg.499 – 505

RESEARCH ARTICLE

Implementation of a Protocol for Secure E-Commerce Transactions

Arvind Tudigani, Lahari .D

[1] University College of Science, Saifabad (UCSS), OU, Hyderabad, Telangana, India
[2] PGRRCDE, OU, Hyderabad, Telangana, India

[1] mr.arvind@rediff.com; [2] lahari22@gmail.com

Abstract-- In today's fast moving age, most of the individuals want all things to happen easily and quickly, which led tremendous developments is the fields of communication technology and E-Commerce domain which holds a major impact on today's business. One of the major concerns now a days is the security of data being exchanged among the desired clients. Third party intervention has lead to new developments in the field of security specially related to networks like internet which are at a great risk.

When the data is over the network there are more chances of attack. It is desired to communicate data with high security keeping these requirements in mind we propose to design a new security protocol using a combination of symmetric and asymmetric techniques to provide security to E-Commerce transactions. This protocol provides three cryptographic primitives – Authentication, Integrity and Confidentiality using AES-Rijndael for encryption, public key cryptography (RSA) for authentication and RIPEMD-160 to check for integrity as well as checks for the authenticity of the data being received.

At present, various types of cryptographic algorithms provide high security to information on controlled networks. These algorithms are required to provide data security and users authenticity. A new security protocol is proposed for better security using a hybrid cryptographic scheme.

Keywords: - Security, Encryption, Hybrid Cryptography, Symmetric and Asymmetric Algorithms, Authentication and Integrity

I. INTRODUCTION

The Internet has become a global marketplace for goods and services. For e-commerce to prosper, you must feel safe when transmitting credit card and other financial information. But data traveling over a network presents an opportunity for some to intercept confidential information.

Let us say you want to buy some merchandise from an online store. If you provide your credit card number and other financial information, how would you know that this information will travel safely from your computer to the destination computer? This can be done by using a technology called encryption. Encryption software encrypts data with a secret code so that no one can make sense of it while it's being

transmitted. When the data reaches its destination, the same software decrypts the information.
Various algorithms are used to secure the data transfer amongst two clients. Symmetric and asymmetric algorithms are frequently used to secure the messages.

In our project we are developing a new security protocol using a combination of Symmetric and asymmetric algorithms to impart maximum security to the transactions like internet shopping where private information like passwords and credit card numbers are exchanged amongst the clients. Symmetric algorithms like AES use a single private key to encrypt a well as to decrypt the message. Asymmetric algorithms like RSA use two different types of keys public as well as private keys to encrypt. We also use the RIPEMD-160 algorithm for hash code calculation that helps to add a signature to the system to ensure tamper free data transfer.

With this project our main motive is to attain all the three primitives of cryptography i.e. Authentication, confidentiality and Integrity with the wise combination of algorithms in one single protocol.

II. OVERVIEW OF THE ALGORITHMS

A. *AES Algorithm*

AES is the Advanced Encryption Standard, a United States government standard algorithm for encrypting and decrypting data. AES is a symmetric block cipher with a block size of 128 bits. Key lengths can be 128 bits, 192 bits or 256 bits.AES-128 uses 10 rounds, AES-192 uses 12
Rounds, AES-256 uses 14 rounds.
The main loop of AES performs the following functions:

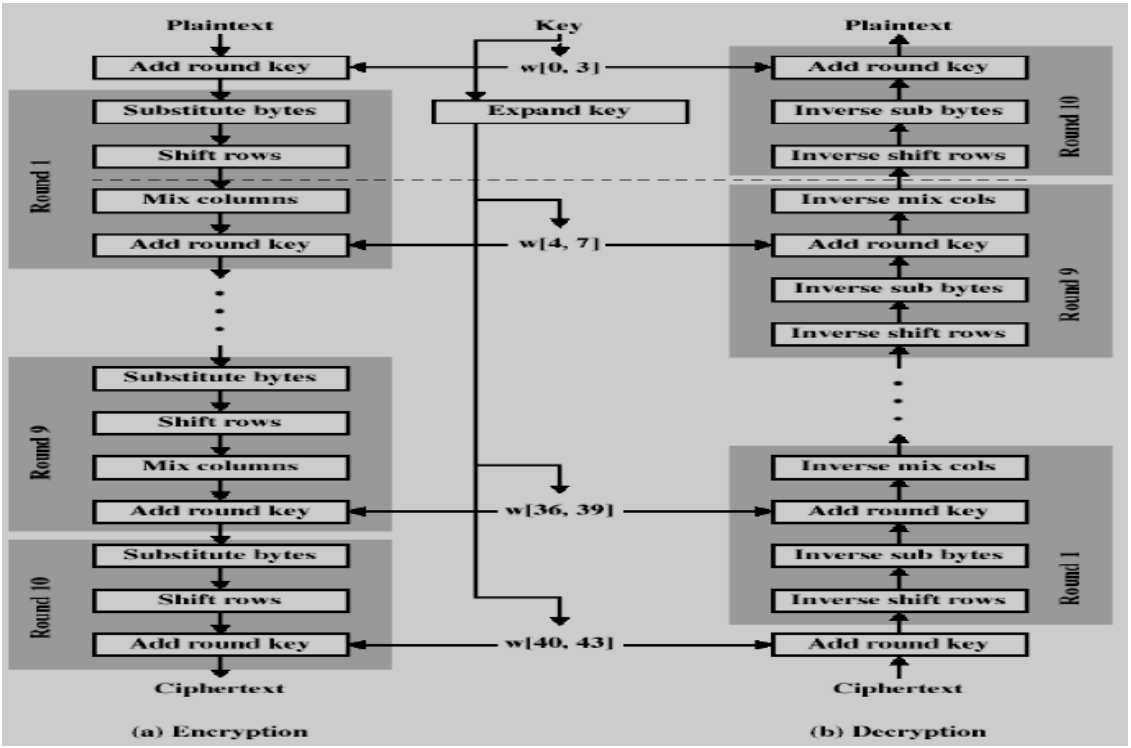

Fig.1 Showing AES Rounds

1) SubBytes(): SubBytes() adds confusion by processing each byte through an S-Box. An S-Box is a substitution table, where one byte is substituted for another, based on a substitution algorithm.

2) ShiftRows(): ShiftRows() provides diffusion by mixing data within rows. Row zero of the State is not shifted, row 1 is shifted 1 byte, row 2 is shifted 2 bytes, and row 3 is shifted 3 bytes.

3) MixColumns(): MixColumns() also provides diffusion by mixing data within columns. The 4 bytes of each column in the State are treated as a 4-byte number and transformed to another 4-byte number via finite field mathematics.

4) AddRoundKey(): The actual 'encryption' is performed in the AddRoundKey() function, when each byte in the State is XORed with the subkey. The subkey is derived from the key according to a key expansion schedule.

B. RS Algorithm

"In cryptology, RSA is an algorithm for public-key encryption. It was the first algorithm known to be suitable for signing as well as encryption, and one of the first great advances in public key cryptography. RSA is still widely used in electronic commerce protocols, and is believed to be secure given sufficiently long keys and the use of up-to-date implementations.

RSA is used in security protocols such as:

- IPSEC/IKE - IP data security
- TLS/SSL - transport data security (web)
- PGP - email security
- SSH - terminal connection security
- SILC - conferencing service security

RSA gets its security from *factorization problem*. Difficulty of *factoring* large numbers is the basis of security of RSA. Over 1000 bits long numbers are used.
Integer factorization problem (finding number's prime factors):
Positive integer *n*, find its prime factors: $n = p1\ p2 \ldots pi$ where *pi* is positive distinct prime number.
Example: $257603 = 41 * 61 * 103$
Factorization algorithms can be used (attempted at least) to factor faster than brute forcing.

C.RIPEMD-160 Algorithm

RIPEMD-160 (RACE Integrity Primitives Evaluation Message Digest) is a 160 bit message digest algorithm (and cryptographic hash function) was developed under the European RACE Integrity Primitives Evaluation (RIPE) project by a group of researchers that launched partially successive attacks on MD4 and MD5.

RIPEMD-160 Logic:
The algorithm takes as input a message of arbitrary length and produces as output a 160-bit message digest. The input is processed in 512 bit blocks.

The process consists of the following steps:

1) Step1: Append padding bit: the message is padded so that its length is congruent to 448 modulo 512 (length = 448 mod 512). Padding is always added even if the message is already of the desired length. Thus the number of padding bits is in the range of 1 to 512.the padding consists of a single 1-bit followed by the necessary number of 0-bits.

2) Step-2: Append length: A block of 64 bits is appended to the message. This block is treated as an unsigned 64-bit integer and contains the length of the original message.

3) Step-3: Initialize MD buffer: A 160-bit buffer is used to hold intermediate and final results of the hash function. The buffer can be represented as five 32-bit registers (A,B,C,D,E). These registers are initialized to hexadecimal values (67452301, efcdab89, 98badcfe, 10325476, c3d2e1f0).

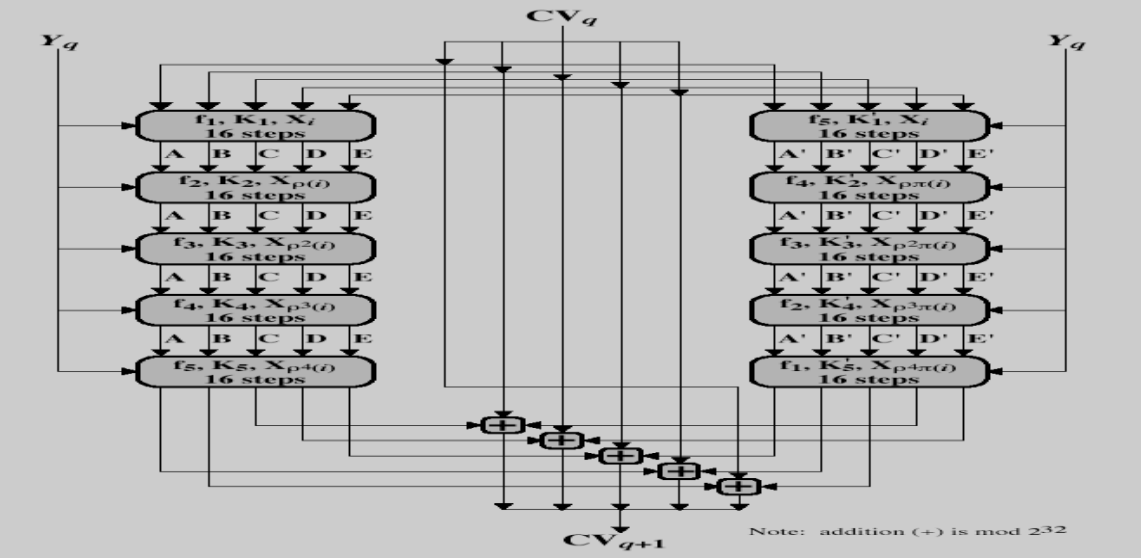

Fig.2 RIEMD-160 Processing of a Single 512-bit Block

4) Step-4: Process message in 512-bit (16 word) blocks: The heart of the algorithm is a module that consists of 10 rounds of processing of 16 steps each. The 10 rounds are arranged as two parallel lines of five rounds. The 10 rounds have a similar structure, but each uses a different primitive logical function, which we refer to as f1, f2, f3, f4 and f5.

5) Step-5: Output: The output hash value is the final buffer value.

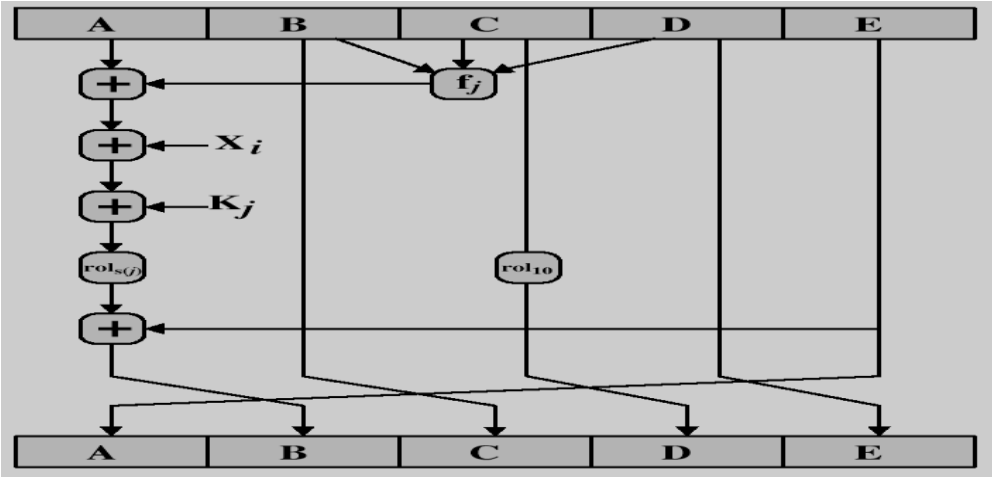

Fig.3 Elementary RIPEMD-160 Operation

D. Proposed Protocol

To increase the security within the transactions we propose to design a combination of the symmetric and asymmetric protocols. The proposed protocol uses AES-Rijindael for encryption thus ensuring a better encryption. RIPMD-160 is used in place of MD5, having a larger key size and ensuring better security towards third party intervention providing better security towards hacking.

E. Overview of the Proposed System

The proposed system mainly relies up on the hybrid cryptographic techniques i.e. symmetric and asymmetric algorithms.

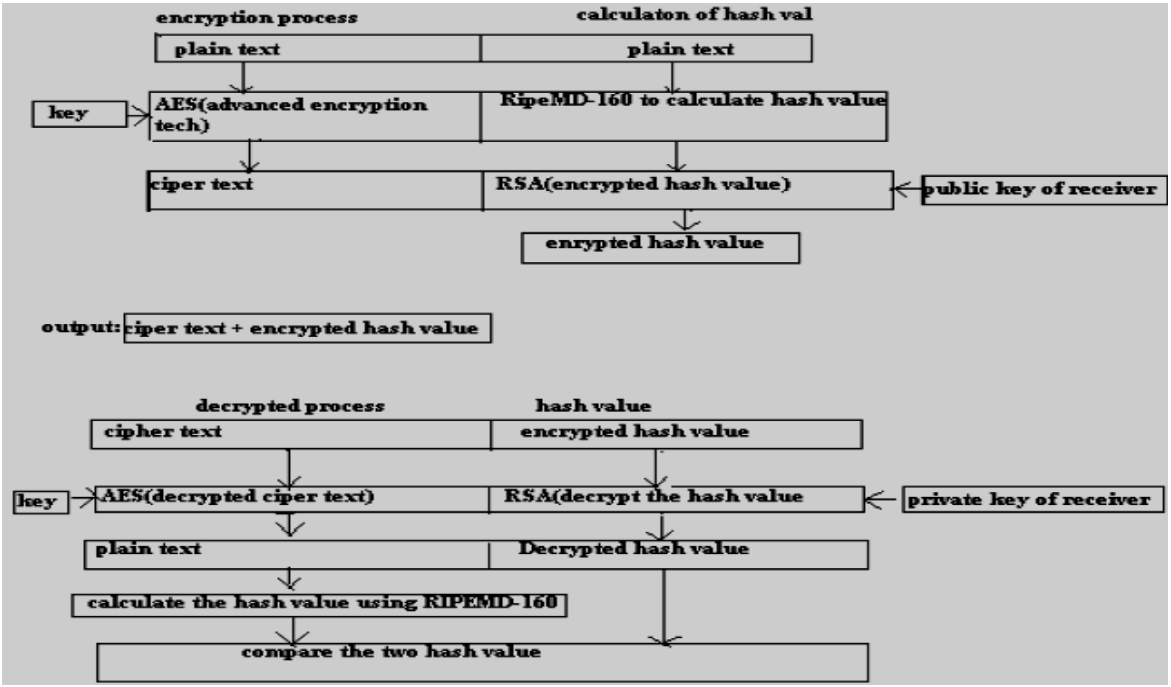

Fig.4 Shows the complete overview of the system

III. ARCHITECTURE FOR THE SENDER'S SIDE

Sender's side architecture involving the generation of key, connection establishment, encryption and hash value calculation.

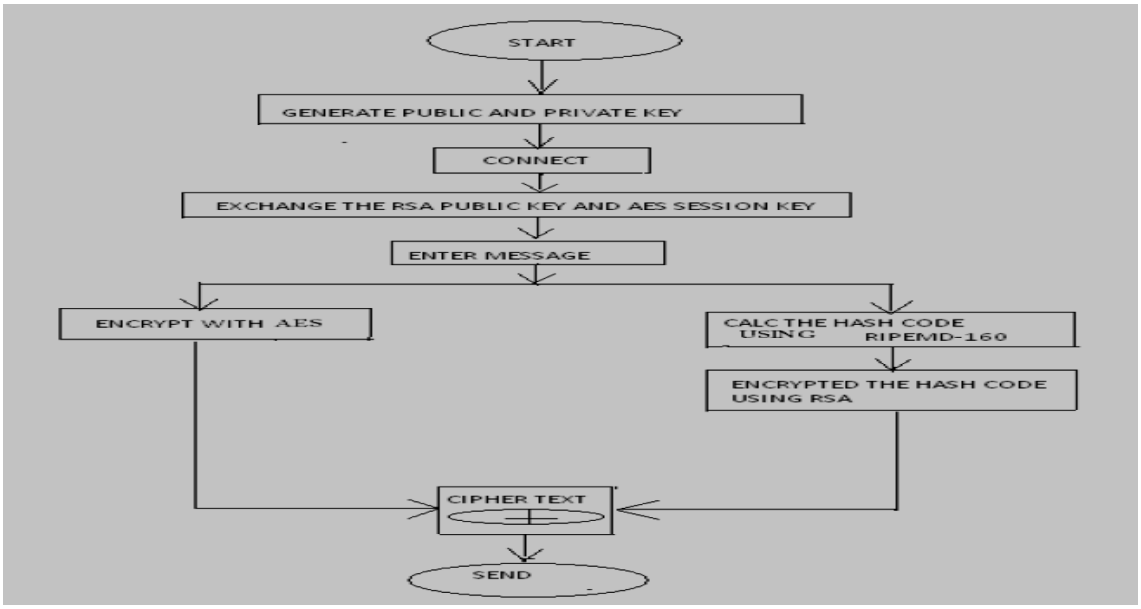

Fig.5 Architecture for Sender's Side

IV. ARCHITECTURE FOR THE RECEIVER'S SIDE

Receiver's side architecture involving decryption and comparison.

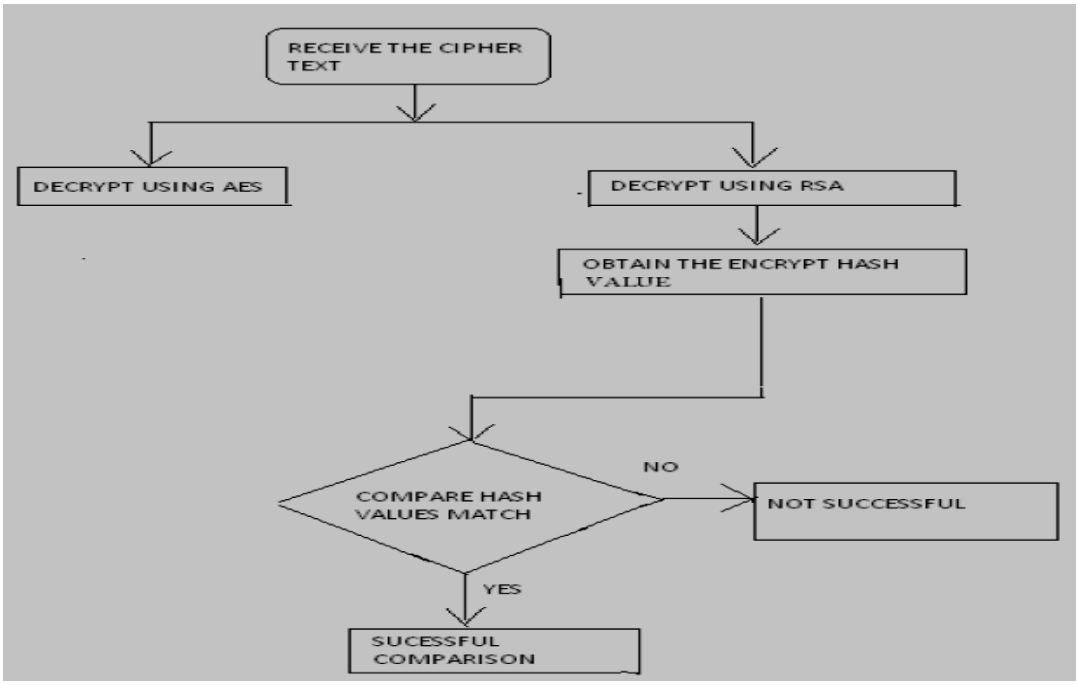

Fig.6 Architecture for Receiver's Side

V. CONCLUSIONS

In this system we have tried to provide security to E-Commerce transactions with the combination of symmetric and asymmetric algorithms used in cryptography. The system encrypts every message that is being sent to the other remote client on the network and on the receiver's side decrypts the cipher text as well as checks for the confidentiality of data with hash value calculation helping to successfully attain all the three primitives of network security Authenticity, Confidentiality and Integrity.

REFERENCES

[1] Mark S. Merkow, Jim Breithaupt, Ken L. Wheeler. Building SET Applications for Secure transactions.
John Wiley & Sons, Inc., New York.
[2] Sung W. T., Yugyung L., et al," Design and Evaluation of Adaptive Secure Protocol for E-Commerce", , ©IEEE, 2005.
[3] William Stallings, *Cryptography and Network Security-Principles and Practices*, 3rd Edition, Pearson Education Asia.
[4**]** Chahar, R.K. Datta, G. Rajpal N, "Design of a New Security Protocol", IEEE 2008-01-07. Conference on Computational Intelligence and Multimedia Applications, 2007.
[5] David hook, "Beginning Cryptography with java".
[6] Mark Rhodes-Ousely Roberta Bragg and Keith Strassberg, "The Complete References of Network Security, Tata McHill".
[7] S.C.Coutinho, "Number Theory and RSA Cryptography
[8] [online] http://homes.esat.kuleuven.be/bosselae/ripemd160.html
[9] H. Dobbertin, "RIPEMD with two-round compress function is not collision free," Journal of Cryptology, to appear.

