# A New Design of Algorithm for Enhancing Security in Bluetooth Communication with Triple DES

[1] B. Parsharamulu, [2] R. V. Krishnaiah

[1]M.Tech Student, DRK Inst of Science & Technology, Hyderabad, India
[2]PhD, M. Tech in CSE from JNTU Hyderabad, M. Tech in EIE from NIT, Warangal, India

**Abstract:** ***Bluetooth technology is an emerging wireless networking standard, which is based on chip that provides short-range wireless frequency hopping communication. Now, Bluetooth technology is mainly applied to the communication between mobile terminal devices, such as palm computers, mobile phones, laptops and so on. However, the phenomenon of data-leaking frequently arises in using the Bluetooth technology for data transfer. To enhance the security of data transmission in Bluetooth communication, a hybrid encryption algorithm based on DES and RSA is proposed. The currently used encryption algorithm employed by the Bluetooth to protect the confidentiality of data during transport between two or more devices is a 128-bit symmetric stream cipher called E0. The proposed hybrid encryption algorithm, instead of the E0 encryption, DES algorithm is used for data transmission because of its higher efficiency in block encryption, and RSA algorithm is used for the encryption of the key of the DES because of its management advantages in key cipher. Under the dual protection with the DES algorithm and the RSA algorithm, the data transmission in the Bluetooth system will be more secure. This project is extended with triple des in place of des to enhance more security.***

**Keywords:** E0 key stream, triple des, RSA, hybrid algorithm

## 1. Introduction

Encryption is an essential process to assure confidentiality over transmission channels, because channels are an open medium to intruders in which they can intercept and alter the contents of any transmitted information. Well known standardized encryption algorithms such as DES and AES were designed to achieve security against intruders. The encryption algorithm using in Bluetooth encryption process is the E0 stream cipher. However, this algorithm has some shortcomings, 128-bit E0 stream ciphers in some cases can be cracked by 0 (264) mode in some cases. So, for most applications that which need to give top priority to confidentiality, the data security is not enough if only use Bluetooth. Now I will introduce the Bluetooth mechanism, its disadvantages, and then propose a hybrid encryption algorithm to solve the current security risk in Bluetooth data transmission [1].

### 1.1 Draw backs of old algorithm

a. The weakness of E0 stream cipher algorithm
b. Limited resources capacity of linear feedback shift registers LFSR.

### 1.2 Symmetric-key cryptography

Symmetric-key cryptography refers to encryption methods in which both the sender and receiver share the same key (or, less commonly, in which their keys are different, but related in an easily computable way). This was the only kind of encryption publicly known until June 1976.

The data encryption standard (DES) and the Advanced Encryption Standard (AES) are block cipher designs which have been designated cryptography standards by the US government (though DES's designation was finally withdrawn after the AES was adopted).

#### 1.2.1 Des algorithm

Despite its deprecation as an official standard, DES (especially its still- approved and much more secure triple-DES variant) remains quite popular; it is used across a wide range of applications, from ATM encryption to e-mail privacy and secure remote access. Many other block ciphers have been designed and released, with considerable variation in quality [2].

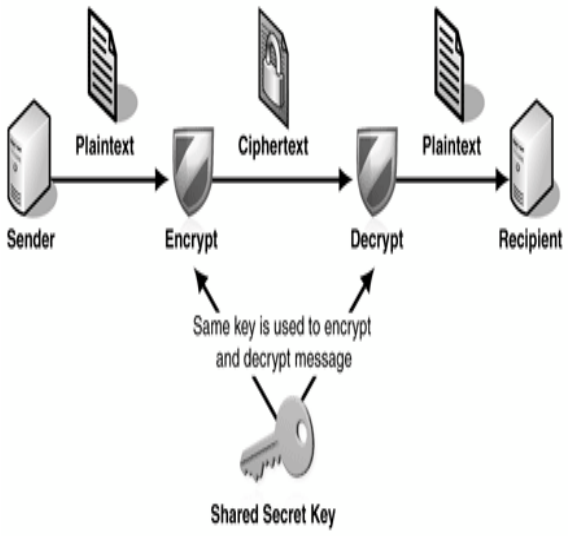


**Figure1:** Diagram for Symmetric-key cryptography

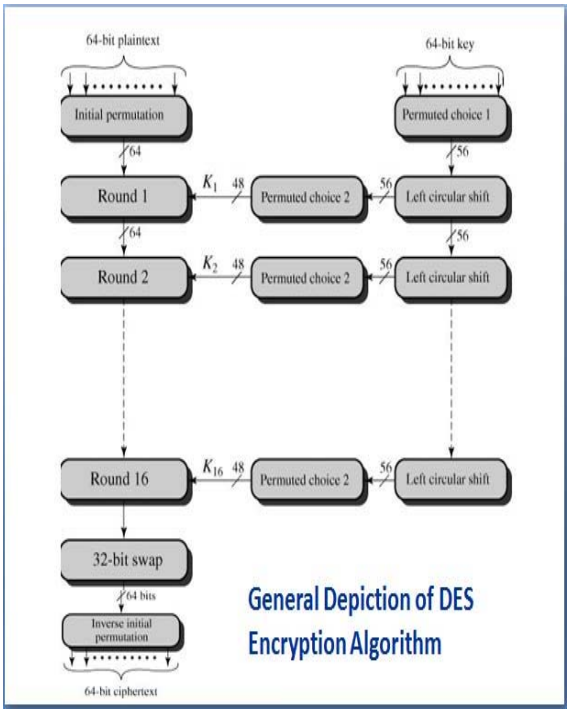


**Figure 2:** Des algorithm

The public key is typically used for encryption, while the private or secret key is used for decryption. Public-key algorithms are most often based on the computational complexity of "hard" problems, often from number theory. For example, the hardness of RSA is related to the integer factorization problem.

### 1.2.2 Single round of des algorithm

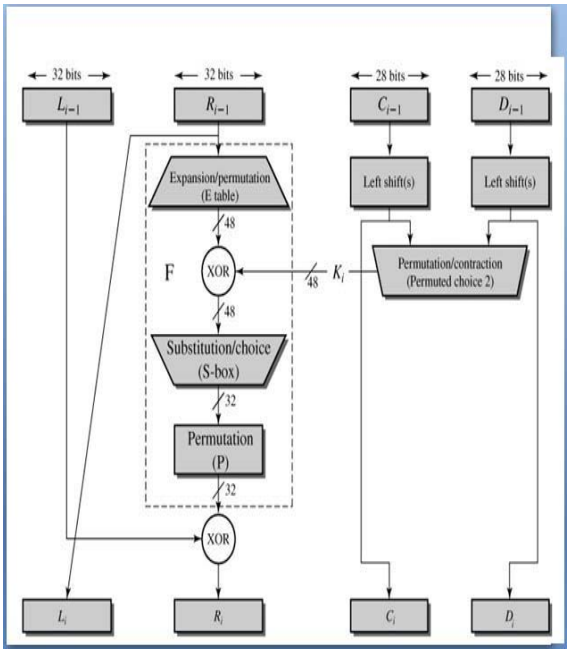


**Figure 3:** Single round of des algorithm

### 1.2 Public-key cryptography

In a groundbreaking 1976 paper, Whitfield Diffie and Martin Hellman proposed the notion of public-key (also, more generally, called asymmetric key) cryptography in which two different but mathematically related keys are used — a public key and a private key In public-key cryptosystems, the public key may be freely distributed, while its paired private key must remain secret. The public key is typically used for encryption, while the private or secret key is used for decryption.

Public-key algorithms are most often based on the computational complexity of "hard" problems, often from number theory. For example, the hardness of RSA is related to the integer factorization problem.

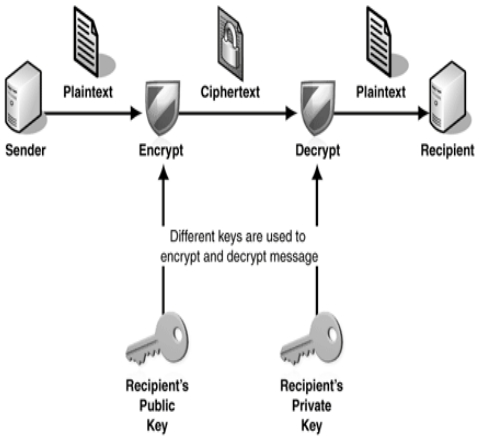


**Figure 4:** Public-key cryptography

### 1.3.1 RSA algorithm

First of all, two large distinct prime numbers p and q must be generated. The product of these, we call n is a component of the public key. It must be large enough such that the numbers p and q cannot be extracted from it - 512 bits at least i.e. numbers greater than 10154. We then generate the encryption key e which must be co-prime to the number m = ϕ (n) = (p − 1) (q − 1). We then create the decryption key d such that demodm = 1. We now have both the public and private keys [3].

Cipher text(C) = M^e mod (n).
Plain text (M) = C^d mod (n).

## 2. The Encryption Algorithm in Bluetooth Security Mechanism

The Bluetooth specification defines three security modes:

1) Safe Mode 1: No safe mode, which has the lowest security level.
2) Safe Mode 2: service-oriented security model, which start after the establishment of the channel.
3) Safe Mode 3: link-oriented security model, which install and initial before communication link is established [4].

### 2.1 The ideas and processes of hybrid algorithm

RSA algorithm is the first relatively complete public key algorithm. It can be used for data encryption, also can be used for digital signature algorithms. RSA cryptosystem is used on the difficulty of integer factorization in the group, and its security establishes in the assumption that constructed by almost all the important mathematicians, it is still a theorem that does not permit, which is lack of

proof, but Mathematicians believe it is existent.

DES is a group cipher algorithm, which encrypts data by a group of 64-bit. A group of 64-bit plaintext is entered from one beginning of the algorithm; 64-bit cipher text is exported from the other side. DES is a symmetric algorithm, encryption and decryption use the same algorithm (e the different key arrangement), the key can be any 56-bit value (the key is usually 64-bit binary number, but every number that is a multiple of 8-bit used for parity are ignored). This algorithm uses two basic encryption techniques, make them chaos and spread, and composite them [6].

Seeing from the efficiency of encryption and decryption, DES algorithm is better than the RSA algorithm. The speeds of DES encryption is up to several M per second, it is suitable for encrypting large number of message; RSA algorithm is based on the difficulty of factoring, and its computing velocity is slower than DES', and it is only suitable for encrypting a small amount of data, The RSA encryption algorithm used in the. NET, it encrypts data at most 117 bytes of once. Seeing from key management, RSA algorithm is more superior to the DES algorithm. Because the RSA algorithm can distribute encryption key openly, it is also very easy to update the encryption keys, and for the different communication objects, just keep the decryption keys secret; DES algorithm requires to distribute a secret key before communication, replacement of key is more difficulty, different communication objects, DES need to generate and keep a different key [7].

Based on the comparison of above DES algorithm and RSA algorithms, in order to give expression to the advantages of the two algorithms, and avoid their shortcomings at the same time, we can conceive a new encryption algorithm, that is, DES and RSA hybrid encryption algorithm. We will apply hybrid encryption algorithm to Bluetooth technology, we can solve the current security risks of Bluetooth technology effectively.

The entire hybrid encryption process is as follows: Let the sender is A, the receiver is B, B's public key is eB, B's private key is dB, K is DES encryption session key (assuming that the two sides of communication know each RSA public key).

### 2.2 Process of encryption

During the process of sending encrypted information, the random number generator uses 64-bit DES session key only once, it encrypt the plaintext to produce cipher text. On the other hand, the sender get debit's public key from public key management centre, and then using RSA to encrypt session key. Finally, the combination of the session key from RSA encryption and the cipher text from DES encryption are sent out.

1) Bluetooth packet plaintext M is divided into 64-bit plaintext Mi (i=1, 2… n)).
2) Crypts Mi for 16 cycles by 64-bit key K ,and Mi will turn into a 64-bit cipher text Ci (i = 1,2, ... n), then all the Ci (i =1,2 , ... n) are combined into cipher text C. The second, RSA algorithm encrypts the key of DES algorithm.
3) Obtain RSA public key of receiver B from the key server, or other sources.
4) Make DES 64-bit session key K for RSA encryption by public key eB that obtains from recipient, then a session key encrypted information CK is formed.
5) Composite Cipher text message C from the use of DES encryption, and session key CK from RSA encryption, we can get the hybrid CM for transmission. Figure is the whole mixed-encryption process.

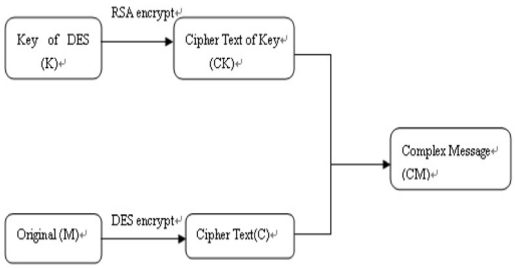


**Figure 5:** The whole mixed-encryption process

### 2.3 Process of decryption

The decryption of hybrid encryption algorithm is as follows. The first, the receiver B divide received cipher text CM into two parts, one is cipher text CK from the RSA algorithm encryption, and the other is cipher text C from the DES algorithm encryption. The second, the receiver B decrypt cipher text CK by their private key dB, receive the key K which belongs DES algorithm, then decrypt the cipher text C to the original M by key K. Figure is a decryption of hybrid encryption algorithm [5].

## 3. Proposed Hybrid Algorithm with Triple DES

The Triple Data Encryption Algorithm (TDEA) is made available for use by Federal agencies within the context of a total security program consisting of physical security procedures, good information management practices, and computer system/network access controls.

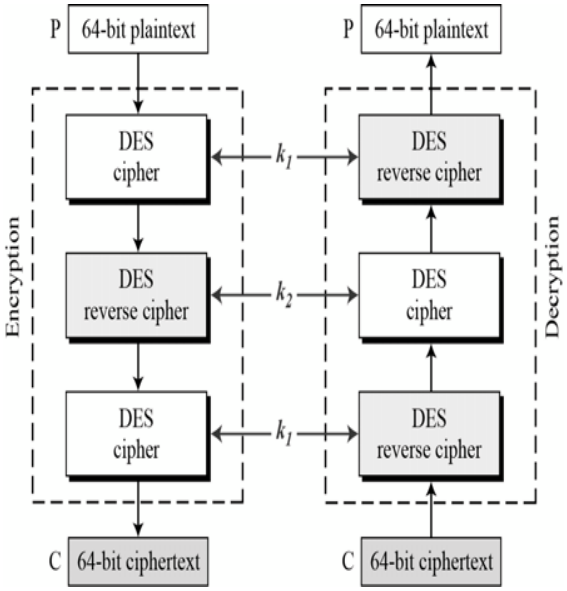


**Figure 6:** Proposed hybrid algorithm with Triple DES

Triple DES uses a "key bundle" which comprises three DES keys, K1, K2 and K3, each of 56 bits (excluding parity bits). The encryption algorithm is:

Cipher text = EK3 (DK2 (EK1 (plaintext))) I.e., DES encrypts with K1, DES decrypt with K2, and then DES encrypt with K3. Decryption is the reverse: Plaintext = DK1 (EK2 (DK3 (cipher text))) i.e., decrypt with K3, encrypt with K2, and then decrypt with K1.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.

Using standard DES encryption, TDES encrypts data three times and uses a different key for at least one of the three passes. The DES "modes of operation" may also be used with triple-DES. This 192-bit (24 characters) cipher uses three separate 64-bit keys and encrypts data using the DES algorithm three times. While anything less than that can be considered reasonably secure only the 192 bit (24 characters) encryption can provide true security. One variation that takes a single 192 bit (24 characters) key and then: encrypts data using first 64 bits (eight characters), decrypts same data using second 64 bits (eight characters), and encrypts same data using the last 64 bits (eight characters). For some time, it has been a common practice to protect and transport a key for DES encryption with triple-DES. This means that the plaintext is, in effect, encrypted three times. 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.
- D E S -EEE2 and DES-EDE2: Same as the previous formats except that the first and third operations use the same key.

In this paper this hybrid encryption algorithm is proposed with triple des algorithm in the place of des algorithm. In triple des here we using 3 keys to encrypt the data, so the key strength becomes stronger, the data will be more secure.

## 4. Simulation Results

### 4.1 DES and RSA Hybrid Encryption Result

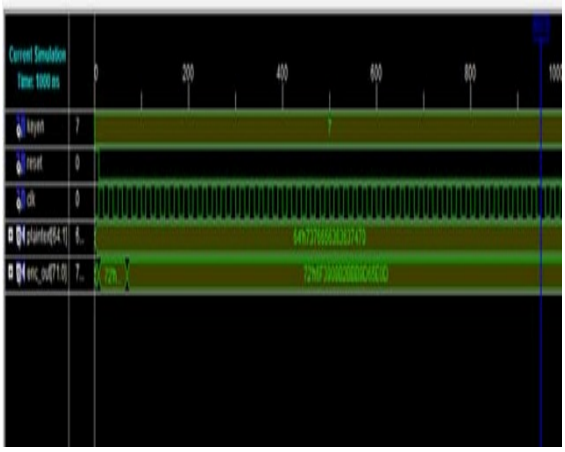

**Figure 7:** Des and RSA Hybrid Encryption Result

### 4.2 DES and RSA hybrid decryption result

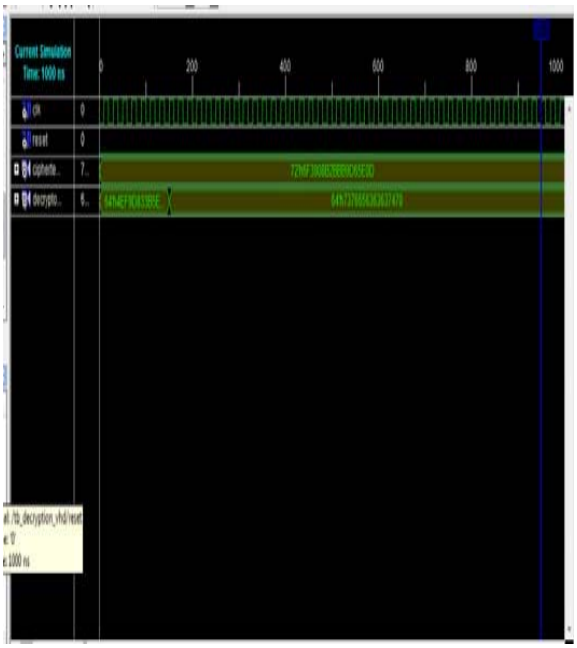

**Figure 8:** Des and RSA hybrid decryption result

### 4.3 TDES and RSA hybrid encryption result

**Figure 9:** TDES and RSA hybrid encryption result

### 4.4 TDES and RSA hybrid decryption result

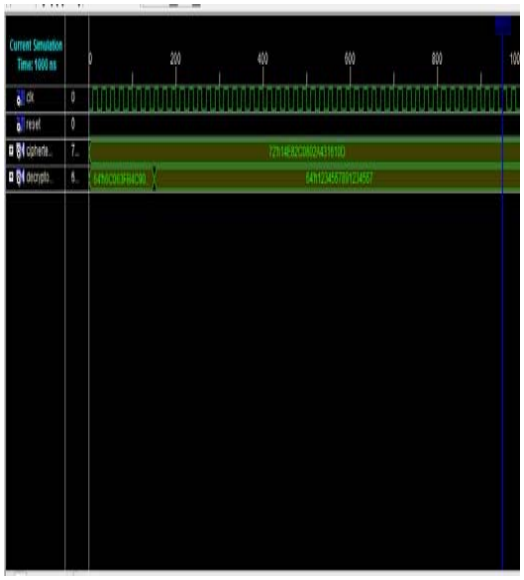

**Figure 10:** TDES and RSA hybrid decryption result

## 5. The Advantages of Hybrid Encryption Algorithm

- Using RSA algorithm and the DES key for data transmission, so it is no need to transfer DES key secretly before communication.
- Management of RSA key is the same as RS situation, only keep one decryption key secret.
- Using RSA to send keys, so it can also use for digital signature.
- The speed of encryption and decryption is the same as DES. In other words, the time-consuming RSA just do with DES keys.

### 5.1 Future Scope

This project leads to very useful to implement hybrid algorithms in Bluetooth communication technology. With the help of many algorithms like idea, Des, md5 and RSA, we can implement many hybrid algorithms for Bluetooth communication to enhance more security. This triple des and RSA hybrid algorithm further extended with triple des and triple RSA to enhance more security.

## 6. Conclusion

Bluetooth technology is a new technology, which will change our transmission method. As communication networks, it uses wireless channel for the transmission medium. Compared to the fixed network Bluetooth network is more vulnerable to be attacked. Currently, stream cipher E0 used in Bluetooth standard has many shortcomings, while the DES and RSA hybrid encryption algorithm is relatively more secure and easier to achieve, thus ensures data transmission between the Bluetooth device safety and real-time. As long as we protect the key that encrypt original, and the security of entire file will be guaranteed. Because of the dual protection of DES algorithm and RSA algorithm, the data in transit is safe.

## References


[1] Zheng Hu Network and Information Security [M], Peking; Tsinghua University.
[2] Data encryption using DES/Triple DES functionality in Spartan-II FPGAS, Amit Dhir
[3] Cryptanalysis of Bluetooth key stream Genarator two-levl E0. YiLu and Serge Vaudenay
[4] Recommendations of the TDEA block cipher revised William C.Barker.
[5] Cracking the Bluetooth PIN, Yaniv Shaked and Avishai Wool.
[6] Man Young Rhee. Network Security Encryption Principle, algorithm and Protocol [M]. Peking: Tsinghua University Press, 2007.
[7] WUxing-Hui ZHOU Yu-Ping.”Analysis of data encryption algorithm based on WEB”.


## Author Profile


**B. Parsharamulu** received B.Tech Degree in Computer Science & Engineering from Avanthi Inst of Engineering & Tech (2011), Hyderabad, and currently pursuing the M.Tech in CSE from JNTU Hyderabad.

**Dr. R. V. Krishnaiah** has received Ph.D from JNTU Ananthapur, M.Tech in CSE from JNTU Hyderabad, M.Tech in EIE from NIT (former REC) Warangal and B.Tech in ECE from Bapatla Engineering College. He has published more than 50 papers in various journals. His interest includes Data Mining, Software Engineering, and Image Processing.