www.ijecs.in

International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 5 May 2015, Page No. 11804-11806

A Hybrid Encryption Algorithm Based on DES and RSA In Bluetooth Communication

[1]*S.Prabhakar*, [2]*Cha. Swamy*, [3] *S.Ravi Kumar*

ABSTRACT: The 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. It may be broken under certain conditions with the time complexity O(2^{64} **).**

To enhance the security of data transmission in algorithm based on Data Encryption Standard (DES) and Rivets Shamir Adelman (RSA) is proposed

***Keywords**:* Encryption, Decryption, RSA algorithm. DES algorithm, Pipelining.

I. INTRODUCTION

A message in its original form (plaintext) is converted (encrypted) into an unintelligible form (cipher text) by a set of procedures known as an encryption algorithm (cipher) and a variable, called a key.

The cipher text is transformed (decrypted) back into plaintext using the decryption algorithm and a key.

Keys are rules used in algorithms to convert a document into a secret document.

Keys are of two types:

A) Symmetric.

B) Asymmetric.

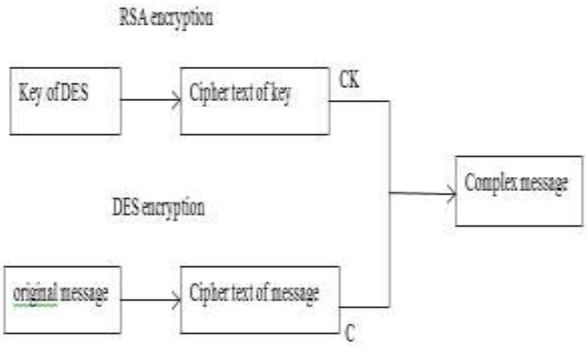
A key is symmetric if the same key is used both for encryption and decryption.

A key is asymmetric if different keys are used for encryption and decryption, depending on the criteria.

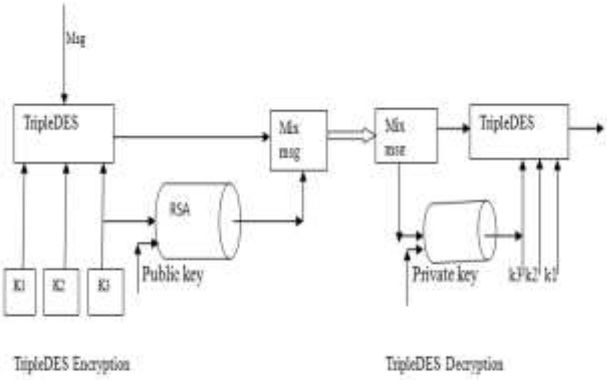
II. Hybrid Encryption Algorithm

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, is called Hybrid Encryption Algorithm.



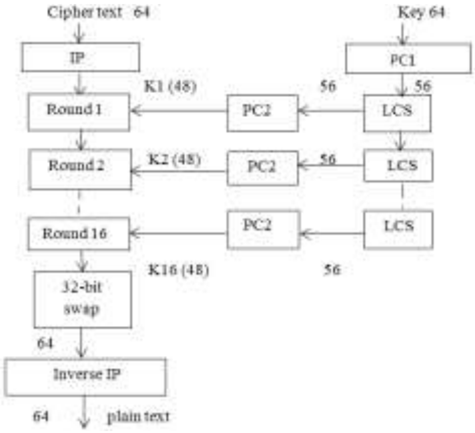
III. Hybrid Encryption Triple DES and RSA



Triple-DES is an extension of Data Encryption Standard (DES) that results in a more complex but more secure block cipher. Unlike DES 3-DES uses 3 64 bit keys and operates on 64 bit plain text to produce 64 bit cipher text. RSA algorithm encrypt one of the 3 keys of 3-DES. 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 3-DES algorithm and the RSA algorithm, the data transmission in the system will be more secure. 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, 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

IV. RSA algorithm

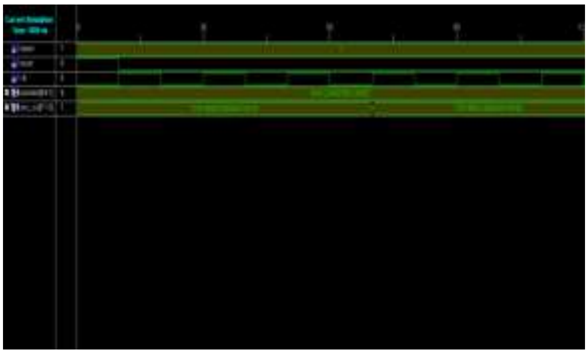
In cryptography, RSA is an algorithm for public key cryptography The RSA algorithm involves the use of two keys a public key, which may be known by anybody, and can be used to encrypt messages. A private key, known only by the recipient, and used to decrypt messages.



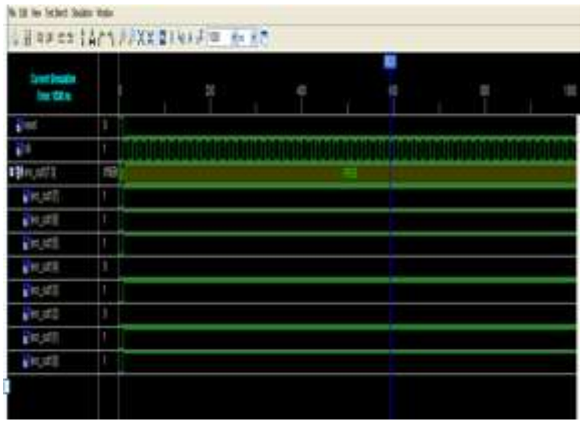
DES Description

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. 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 10^{154}. We then generate the encryption key *e* which must be co-prime to the number m = ψ(n) = (p - 1)(*q* - 1) We then create the decryption key *d* such that de modem = 1. We now have both the public and private keys.

Hybrid Encryption Triple DES and RSA



V. Implementing Hybrid Encryption Triple DES and RSA using chip scope



VI. CONCLUSION

Bluetooth technology is a new technology. However, the Bluetooth technology has not fully considerate security issues in the standardization process. As communication networks, it uses wireless channel for the transmission medium. Compared to the fixed network Bluetooth network is more vulnerable to be attacked. For the applications that take data security as priori, achieving a high level of data security is essential. Currently, stream cipher E0 used in Bluetooth standard has many shortcomings, while the 3DES 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

VII. FUTURE SCOPE

For limited security options we can still prefer DES with pipelining for efficient operation.

We can also induce much required speed by pipelining in Triple DES.

In future We can improve this triple DES by increasing its speed by using buffers and reduce its size by using compact DES .

VIII. REFERENCE

[1] Zheng Hu. Network and Information Security [M]. Peking: Tsinghua University Pres,2006.

[2] Man Young Rhee. Network Security Encryption Principle, algorithm and Protocol[M]. Peking: Tsinghua University Pres, 2007.

[3] Suri , P. R . ; Rani , S. Bluetooth security Need to increase the efficiency in pairing [J]. IEEE/ Southeastcon , 2008.

[4] Fengying Wang. Dynamic Key 3DES Algorithm of Discrete System Based on Multi-dimension Chaos[J]. Microelectronics and Computer, 2005, 7: 25-28.

[5] Falk A. The IETF, the IRTF and the networking research community[C].Computer Communication Review, v35, n5 , Oct . 2005.

S.Prabhakar , a student of Hyderabad Institute of Technology And Management and his areas of interest in Embedded systems, Digital designs.

CH.A.Swamy working as Assoc.professor in Marri Laxman Reddy institute of technology and Management .And his areas of interest in vlsi design, Embedded system-design, cmos Technologies.

S.Ravi kumar, a student of Hyderabad Institute of Technology And management and his areas of interest in Ardunio, Embedded System.