Volume 4, Issue 1, January 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

# Implementation of Triple Data Encryption Standard using Verilog

**Mandeep Singh Narula**
*Assistant Professor, G D Goenka University*
*India*

**Simarpreet Singh**
*Associate Test Engineer, UHG Noida*
*India*

***Abstract— Encryption is an essential tool for protecting the confidentiality of data. Network security protocols such as SSL or IPSec use encryption to protect Internet traffic from eavesdropping. Encryption is also used to protect sensitive data before it is stored on non-secure disks or tapes. Encryption, however, is computationally expensive. A computer server that must encrypt data for thousands of clients before sending it over the network can easily become crypto-bound. The capacity of the server is then determined by the speed at which it can perform encryption. This is especially the case when slow encryption protocols such as the Digital Encryption Standard (DES) or Triple-DES are employed. Since DES and Triple-DES are very widely used, it is important to optimize the performance of these algorithms. Triple-DES (TDES) is basically used in various cryptographic applications and wireless protocol security layers [2]. This paper presents the design and the implementation of the Triple Data Encryption Standard (DES) algorithm. The main objective is to provide with a deep insight of the theory and design of a digital cryptographic circuit with the use of Verilog.***

***Keywords— Verilog, Data Encryption Standard, Triple DES encryption, Encryption system, Plaintext***

## I. INTRODUCTION

Beyond any doubt, the need for secure storage or transfer of information is an inextricable part of human history. Nowadays, the rapid evolution of communication systems offers, to a very large percentage of population, access to a huge amount of information and a variety of means to use in order to exchange personal data. Therefore, every single transmitted bit of information needs to be processed into an unrecognizable form in order to be secured. This enciphering of the data is necessary to take place in real time and for this procedure cryptography is the main mechanism to secure digital information. Due to the heavy increase in the volume of information data, a variety of encryption algorithms have been developed [1]. Among the different cryptographic algorithms, the most popular example in the field of symmetric ciphers is the Data Encryption Standard (DES) algorithm, which was developed by IBM in the mid-seventies.

The DES algorithm is popular and in wide use today because it is still reasonably secure and fast. There is no feasible way to break DES, however because DES is only a 64-bit (eight characters) block cipher, an exhaustive search of 255 steps on average, can retrieve the key used in the encryption. the rapid advances in the speed of electronic circuitry over the last 20 years, combined with the natural parallelism of Feistel ciphers and DES's relatively small key size, have rendered the algorithm obsolete [5]. A much more secure version of DES called Triple-DES (TDES), which is essentially equivalent to using DES three times on plaintext with three different keys. Naturally, it is three times slower than the original form of DES but it is way more secure. This paper examines the full procedure of implementing a DES and Triple DES algorithm using a high-level hardware description language verilog.

## II. PROPOSED DATA ENCRYPTION STANDARD

### *A. Previous Work*

A lot of research & development are going on over DES & Triple DES. DES and Triple-DES are already implemented in Spartan –II devices. DES is also developed using the Handel-C. Triple DES was developed to address the obvious flaws in DES without designing a whole new cryptosystem. Triple DES simply extends the key size of DES by applying the algorithm three times in succession with three different keys [5].

### *B. Data Encryption Standard*

Complete function of DES algorithm can be described briefly as follows [7]. DES is a block cipher. It operates on blocks of 64-bits in size. A 64-bit input block of plaintext will be encrypted into a 64-bit output block of cipher text. It is a symmetric algorithm, which means the same algorithm and key are used for encryption and decryption. The security of DES rests in the 56-bit key. The plaintext block is taken in and put through an initial permutation. The key is also taken in at the same time. The key is presented in a 64-bit block with every 8th bit being a parity check. The 56-bit key is then extracted ready for use. The 64-bit plaintext block is split into two 32- bit halves, named the right half and left half. The two halves of the plaintext are then combined with data from the key in an operation called Function F. There are 16 rounds of Function f, after which the two halves are recombined into one 64-bit block, which is then put through a final permutation to complete the operation of the algorithm and a 64-bit cipher text block is outputted [4]. The detailed procedure is represented with a flowchart in Figure 1.

 

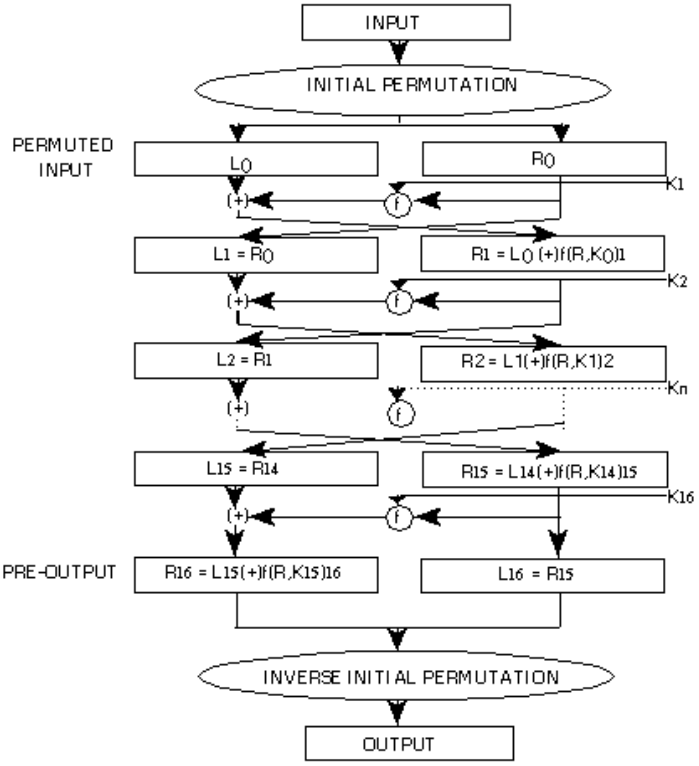


Figure 1. DES Encryption

## III. THE F FUNCTION AND KEY SCHEDULE

As shown in Figure.1 the right half of the plaintext after been expanded from 32 bits to 48 bits is exclusively-ored with a certain round key. The result of this operation is led to the eight following substitution boxes which transforms the 48-bit input to a 32-bit output. Finally a simple permutation (P) is performed before the final output [7].

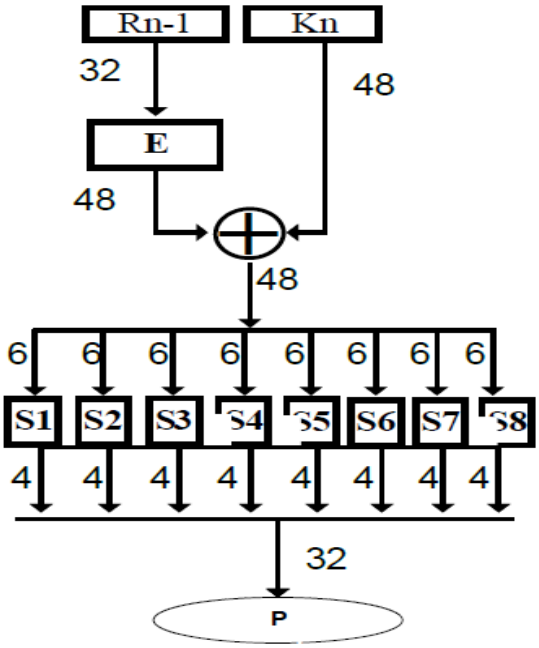


Figure 2. Function f

On each round a certain key is applied. The function f and key is shown in figure 2 and 3 respectively. This key is produced by a specific procedure shown and its characteristic is its two substitution permutations. When the initial 64-bit key is inserted, a permutation occurs (PC-1) in which every 8th bit of the key is used only for parity check and so its final size is reduced to 56-bits. Then, the key splits in two equal halves of 28-bits and each half is shifted (left, when we have an encryption progress or right, when decryption) zero, one or two bits depending on the number of round. After this operation a final permutation (PC-2) occurs.

 

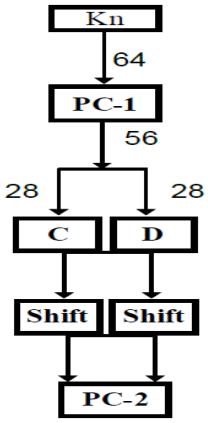


Figure 3. Key Schedule

## IV. TRIPLE DATA ENCRYPTION STANDARD

A concise representation of Triple Data Encryption Algorithm is described .TDES is a block cipher operating on 64-bit data blocks [2-8]. There are several forms, each of which uses the DES cipher three times. TDES can however work with one, two or three 56-bit keys. This means that the plaintext is encrypted three times [6]. A number of modes of TDES have been proposed:

- DES-EEE3: Three DES encryptions with three different keys.
- DES-EDE3: Three DES operations in the sequence encrypt-decrypt-encrypt with three different keys.
- DES-EEE2 and DES-EDE2: Same as the previous formats except that the first and third operations use the same

Let EK(I) and DK(I) represent the DES encryption and decryption of I using DES key K respectively. Each TDEA encryption/decryption operation is a compound operation of DES encryption and decryption operations. The following operations are used:

1. TDEA encryption operation: the transformation of a 64-bit block I into a 64-bit block O that is defined as follows: O = EK3 (DK2 (EK1 (I))).

2. TDEA decryption operation: the transformation of a 64-bit block I into a 64-bit block O that is defined as follows: O = DK1(EK2(DK3(I))).

The round function of DES is applied sixteen times for tdes as Shown below in figure 4:

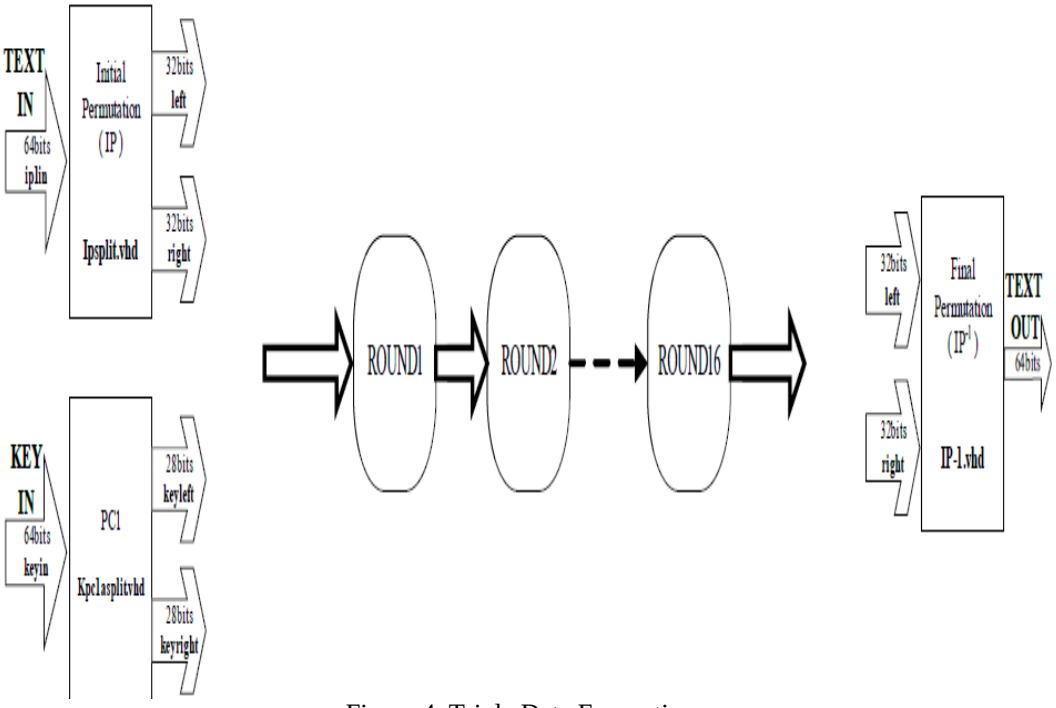


Figure 4. Triple Data Encryption

 

## V. SIMULATION RESULTS

### *A. Synthesis and Implementation*

The complete design was synthesized and implemented with the use of verilog using ISE Foundation. Simulation was done by ISE simulator. The RTL architecture of DES and TDES is shown in Figure 5 and 6 respectively.

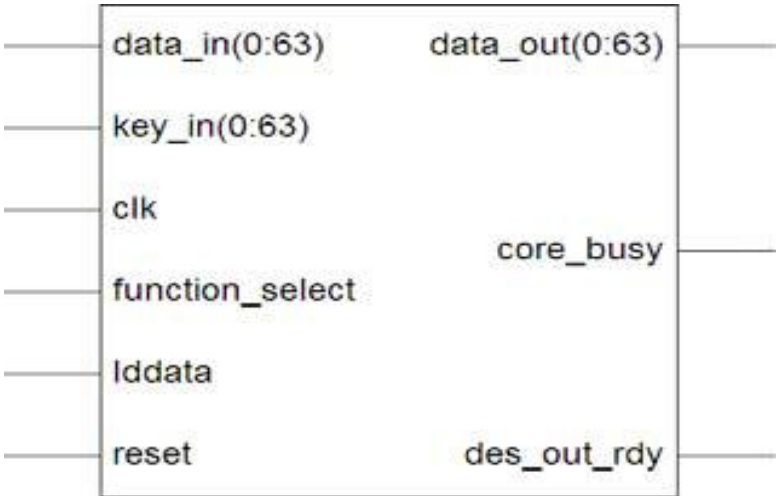


Figure 5. RTL Schematic of DES

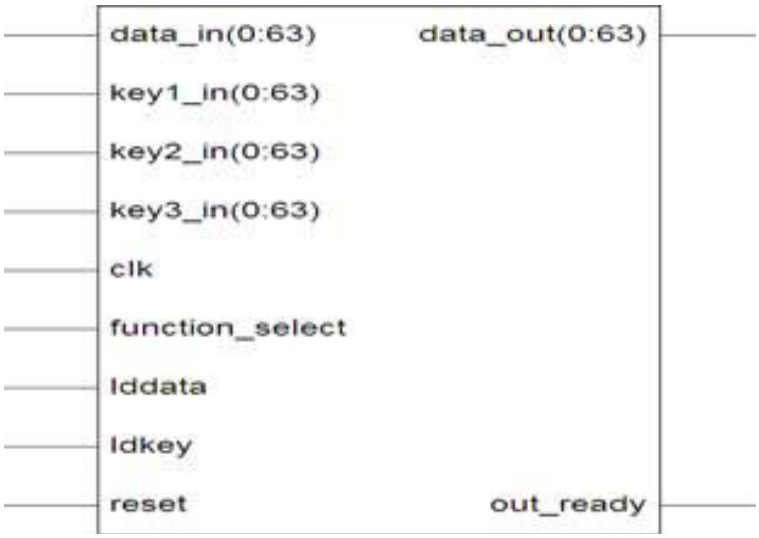


Figure 6. RTL Schematic of TDES

Figure 7 and Figure 8 illustrate the implemented components inside the chip. Additionally, the interconnections of the components are shown.

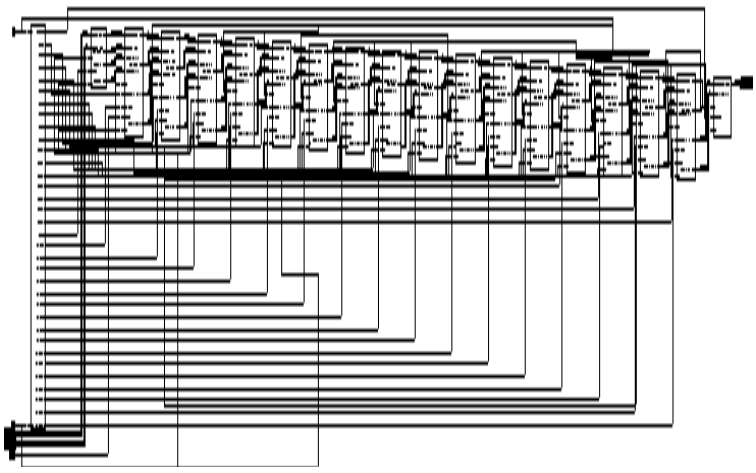

Figure 7. Technology Schematic of DES

 

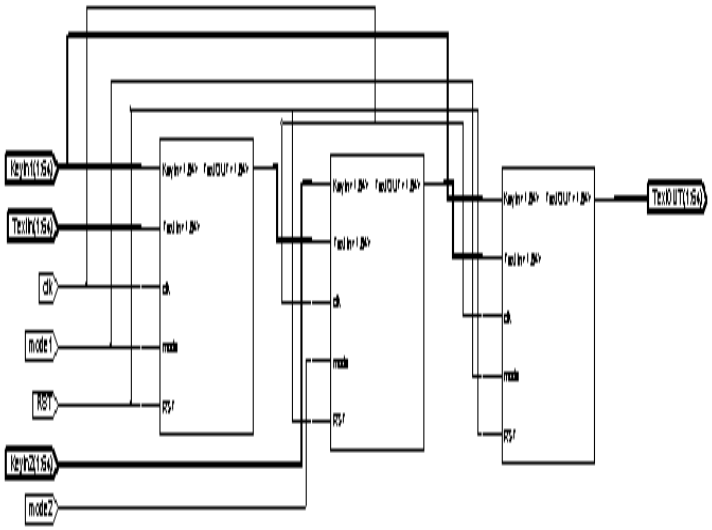


Figure 8. Technology Schematic of TDES

*B. Simulation Waveforms*

Figure 9 and 10 shows the waveforms for single Des block.

Encryption:

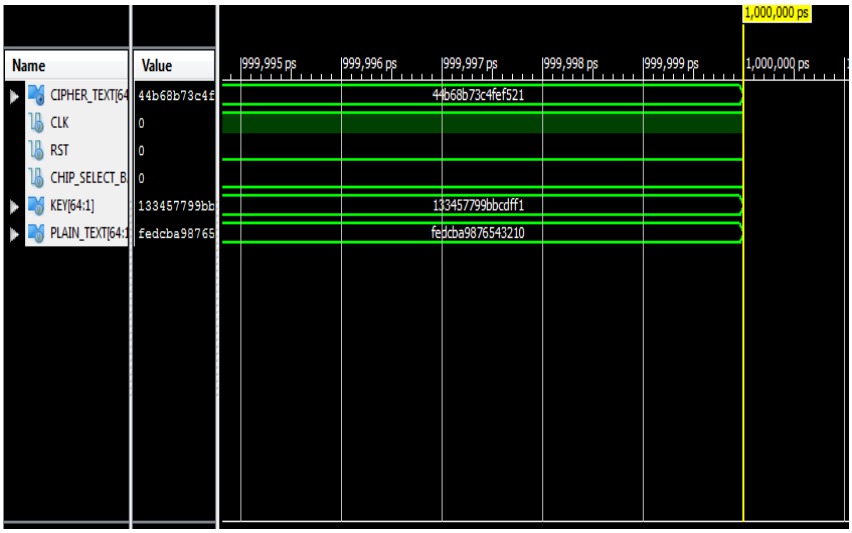


Figure 9. Encryption for single Des block

Decryption :

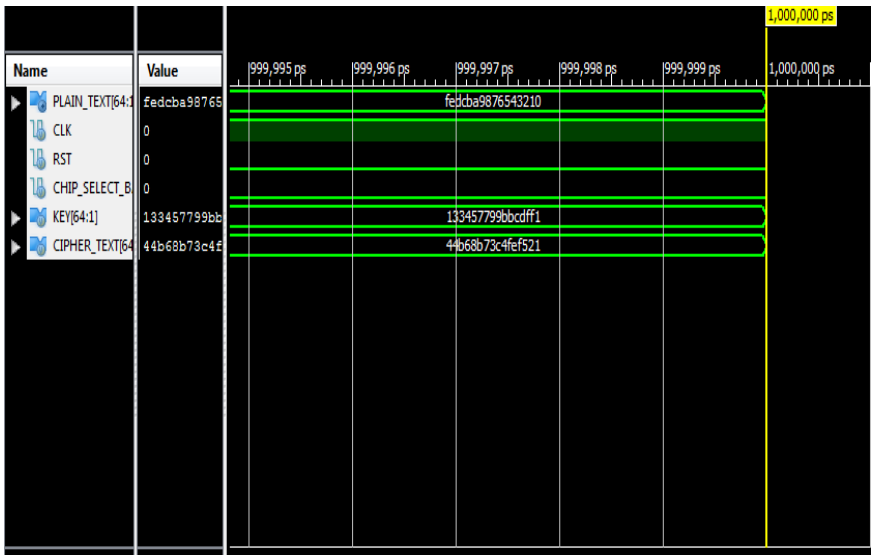


Figure 10. Decryption for single Des block

 

Figure 11 and 12 shows encryption and decryption both for TDES Systems.

Encryption :

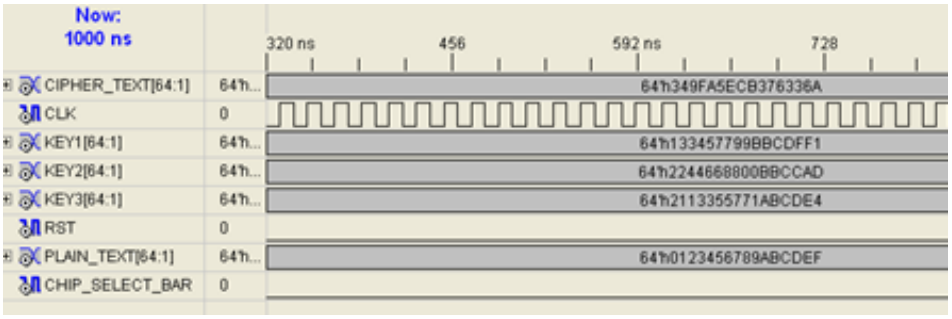


Figure 11. Encryption for Tdes Systems

Decryption:

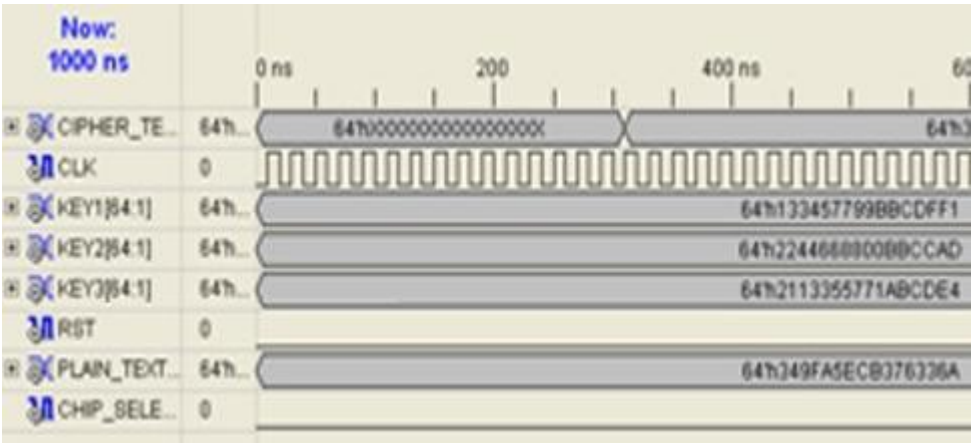


Figure 12. Decryption for Tdes Systems

## VI. CONCLUSION

The proposed implementation of DES and TDES provide high-speed performance with very compact hardware implementation. This paper examines the full procedure of implementing a DES and Triple DES algorithm using a high-level hardware description language verilog. It is a flexible solution for any cryptographic system and security layers of wireless protocol. The electronic payment industry uses Triple DES and continues to develop and promulgate standards based upon it to protect user content and system data.

## REFERENCES

[1] "Data Encryption Standard (DES)", Federal Information Processing Standard Publication, FIPS PUB 46-3, National Bureau of Standards, 1977.

[2] P. Kitsos, S. Goudevenos, "VLSI implementations of the triple-DES block cipher", Electronics, Circuits and Systems, ICECS 2003, Proceedings of the 2003 10th IEEE International Conference, pp 76-79, vol. 1, 2003

[3] T. Schaffer, A. Glaser, "Chip-package Co-implementation of a triple DES Processor", IEEE Transactions on Advanced Packaging, vol. 27 , pp. 194-202, 2004

[4] S. Praveen, M. Nagesh, "Implementaion of the Triple DES Block Cipher using VHDL", International Journal of Advances in Engineering & Technology, pp. 117-128, vol 3, issue 1, 2012.

[5] O. Hamdan, B. Zaidan, "New Comparative Study between DES, 3DES and AES within Nine Factors", Journal of Computing, pp. 152-157, vol 2, issue 3, 2010

[6] R. Shantamurty, "Implementing Triple DES (TCBC) on OpenVMS", OpenVMS Technical Journal, V15, 2010

[7] Aqib Al Azad, "Efficient VLSI Implementation of DES and Triple DES Algorithm with Cipher Block Chaining concept using Verilog and FPGA", International Journal of Computer Applications, pp. 6-15, vol 44, No. 16, 2012

[8] V. Kakarla, N.S.Govind, "FPGA Implementation of Hybrid Encryption Algorithm Based on Triple DES and RSA in Bluetooth Communication", International Journal of Applied Research & Studies, vol. 1, 2012

 