ISSN: 2321-7782 (Online)
e-ISJN: A4372-3114
Impact Factor: 7.327

Volume 6, Issue 3, March 2018

International Journal of Advance Research in Computer Science and Management Studies

Research Article / Survey Paper / Case Study

Available online at: www.ijarcsms.com

A Review on AES Cryptosystem for Secure Online Purchase

K. Devika Rani Dhivya[1]
(M.Sc., M.Phil., MBA)Assistant Professor
Department of BCA &M.Sc SS
Sri Krishna Arts and Science College
Coimbatore, Tamil Nadu – India

A. Poojitha Shree[2]
IV M.Sc SS
Department of BCA &M.Sc SS
Sri Krishna Arts and Science College
Coimbatore, Tamil Nadu – India

Abstract: ***Payment fraud is the most common issue in card payment industry. Credit card is a card provided by the bank and used by the card holder to make purchases on credit .Debit card is a card which allows the user to transfer money from their bank account while making purchase. Nowadays purchases through credit cards and debit cards are increasing day by day. Through the more usage of credit cards and debit cards for online purchase as well as for regular purchase, the fraud associated with it also increases. In this project the technique of cryptography is followed. Cryptography is one of the most secure technologies used to secure the data and data transmission. Cryptography uses a variety of encryption methods and algorithms. One of the most popular algorithms of cryptography is Advanced Encryption Standard algorithm (AES). Advanced Encryption Standard is based on "Substitution permutation network". It composes of a series of linked operations. AES performs all its operations on bytes instead of bits .The major advantage of AES is, it is stronger and faster than Triple Data Encryption Standard and it supports larger key sizes than triple DES.***

Keywords: AES, TDES, Keys, Encryption, Decryption, cryptography.

I. INTRODUCTION

Due to the rapid growth of electronic transactions and digital communication, data security has become a serious issue in the society. Cryptography techniques help in securing data and information. Payment fraud through debit card and Credit Card is one of the biggest problems to business administration today. However, to prevent the fraud effectively, first it is important to understand the techniques and mechanisms of executing the fraud. Debit card and Credit card fraudsters employ a large number of techniques to commit fraud.Credit card and debit fraud is a form of theft that involves an unauthorized person taking another's card information for the charging on purchases. Nowadays most of the administrations and institutions are facing a large number of frauds and consequently there are in a need of automation systems to detect and fight against frauds. These systems are necessary since it is not easy for a human analyst to detect fraud in transactions. Debit and credit card fraud is committed when a person,

- Fraudulently takes, uses, signs, sells someone else's card information
- Uses their card with the knowledge that the card is revoked or expired or that the account lacks enough money.
- Use of unauthorized card to sell goods and services to someone else.

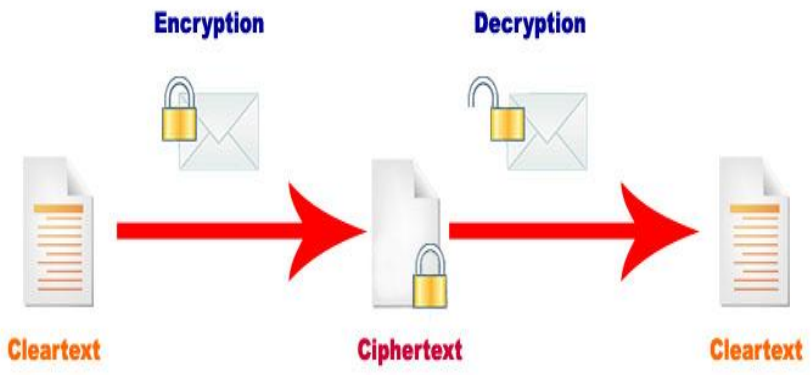

Fig1. Encryption-Decryption process

Data encryption is used largely in today's modern society. The basic facts of data encryption are privacy of data and authentication. As today's society becomes more connected, more information is available so there is a need of securing information with integrity and privacy.(5)

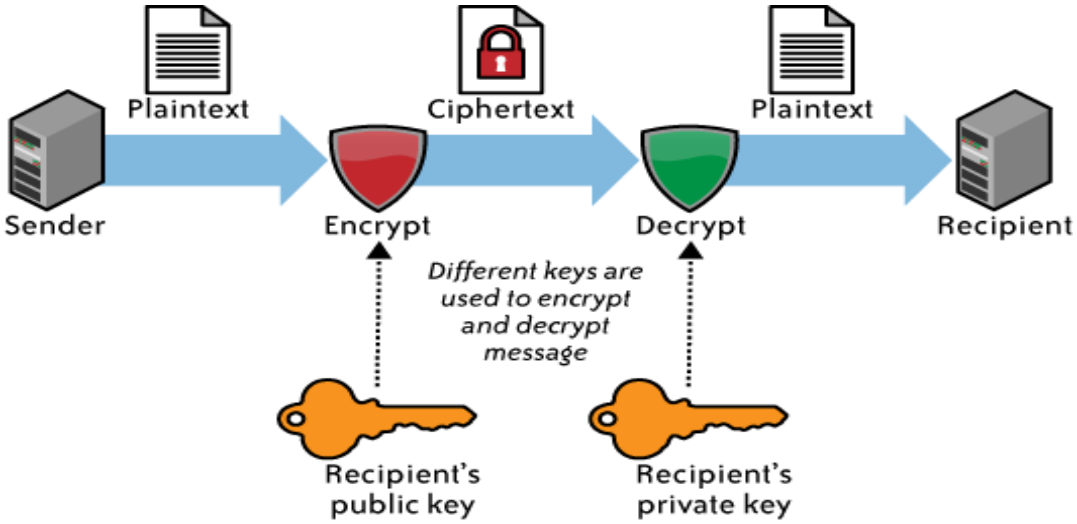

Fig.2 General Key Generation

II. METHODOLOGY

A. *Study on Existing System*

Whenever a new user logins to make purchase their personal details are not cross checked. Access is provided to the user instantly. This allows any user to login and thusalso allowingthe unauthorised users also. Persons who commit credit card and debit card fraud mostly go unpunished .A common method which is used to prevent fraud is"non-matching plastic" that is credit cards and debit cards which have been re-encoded with a different skimmed dump which is employed by many organisations, is to confirm whether the last four digits on the card match those on the magstripe. This is called as"checking last four". Nowadays all the credit and debit card frauds are conducted online. The fraudster makes online purchases without the knowledge of the card holder.(1)(5)

- *Triple Data Encryption Standard*

In existing system Triple Data Encryption Standard is used .TDES is an instance of three DES in a row.It is another mode of DES. It provides triple security in comparison to DES but it is a time consuming process, since it executes three times the process of DES. Three keys are used k1,k2 and k3 since it processes DES operation three times,(2)(3)

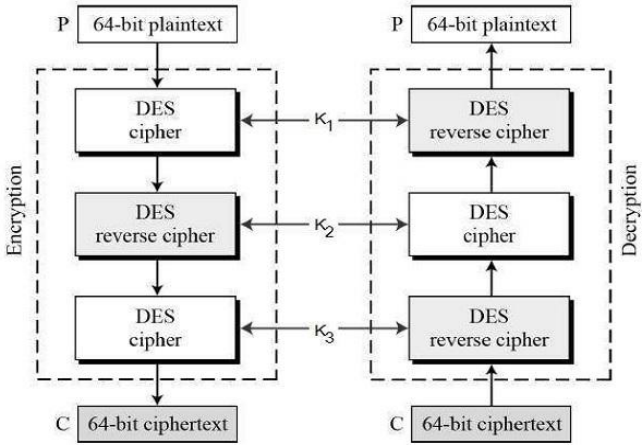

Fig.3 Working of TDES

The above fig.3 shows the working of TDES. The TDES key lengths are 56 bit, 112 bit, 168 bits instead of 64, 128,192 bits respectively. Since 8, 12, 24 bits used for parity check. Whenever a plain text of 64 bit is sent, every A is replaced by C and every B is replaced by D and so on by the alphabet, and by knowing only the "shift by 3" rule can decrypt the messages. Therefore "shift by n" technique of encryption is used for different values of n. There are 3 different keying options they are,

Option1: All the three keys are independent

Option2: Key k1 and key k2 are independent where k3=k1.

Option3: All the three keys are identical that is k1=k2=k3

Encryption-Decryption process is as follows,

- Encrypts the plain text using single DES with key k1.
- Then decrypts the output of step 1 with single DES using key k2.
- Finally, encrypts the output of that with single DES with key k3.
- The output is the encrypted text that is the cipher text.
- Decryption is the reverse process.
- Here user first decrypts the encrypted text with key k3.
- Then encrypts the text with key k2.
- Finally decrypts with key k1.

Since Triple DES is three times the process of DES (Data Encryption Standard) .It is a time consuming process, it does not support larger key sizes and it is very slow especially in software implementations since Data Encryption Standard is design for hardware purposes.(1)(2)(5)

B. Problem Definition

The main objective is to build a website to purchase goods online. The payment is credited or debited through card. Whenever a new customer login, the admin checks the personal details provided by the customer with the bank data which is already available and send the information to the customer by granting permission to access the account. The customers with minimum balance in their account can only make the purchase. Then the admin checks all the details of the customer account by verifying the credit card or debit card number used, so that only valid customers will be allowed to make the purchase. If in case unauthorised person logging using another's account it automatically logs out and sends an alert message to the authorised person. This increases the security advantage to the proposed system.(5)

C. Proposed System

The proposed system uses AES that is Advanced Encryption Standard. Whenever a new user login their personal information and account information such as credit card number or debit card number ,their bank ,contact number are cross checked. Only when their details are valid the customer can make the purchase. This prevents the unauthorized login so that only the customer with valid information can login and make the purchase. Each time when the customer makes the purchase their credit card number or debit card number is verified with the encrypted number in the bank database which is already available. Due to this verification of card number during each login only the right users alone can buy the products. This safeguards the customer from frauds. Every time when the customer leaves the browser it automatically encrypts the credit card or debit card number so that no fraudsters can hack the original credit or debit card number of the card holder. After verifying the credit card and debit number it is automatically encrypted or decrypted as the need by the bank. To overcome the problems raised in the existing system can be overcome by the implementations in proposed system.(4)(5)

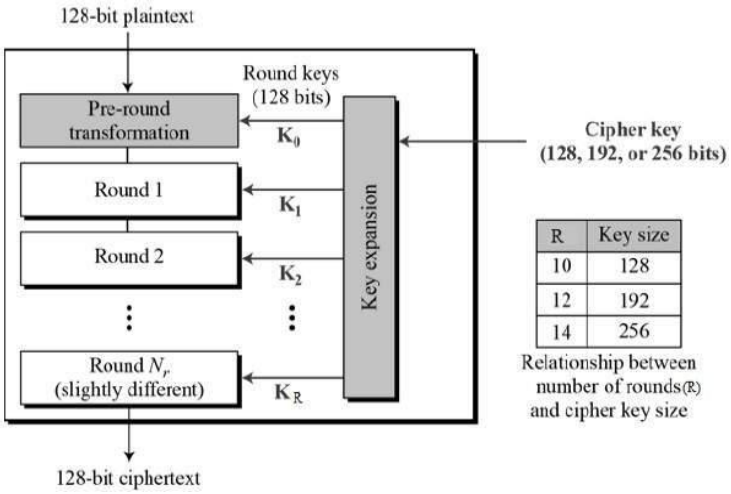

Fig.4 Working of AES

Fig.4 Explains the working AES. It is used to encrypt the plain text into the encrypted text which is called as cipher text. If any hacker accesses the database they cannot change or modify the data. It can perform on 128,192 and 256 bits of plain text using keys. In AES operations, there are specific rounds for key lengths such as 10 rounds for 128-bit and 12 rounds for 192-bit and 14 rounds for 256-bit. Normally rounds are 9, 11, 13 and the final round is 10^{th}, 12^{th} and 14th.

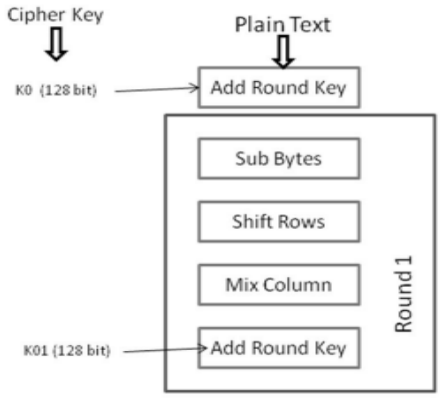

Fig5. Encryption Process

Fig. 5 Explains Encryption process. Four operations are involved to convert the plain text to cipher text. They are,

1. Sub bytes. Shift Rows, Mix Columns, Add Round Key

➢ *Sub bytes*

The input 16 bytes are replaced in the state array with its corresponding value by looking upon a fixed table which is referred to as s-box. The result is in matrix form of 4 rows and 4 columns.

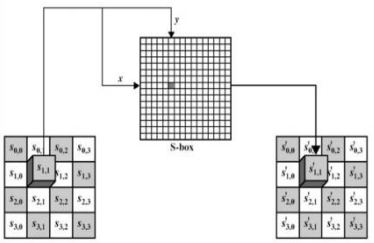

Fig.6 Sub Bytes

➢ *Shift Rows*

Four rows each of the matrix is shifted towards the left. Any entries that are left that is "fall off" are inserted on the right side of the row.The shift is carried out as the following steps,

- 1st row is not shifted.
- 2nd row is shifted one byte position towards left.
- 3rd row is shifted towards two positions to the left.
- 4th row is shifted three positions towards left.
- The resultant matrix contains same 16 bytes but shifted to each other.

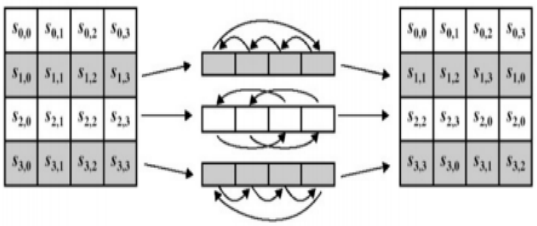

Fig.7 Shift rows

➢ *Mix columns*

Each column which contains four bytes is converted using a special mathematical process. This process takes four bytes of one column as input and converts into completely new bytes of output which is replaced by the true column.The resultant matrix is a new matrix of 16 new bytes .This step is not processed in the last round.

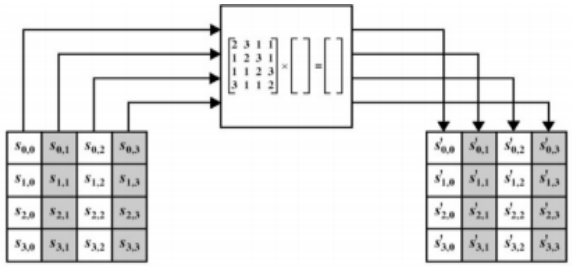

Fig.8 Mix columns

➢ *Add Round key*

The new matrix of 16 bytes is now considered as 128 bits. If this round is the last round then the output is the encrypted text. Or else, the resultant 128 bits are considered as 16 bytes and another similar round begins.

Decryption Process

The decryption process of an AES algorithm is same as the encryption process but it executes in reverse order. The same four processes are performed but in reverse order such as,

- Add Round key

- Mix columns
- Shift Rows
- Byte Substitution

III. Result and Discussion

Cryptography involves the protection of data and authentication of users. The graphical representation of cryptographic algorithms over their performance is shown,

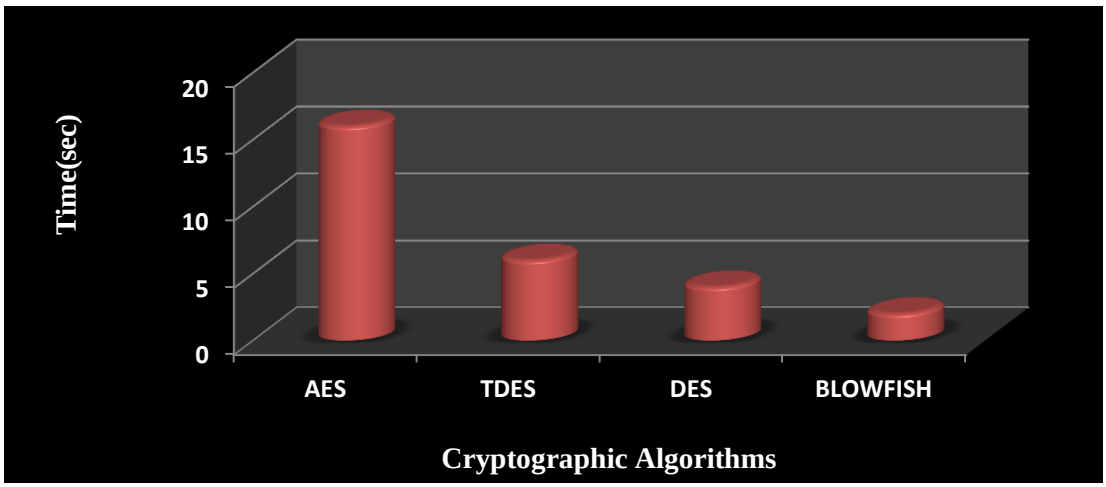

Fig.9 Comparison of cryptographic algorithms

The above fig shows the high level performance of AES when compared to DES, TDES, Blowfish. The comparison of time in seconds is used.(5)

IV. Conclusion

Cryptography provides data privacy and authentication of valid users. It is more about customer privacy and security. Efficient debit card and credit card fraud prevention is the requirement for bank and all types of online transactions. AES is widely used and implemented in both hardware and software. Till date there is no cryptanalytic attacks on the AES algorithm has been invented. It has inbuilt flexibility of key length which provides a technique of "future proofing" which performs exhaustive key searches. As in DES, the AES security is also enhanced only if it is implemented correctly with good management of keys. By implementing this algorithm the speed of transactions has become faster now.(2)(5)

References

1. Rimpi Debnath, Priyanka Agrawal, Geetanjali Vaishnav, "DES, AES AND Triple DES: Symmetric Key Cryptography Algorithm", International Journal of Science, Engineering and Technology Research (IJSETR), Volume 3, Issue 3, March 2014.
2. V. M. Silva-Garc´ia , R. Flores-Carapia , B. Luna-Benoso , "The Triple-DES-96 Cryptographic System", Int. J. Contemp. Math. Sciences, Vol. 8, 2013, no. 19, 925 – 934
3. Grabbe J, Data Encryption Standard: The Triple DES algorithm illustrated Laissez faire city time, Volume: 2, No. 28, and 2003.
4. Gaurav Berad, Ashish Jaggi,Vaibhav Jagadales,"Review on implementation of AES algorithm for device based encryption" International Journal of Advanced Computational Engineering and Networking, Volume-4, Issue-2, Feb.-2016
5. S aishwarya, kdr dhivya,"Online Payment Fraud Prevention Using Cryptographic Algorithm TDES", International Journal of Computer Science and Mobile Computing(IJCSMC), Vol. 4, Issue. 4, April 2015.

AUTHOR(S) PROFILE

Mrs. K Devika Rani Dhivya, Msc., M.Phil., M.B.A., is working as an Assistant Professor in the Dept. of BCA & MSc SS at Sri Krishna College of Arts and Science, Coimbatore. She is pursuing her Ph.D. at Bharathiar University, Coimbatore and doing research work on Software Engineering. She has published papers in International journals and presented at various Seminars, National and International Conferences and wishes to contribute to the Computing arena.

A. Poojitha Shree, currently studies Msc Software Systems at Sri Krishna College of Arts and Science. Completed her project on "AES Crypto System for Secure Online Purchase" by comparing TDES and AES algorithms.

