CHITTAGONG UNIVERSITY OF ENGINEERING AND TECHNOLOGY
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
CHITTAGONG-4349

(Thesis Proposal)

Application for the approval of B.Sc. Engg. Thesis (Computer Science & Engineering)

Date: April 22, 2013

1. **Name of the Student** : Md. Akibul Alam
   Roll No : 0804060 **Sessions:** 2011-12

2. **Present Address** : 310, Shaheed Mohammad Shah Hall
   Chittagong University of Engineering &Technology
   Chittagong-4349, Bangladesh.

3. **Name of the Supervisor** : Thomas Chowdhury
   Designation : Assistant Professor
   Department of Computer Science & Engineering
   Chittagong University of Engineering & Technology
   Chittagong-4349, Bangladesh.

4. **Name of the Department** : Computer Science & Engineering
   Program : B.Sc. Engineering

5. **Date of First Enrolment**
   In the Program : March 01, 2009.

6. **Tentative Title** : Enhance Bluetooth Security by Improving
   RSA Algorithm.

7. Introduction

Bluetooth is a short range wireless radio specification adhoc network designed to replace wire as the medium for data and voice signal between electronic devices operates in the unlicensed 2.4000 gigahertz (GHz) to 2.4835 GHz Industrial, Scientific, and Medical (ISM) frequency band planned and implemented by Bluetooth Special Interest Group. For Bluetooth communication security issue currently used 128 bit symmetric stream cipher called an encryption algorithm. This symmetric cipher may be broken under certain conditions. There also popularly used algorithm for Bluetooth security like Data Encryption Standard (DES) and Ron Rivest, Adi Shamir and leonard adleman (RSA) algorithm. These algorithms are vulnerable to possible attacks. To remedy these limitations and increase the security in Bluetooth communication this paper proposes an algorithm that may consider as improved RSA for the Bluetooth communications. Authentication, confidentiality and integrity will be achieved together using this algorithm.

8. Background and Related Research Work

Communication technology has been developed day by day. Researchers put remarkable contributions in Bluetooth communication. A solution to the short comings [1] 128-bit E0 stream ciphers in some cases can be cracked, Low credibility of PIN, High probability of non-link key cheat, Address Spoofing present in existing security system of Bluetooth. There is a hybrid system based on DES and RSA. DES is a symmetric key cryptographic algorithm and RSA is an asymmetric key cryptographic algorithm. In which public and private key pair is used. Here DES use symmetric key and the size of the key is 56-bit only that is more vulnerable to attacks like brute force attack, man-in-middle attack etc. A solution to the limitations [2] of the E0 stream cipher that is used in Bluetooth System, by using DES algorithm. The problem with this approach is distribution of encryption key used in DES. In which both communication parties agree on one shared secret key that is known as symmetric key. But the problem arises that how one party exchange this secret key with other party because it is possible that opponent can intercept the key during transmission of symmetric key. Another problem is again the small size of the key that is highly vulnerable to brute force attack. Key agreement protocols [3] used in Bluetooth communication security and weakness of Bluetooth transmission. That paper [3] gave an outline about generation of keys that are used to implement security in Bluetooth communication like encryption key generation, link key generation, unit key generation, initialization key generation and combination key generation. The security issues of Bluetooth standard **[**4] and introduced security frame work which includes both link level and service level security schemes [5] [6]. Flexible security architecture is implemented at service level security. In the security frame work security modes can be defined for each Bluetooth device. This article gives an analysis of potential risks, attacks against the vulnerabilities like DOS, man-in–middle attack, spoofing, session hijacking, eavesdropping etc. this countermeasures is to improve Bluetooth security.

9. Objectives

- Understand the basics of Bluetooth technology and its networking concepts.
- Describe the Bluetooth technology, its historical evaluation, and some applications scenarios, and fundamental terminology.
- Improving the RSA algorithm for Bluetooth communication.
- Implementing the improved algorithm.

10. Outline of Methodology Design

This paper describes the security of Bluetooth network and reduces the weakness of the RSA algorithm. Here RSA is modified by using public key and private key, then the algorithm perform the task of security. This modification is advantageous because the fact the public and private keys in the public key system are related in such a way that only the public key can be used to encrypt the messages and only the corresponding private key can be used to decrypt them. Moreover, it is virtually impossible to deduce the private key if you know the public key.

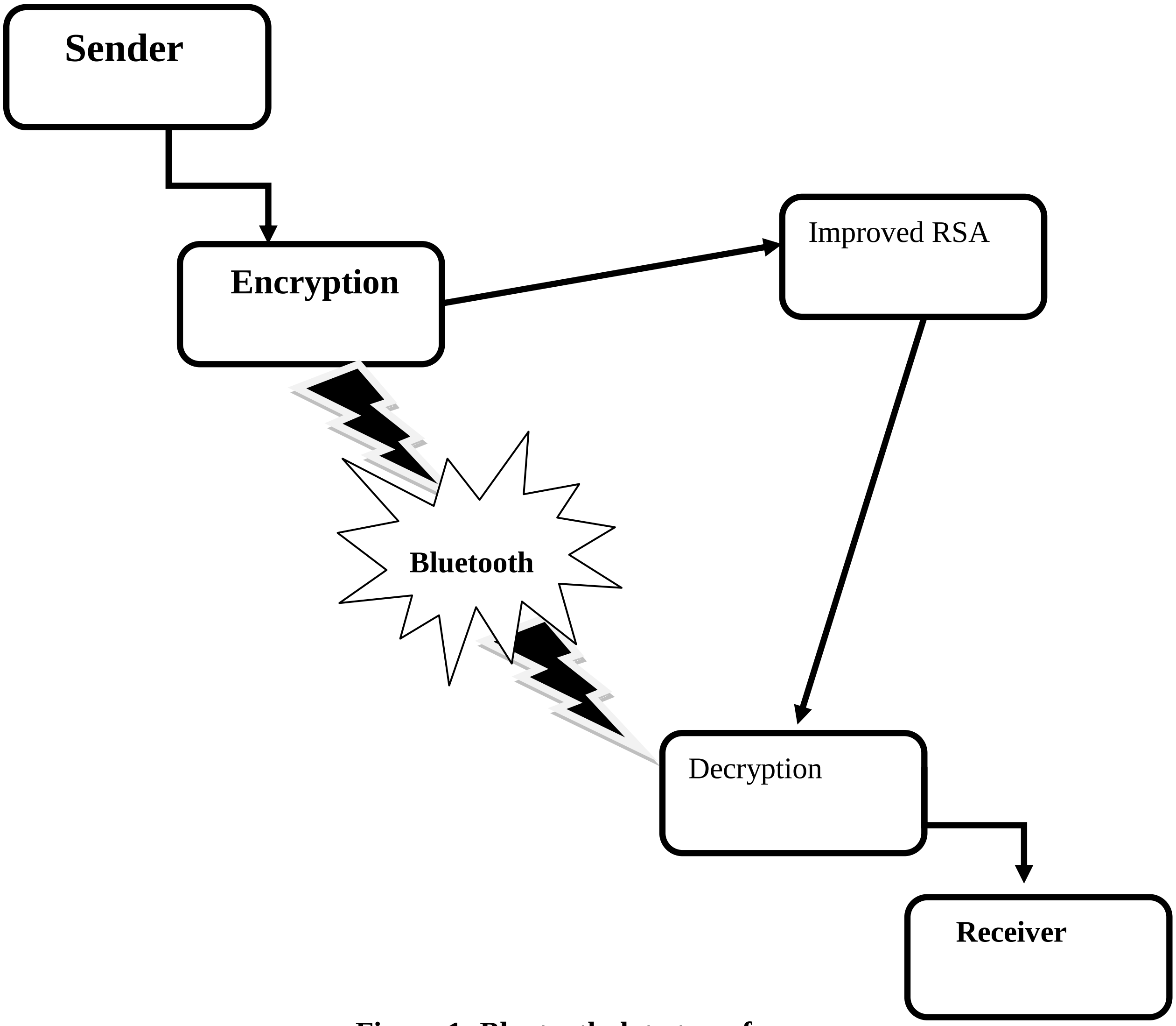

Figure 1: Bluetooth data transfer process

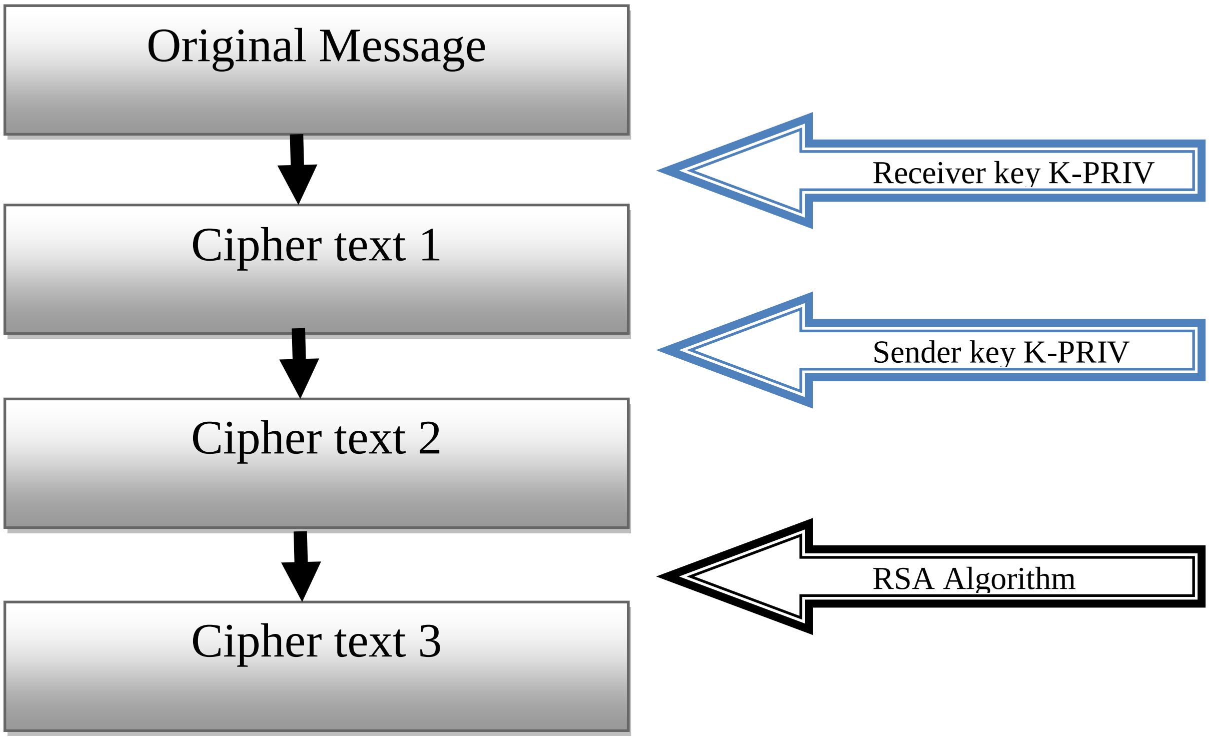

Figure 2: Encryption Improvements

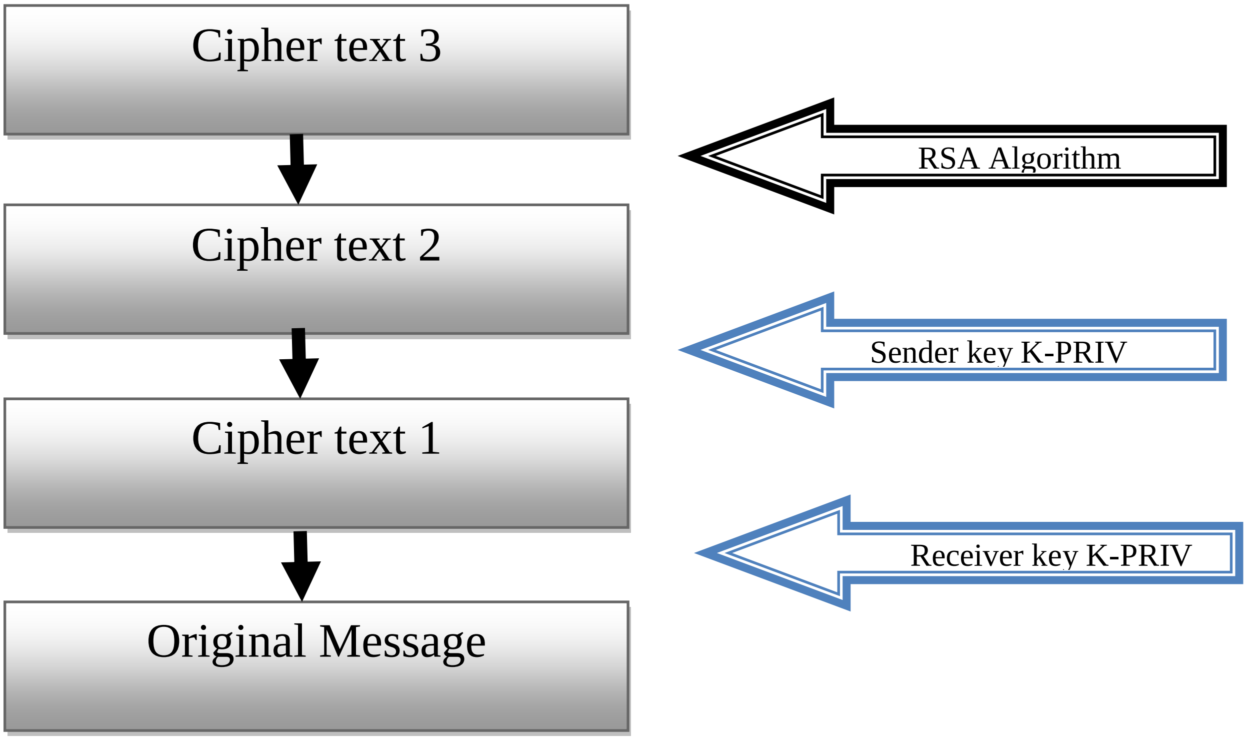

Figure 3: Decryption Improvements

7. Resources Required to Accomplish the Task

- Personal Computer.
- Operating System windows XP/7.
- MATLAB.
- Bluetooth Device.

8. Cost estimation

Bluetooth Devices	- 1000 TK.
Miscellaneous	- 1000 TK.

9. References

[1] Wuling Ren, Zhiqian Miao, "*A Hybrid Encryption Algorithm Based on DES and RSA in Bluetooth Communication",* International Journal of Computer Science and Security (IJCSS), Vol.2,: Issue No .2,Year 2011.

[2] Li Juan, Chen Bin, Li Kun, "*Study on the Improvement of Encryption Algorithm of Bluetooth*" 21-23 Oct. 2011, in conference of Computational and Information Sciences (ICCIS), 2011 International Conference, pp. 971 – 974.

[3] Trishna Panse, Vivek Kapoor, Prashant Panse, "*A Review on Key Agreement Protocols used in Bluetooth Standard and Security Vulnerabilities in Bluetooth Transmission*" International Journal of Information and Communication Technology, Research, Volume 2, Number 3, 2012.

[4] Jun-Zhao Sun, Douglas Howie, Antti Koivisto and Jaakko Sauvola, Media Team, Machine Vision and Media Processing unit, InfoTech Oulu, University of Oulu, Finland "*Design Implementation and Evaluation of Bluetooth Security",* http://www.mediateam.oulu.fi/publication/pdf/83.pdf.

[5] Trishna Panse, Vivek Kapoor, "*A Review paper on Architechture and Security system of Bluetooth Transmission*" International Journal of Advanced Research in Computer Science, Volume 3, No. 1, Jan-Feb 2012.

[6] Trishna Panse, Vivek Kapoor, "*A Review on Security Mechanism of Bluetooth Communication*", International Journal of Computer Science and Information Technologies,Vol. 3 (2), August, 2012.

10. CSE Undergraduate Studies Committee Reference:

Meeting No: Resolution No: Date:

11. Number of Undergraduate Students Working with the Supervisor at Present:

Signature of the Student

Signature of the Supervisor

--
Signature of the Head of the Department