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. 4, Issue. 4, April 2015, pg.317 – 323

RESEARCH ARTICLE

Online Payment Fraud Prevention Using Cryptographic Algorithm TDES

S. AISHWARYA[1]
III MSc (SS),
Department of CA & SS,
Sri Krishna Arts and Science College,
Coimbatore, Tamil Nadu,
India

K.DEVIKA RANI DHIVYA*[2]
Assistant Professor,
Department of CA & SS,
Sri Krishna Arts and Science College,
Coimbatore, Tamil Nadu,
India

ABSTRACT: Credit card is a small plastic card issued by a bank, building society, etc., allowing the holder to purchase goods or services on credit. Debit card is a card allowing the holder to transfer money electronically from their bank account when making a purchase. The use of credit cards and debit cards are increasing day by day. People are relying more on both cards nowadays than in the previous days. As credit cards and debit cards becomes the most popular mode of payment for both online as well as regular purchase, cases of fraud associated with it are also rising. In real life, fraudulent transactions are scattered with genuine transactions and simple pattern matching techniques are not often sufficient to detect those frauds accurately. In this project the process of Cryptography has been followed, it is one of the most important security technologies which used to secure the data transmission and the data itself. As the time and challenge growth, the cryptography also grows up with variety of encryption techniques and algorithms. Among the algorithms, one of the most popular is the Triple Data Encryption Standard algorithm. Triple Data Encryption Standard is a type of computerized cryptography where block cipher algorithms are applied three times to each data block. The key size is increased in Triple DES to ensure additional security through encryption capabilities. The major advantage of TDES is, it is three times slower than regular DES but can be billions of times more secure if used properly. Since it is based on the DES algorithm, it is very easy to modify existing software to use Triple DES.

I. INTRODUCTION

Due to the rapid growth of digital communication and electronic data exchange, information security has become a crucial issue in industry, business, and administration. Modern cryptography provides essential techniques for securing information and protecting data. Credit Card and debit card Fraud is one of the biggest threats to business establishments today. However, to combat the fraud effectively, it is important to first understand the mechanisms of executing a fraud. Credit card and debit card fraudsters employ a large number of modus operandi to commit fraud. Nowadays, enterprises and public institutions have to face a growing presence of frauds and consequently need automatic systems able to support fraud detection and fight. These systems are essential since it is not always possible or easy for a human analyst to detect fraudulent patterns in transaction datasets, often characterized by a large number of samples, many dimensions and online update.

Credit card and debit card frauds are committed in the following ways:

- An act of criminal deception (mislead with intent) by use of unauthorized account and/or personal information
- Illegal or unauthorized use of account for personal gain
- Misrepresentation of account information to obtain goods and/or services.

Data encryption is used pervasively in today's connected society. The two most basic facets of modern day data encryption are data privacy and authentication. As modern society becomes more connected, and more information becomes available there is a need for safeguards which bring data integrity and data secrecy. In addition, authenticating the source of information gives the recipient, with complete certainty that the information came from the original source and that it has not been altered from its original state. [5]

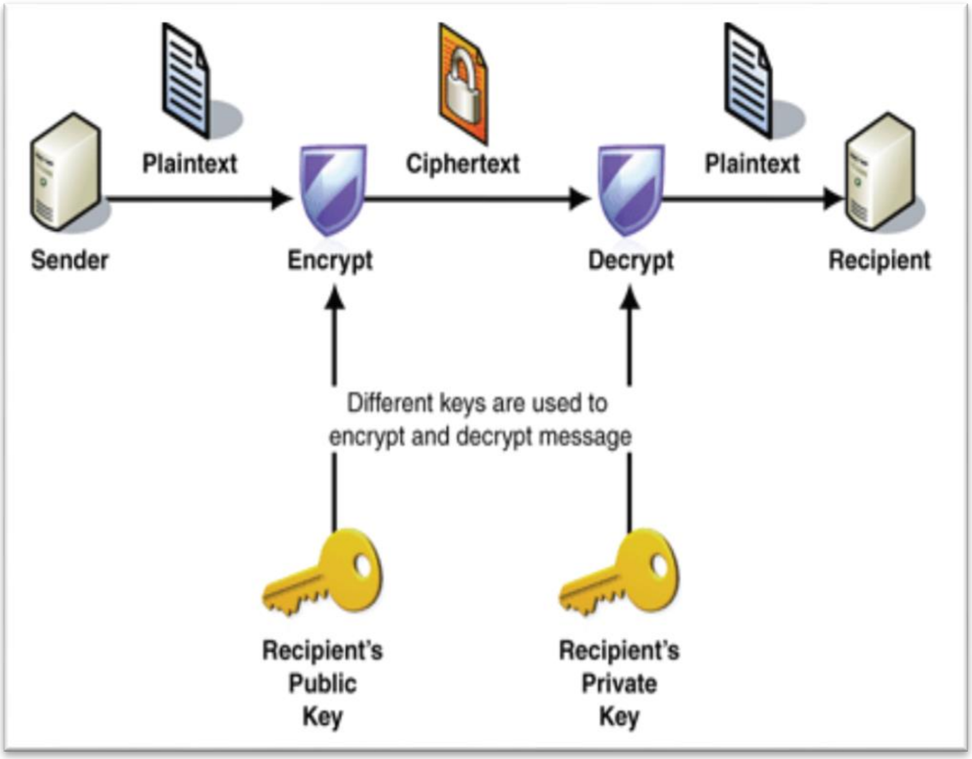

Fig. 1 General Key generation

II. METHODOLOGY

A. Study On Existing System

Whenever a new user registers, his personal details are not cross checked. Access is provided to him instantly. There is no credit card and debit card fake checking. This may allow any user to register and thus allowing malicious users also. And also there is no any security in transferring the credit card and debit card number to bank. Persons that commit credit card and debit card crime largely go unpunished and repeatedly victimize consumers and businesses.

A common technique to prevent 'non-matching plastic' (credit cards/debit cards which have been re-encoded with a different skimmed dump) which is employed by many companies, is to confirm that the last four digits embossed on the card match those on the magstripe (and therefore the sales receipt). This is called 'checking last four.

Typically, the fraudster causes a credit card and debit card of another person to be charged for a purchase. Today, half of all credit card and debit card fraud is conducted online, meaning that the fraudsters make online purchases with the credit card details of other people.

In the existing system, the encrypted key is send with the document. If the key is send with document, any user can view the encrypted document with that key. It means the security provided for the encryption is not handled properly. And also the Key byte (encrypted key) generate with random byte [1]. Without the user interaction the Key byte is generated. Use of multiple length keys leads us to the Triple-DES algorithm, in which DES is applied three times. The main drawbacks of the existing system are, the algorithm which were used before, leads to the Lack of security. There is more Complexity in the creation **of** key**s.** Existing algorithms are limited by the prime and efficiency of generating primes is relatively low, so it is difficult to achieve a secret once.

- *Data Encryption Standard (DES)*

The Data Encryption Standard (DES) is a block cipher that uses shared secret encryption. The main purposes of using data encryption standard are as follows:

UNIX passwords: In the UNIX password scheme there are 2^{12} different modified DES algorithms all with slightly different S-boxes. The particular S-box used is determined by a random 12-bit integer called a `salt'. The key consists of the first 8 characters (only) of the password entered[4][6][7].

Setting up a password: A random 12-bit is found and used as the `salt'. A system dependent constant is encrypted using the password as the key and the appropriate (to the salt) DES algorithm, giving a result which is again encrypted. In total it is encrypted 25 times recursively and the final result is the encrypted password. The login name, salt and encrypted password are then recorded in the password file.

Checking a password: The login name is given, the salt is looked up in the password file, then after the password is entered it is used as the key, and encrypted as above, and the final result is compared with the encrypted password in the password file. If they match then the password is accepted, otherwise it is rejected.

The Data Encryption Standard (DES) is susceptible to brute-force attacks, so that designers and implementers have all the information they need to make judicious decisions regarding its use [2][3][8].

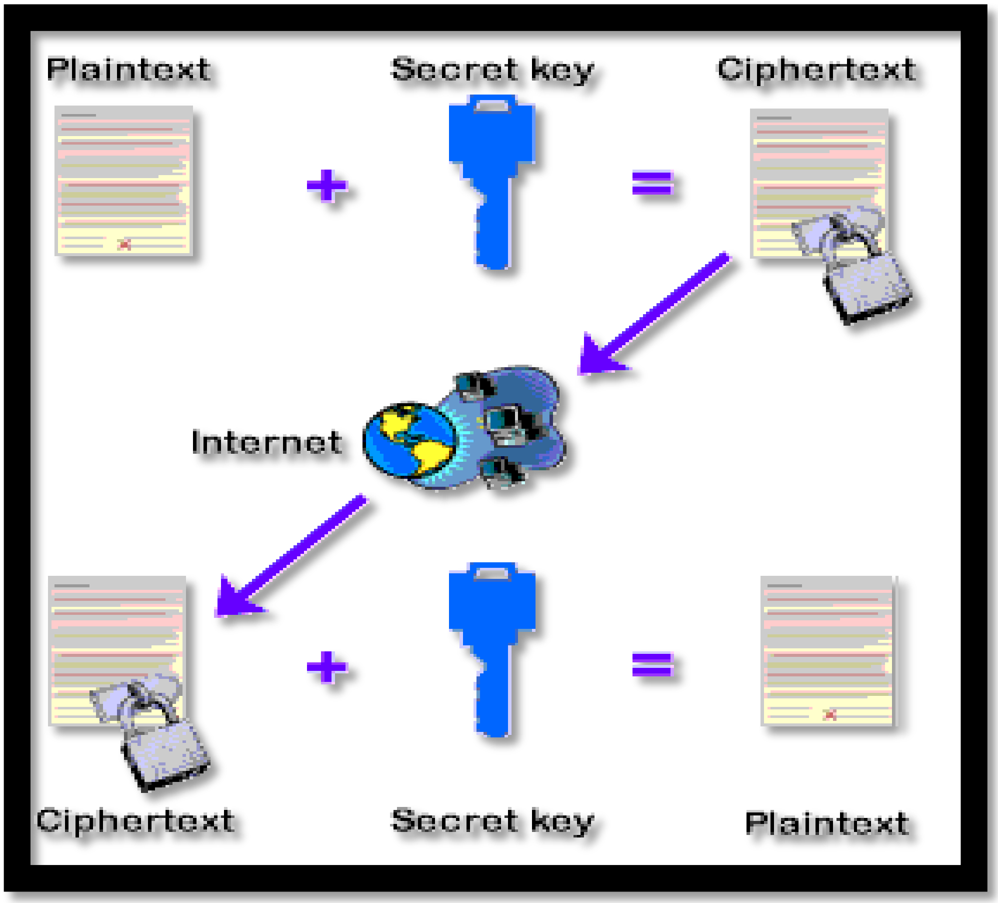

Fig.2 Working of DES [7]

B. *Problem Definition*

The main aim is to develop a full website for purchase of goods. The customers can easily purchase goods through online with security. All amounts is credited or debited through credit card and it will transfer to back safely. Whenever a new customer joins, the administrator check the details provided by the customer, with the bank database already available and send a mail to the customer giving permission to access the account. The customer is allowed to see his/her recent transactions. Only customers having a minimum balance in their credit card can buy products. Also the administrator verifies the credit card number and account number before he/she buys any product in order to allow only valid customers. To avoid invalid customer's purchase product in another user's account, the system automatically logs out in the first trial itself. This is to add another security advantage to the proposed system.

C. *Proposed System*

In proposed system, whenever a new user registers, the credit card and debit card details are cross checked and then only the user id is generated. This allows only correct users to login each time. At the same time credit card and debit card details are verified each time whenever a customer buys product. This verification enables only right users to buy products. And also the credit card number will be encrypted before leaving the browser, so hacker cannot able to chase the apt credit card number. Similar to this, debit card details also will be encrypted before leaving the browser, so hacker cannot able to chase the apt debit card details.

After reaching the encrypted credit card number and debit card number to bank, that will be decrypted by the bank. To overcome all the problems in the existing system, development to ease the operation is implemented. A system is required which is being capable of elimination all the problems and become useful to users and thus the new system is derived. Here, User can set the byte of key manually.

► *Triple Data Encryption Standard (TDES)*

Triple Data Encryption Standard is an enhancement to Data Encryption Standard, which provided triple security in comparison to DES. The algorithm is same, only the encryption technique is applied thrice in order to increase the level of security. Triple DES is advantageous because it has a significantly sized key length, which is longer than most key lengths affiliated with other encryption modes. Triple-DES is still in use today but is widely considered a legacy encryption algorithm. DES is inherently insecure, while Triple-DES has much better security characteristics [9].

Security of 3DES is, in an academic way, about 2^{112} operations, which translates as "cannot break that". 3DES was created to work with legacy financial systems that had previously been working with DES. During the cutover, replacing a DES module with a 3DES using the legacy DES key repeated 3 times (keying option 3) was a transparent operation. Once all the systems were ready, the full 3DES keys (keying option 1) could be deployed.

Triple DES enjoys much wider use than DES because DES is so easy to break with today's rapidly advancing technology. This just serves to illustrate that any organization with moderate resources can break through DES with very little effort these days. Triple DES was the answer to many of the shortcomings of DES. Since it is based on the DES algorithm, it is very easy to modify existing software to use Triple DES.

It also has the advantage of proven reliability and a longer key length that eliminates many of the shortcut attacks that can be used to reduce the amount of time it takes to break DES. However, even this more powerful version of DES may not be strong enough to protect data for very much longer. The DES algorithm itself has become obsolete and is in need of replacement. Triple DES is simply another mode of DES operation. After reaching the encrypted credit card number and debit card number to bank, that will be decrypted by the bank. To overcome all the problems in the existing system, development to ease the operation is implemented. A system is required which is being capable of elimination all the problems and become useful to users and thus the new system is derived. Here, User can set the byte of key manually.

If we consider a triple length key to consist of three 32-bit keys K1, K2, K3 then encryption is as follows:

○ **ENCRYPT WITH K1**
○ **DECRYPT WITH K2**
○ **ENCRYPT WITH K3**

Decryption is the reverse process:

- ○ **DECRYPT WITH K3**
- ○ **ENCRYPT WITH K2**
- ○ **DECRYPT WITH K1**

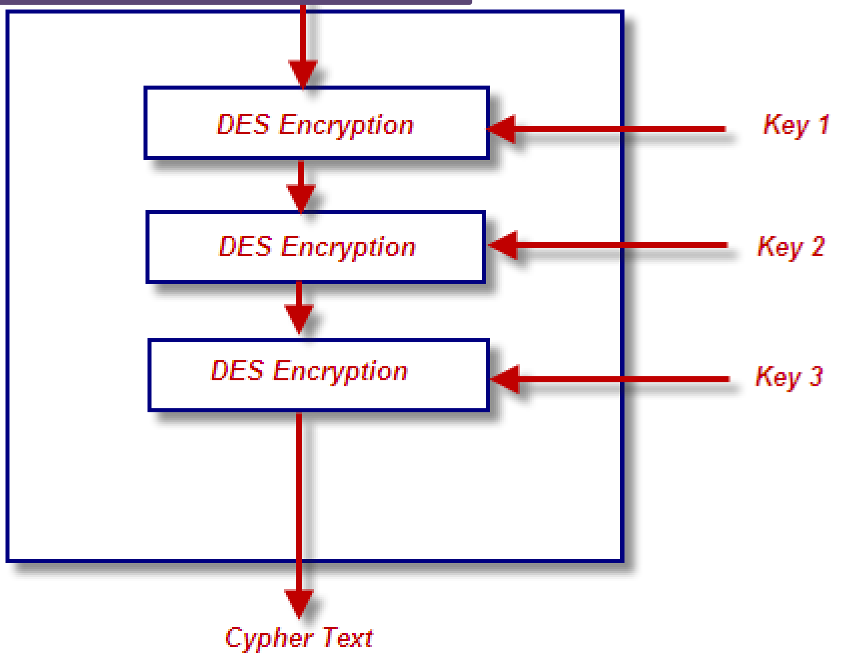

Fig..3 Working of TDES

The above fig.1 shows the Working of TDES [9][10]. As an example, for a plaintext message being sent, if every A is replaced with a D, every B is replaced with an E, and so on through the alphabet, only someone who knows the "shift by 3" rule can decipher the messages. Hence a "shift by n'' encryption technique can be performed for several different values of n. Therefore, n is the key here.

The standards define three keying options:

- Keying option 1: All three keys are independent.
- Keying option 2: K1 and K2 are independent, and K3 = K1.
- Keying option 3: All three keys are identical, i.e. K1 = K2 = K3.

Key option #3 is known as triple DES. Triple DES is advantageous because it has a significantly sized key length, which is longer than most key lengths affiliated with other encryption modes. Triple DES encrypts input data three times. The three keys are referred to as K1, K2 and K3. Triple DES is backward compatible with regular DES. The Triple-DES variant was developed after it became clear that DES by itself was too easy to crack.

3DES nominally uses a 192-bit key (three 64-bit DES keys), out of which 168 bits are really used. Yet, there is an "academic" attack against 3DES with cost 2^{112}, so it is often said that the overall security of 3DES is similar to that offered by a theoretically perfect block cipher with a 112-bit key. Hence, there is a widespread usage mode of 3DES in which we use a 128-bit key: 64 bits for K_1 and 64 bits for K_2, and then set $K_3 = K_1$. In plain words, encrypt the block with K_1, then decrypt with K_2, then encrypt again withK_1. This seems sufficient to achieve the 112-bit level of security (of the 128 key bits, only 112 are really used), and the academic attack shows that you cannot go beyond that level anyway. This is what the smartcard implements.

It uses three 32-bit DES keys, giving a total key length of 96 bits. Encryption using Triple-DES is simply

✓ encryption using DES with the first 32-bit key
✓ decryption using DES with the second 32-bit key
✓ encryption using DES with the third 32-bit key

Because Triple-DES applies the DES algorithm three times (hence the name), Triple-DES takes three times as long as standard DES. Decryption using Triple-DES is the same as the encryption, except it is executed in reverse. TDES standard based on the DES algorithm; therefore it is very easy to modify existing software to use TDES. It also has the advantage of proven reliability and longer key length that eliminates many of the attacks that can be used to reduce the amount of time it takes to break DES.

Triple DES uses a "key bundle" that comprises three DES keys, K_1, K_2 and K_3, each of 64 bits.
The encryption algorithm is:

$$\textbf{CIPHER TEXT} = E_{K3}\,(D_{K2}\,(E_{K1}\,(\textbf{PLAINTEXT})))$$

Which means, encrypts with K_1, decrypt with K_2, and then encrypt with K_3.
Decryption is the reverse:

$$\textbf{PLAINTEXT} = D_{K1}\,(E_{K2}\,(D_{K3}\,(\textbf{CIPHER TEXT})))$$

Which means, decrypts with K_3, encrypt with K_2, and then decrypt with K_1.

Each triple encryption encrypts one block of 64 bits of data. In each case the middle operation is the reverse of the first and last. This improves the strength of the algorithm when using keying 2, and provides backward compatibility with DES with keying option 3.

► *Advantages*

- TDES is easy to implement (and accelerate) in both hardware and software.
- The speed of TDES is much faster than public key cryptography methods like RSA.
- 3DES is ubiquitous and hence most systems, libraries, and protocols include support for it.
- Provide easy and well security to Online Shopping.
- The detection of the fraud use of the card is found much faster than the existing system.
- In case of the existing system even the original card holder is also checked for fraud detection. But in this system no need to check the original user as here maintains a log.
- This reduces the tedious work of an employee in the bank.
- Security is enhanced in well manner, and the user only knows the key.

III. RESULT AND DISCUSSION

Cryptography protects users by providing functionality for the encryption of data and authentication of other users. The graphical representation on discussion of various cryptographic algorithms over security is shown in Fig1.

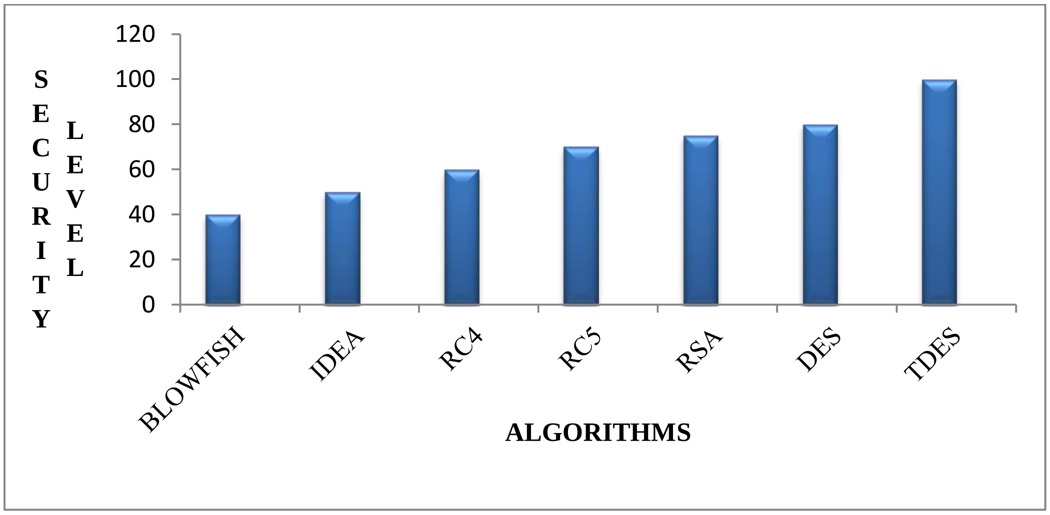

Fig4. Comparison between Cryptographic algorithms

The above fig shows that the TDES performs good to secure the data while transferring, Software enhancement may involve providing new functional capabilities, improving user display and modes of interaction, upgrading external documents or the performance characteristics of the system. Implementation is the most crucial stage in achieving a successful system and giving the user's confidence that the new system is workable and effective. Implementation of a modified application to replace an existing one. This type of conversation is relatively easy to handle, provide there are no major changes in the system.

Each program is tested individually at the time of development using the data and has verified that this program linked together in the way specified in the programs specification, the computer system and its environment is tested to the satisfaction of the user. The system that has been developed is accepted and proved to be satisfactory for the user. And so the system is going to be implemented very soon. A simple operating procedure is included so that the user can understand the different functions clearly and quickly. Initially as a first step the executable form of the application is to be created and loaded in the common server machine which is accessible to the entire user and the server is to be connected to a network. The final stage is to document the entire system which provides components and the operating procedures of the system.

IV. CONCLUSION

Cryptography protects users by providing functionality for the encryption of data and authentication of other users. The Data Encryption Standard (DES) is one of the most popular encryption algorithm used until recently. Efficient credit card and debit card fraud prevention system is an utmost required for card issuing bank or all type of online transaction that through using credit card. Implementation of triple data encryption standard algorithm in credit card and debit card fraud prevention is used in this report. It has also explained the triple data encryption standard how can prevent whether an incoming transaction is fraudulent or not comparative studies reveal that the accuracy to the system is also over a wide variation in the input data. In triple data encryption standard, methods are very low in comparing techniques using fraud prevention rate. I have suggested a method for finding the spending profile of cardholders, as well as application of this knowledge in deciding the value of observation symbols and initial estimate of the model parameters. It also have been explained, the triple data encryption standard can detect whether an incoming transaction is fraudulent or not. The system is also scalable for handling large volumes of transactions. The application works well. The application is tested very well and errors are properly debugged. The site is simultaneously accessed from more than one system. Simultaneous login from more than one place is tested. The site works according to the restrictions provided in their respective browsers. Further enhancements can be made to the application, so that the web site functions very attractive and useful manner than the present one. The speed of the transactions become more enough now.

REFERENCES

1. Anjula Gupta, Navpreet Kaur Walia,"Cryptography Algorithms: A Review", 2014 IJEDR | Volume 2, Issue 2 | ISSN: 2321-9939.
2. Brad Hammell , "A Secure Double-Length Hash Function using 2-key 3DES with Rate One", 21st Computer Science Seminar Addendum-T1-4.
3. Fiolitakis Antonios, Petrakis Nikolaos, Margaronis Panagiotis, Antonidakis Emmanouel "Hardware Implementation of Triple-DES Encryption/ Decryption Algorithm", 2013.
4. Grabbe J, Data Encryption Standard: The Triple DES algorithm illustrated Laissez faire city time, Volume: 2, No. 28, and 2003.
5. Karthik .S, Muruganandam. A, "Data Encryption and Decryption by Using Triple DES and Performance Analysis of Crypto System", International Journal of Scientific Engineering and Research (IJSER) www.ijser.in ISSN (Online): 2347-3878 Volume 2 Issue 11, November 2014.
6. Kitsos. P, Goudevenos and Koufopaylou, "Vlsiimplementations of the triple-DES block cipher", ICECS-2003, 76-79, 0-7803-8163-7/03/$17.002003IEEE.
7. Raymond G. Kammer. FIPS 46-3 Data Encryption Standard (DES). In Federal Information Processing Standards Publication. Oct 1999.
8. 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.
9. 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.
10. V. M. Silva-García, R. Flores-Carapia and C. Rentería-Márquez, "Triple-DES Block of 96 Bits: An Application to Colour Image Encryption", Applied Mathematical Sciences, Vol. 7, 2013, no. 23, 1143 - 1155 HIKARI Ltd.