International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Cryptography Algorithm based on DES and RSA in Bluetooth Communication

Veeresh K.[1], Arunkumar Madupu[2]

[1]M. Tech Student, Malla Reddy collage of engineering &Technology, Hyderabad, India,

[2]Assistant Professor, Department of ECE, Malla Reddy collage of engineering & Technology, Hyderabad, India

Abstract: ***At present, 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. Due to higher efficiency in block encryption, hybrid encryption algorithm is used, instead of the E0 encryption 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. The RSA algorithm is used 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.***

Keywords: Bluetooth; E0 key stream; hybrid encryption algorithm; data transmission

1. Introduction

Bluetooth technology has the characteristic of wireless, openness, low power and so on. However, the phenomenon of data-leaking frequently arise in using the Bluetooth technology for data transfer, since the emergence of Bluetooth, even if the Bluetooth takes the very robust security measures, there are still serious security risks. The encryption algorithm using in Bluetooth encryption process is the E0stream 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. Shown in Fig. 1&2

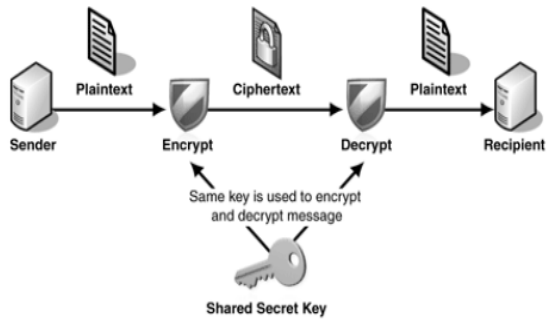


Figure 1

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
c) Low credibility of PIN
d) Address Spoofing

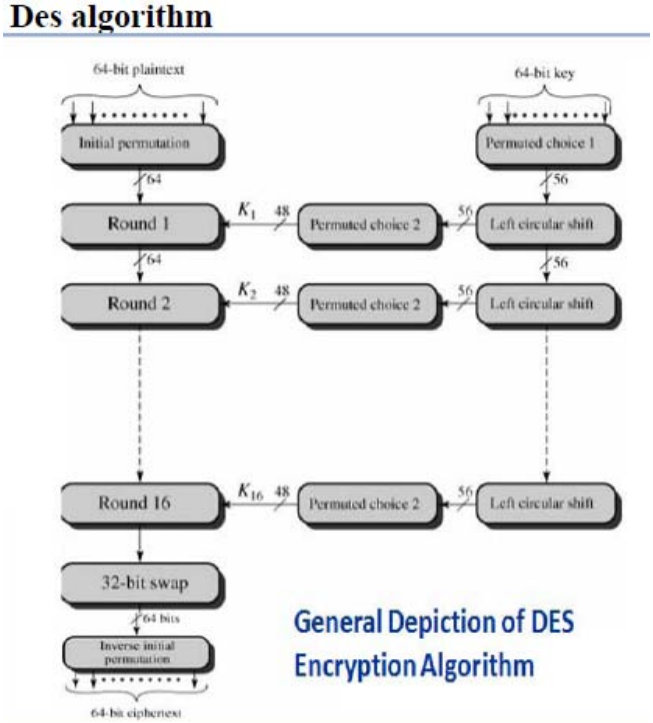


Figure 2

2. 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 = $\phi(n) = (p - 1)(q - 1)$. We then create the decryption key d such that demodm = 1. We now have both the public and private keys.

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

3. The encryption algorithm in Bluetooth security mechanism

The Bluetooth specification defines three security **modes**:

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

4. The 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 253 (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. 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.

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 then 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).

4.1. 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 center, 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.

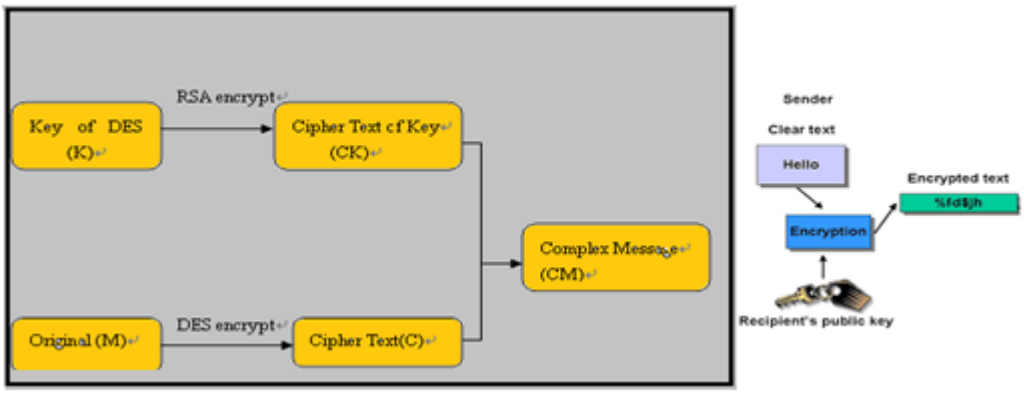


Figure 4.1

4.2. 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 own private key dB, receive the key K which belongs DES algorithm, then decrypt the cipher text C to the original M by key K.

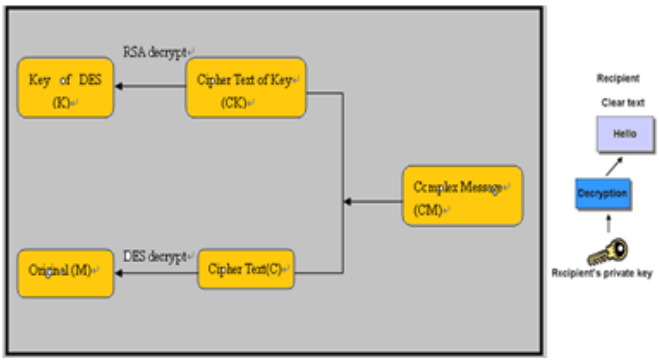
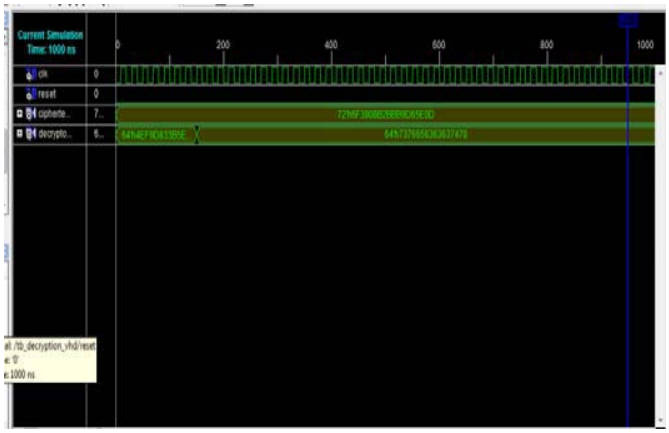
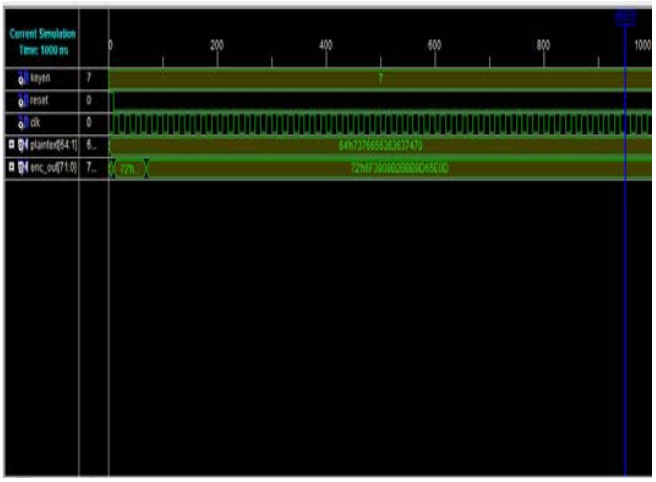


Figure 4.2

5. Simulation Results



DES and RSA Hybrid Decryption Result



DES and RSA Hybrid Encryption Result

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.

6. Future Scope

This project leads to very useful to implement hybrid algorithms in Wi-Fi communication technology. With the help of many algorithms like idea, AES, MD5 and RSA, we can implement many hybrid algorithms for Bluetooth 255 communication to enhance more security. This triple des and RSA hybrid algorithm further extended with triple des and triple RSA to enhance more security for Wi-Fi.

7. 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 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].Computerb Communication Review, v35, n5, Oct. 2005:6970
[6] Yaniv Shaked, Avishai Wool . Cracking t he Bluetooth P[C]. 3rd USEN IX/ ACM Conf. Mobile Systems, Application and Services (MobiSys).Seattle, WA , J une 2005 :39250.
[7] Data encryption using DES, AmitDhir

Author Profile

Veeresh K received his B. Tech degree in electronics &communication from VTU University, Belgaum in 2012, and currently pursuing M. Tech in the specialization of VLSI & Embedded System at Malla Reddy College of engineering & technology Hyderabad, India

Arunkumar Madupu received his B. Tech Degree in Electronics & Communication Engineering from JNT University, Hyderabad, and M. Tech degree in VLSI System Design from JNT University, Hyderabad and MBA from Pondicherry Central University, India. He is currently working as Assistant Professor in the Dept. of ECE, Malla Reddy College of Engineering and Technology, Hyderabad, India.