International Journal of Research (IJR)
e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 11, November 2015
Available at http://internationaljournalofresearch.org

Secure Data Communication between Two Army Stations

Katti Rajesh Khanna[1]& Prof. Yerraboina Sreenivasulu[2]

[1]PG Scholar,Dept of ECE, GVR&S College of Engg & Tech,Budampadu,Guntur,Andhra Pradesh.
[2]Professor&HOD,Dept of ECE, GVR&S College of Engg & Tech,Budampadu,Guntur,Andhra Pradesh.

Abstract:

Nowadays confidential data transfer is a crucial task in many multinational companies, military departments, intelligence and surveillance departments, and so on. In such departments and companies lots of efforts are put forth for securing confidential data. Therefore, they need Data encryption and decryption for their applications. An example, which is given below describes data encryption and decryption to secure data using Zigbee wireless communication technology for short distances. A popular way to protect data is to encrypt the data while sending and decrypt it while receiving to regain the original message. Before transmitting, the data is converted into unreadable format, and then the data is encrypted and decrypted in the receiver end to get the original message. Let us demonstrate the project in brief with the help of a block diagram given below.

Keywords: ARM7 LPC2148; Zigbee; LCD display

I.INTRODUCTION :

An embedded system is a special-purpose computer system designed to perform a dedicated function. Since the system is dedicated to specific tasks, design engineers can optimize it, reducing the size and cost of the product. Embedded system is fast growing technology in various fields like industrial automation, home appliances, automobiles, aeronautics etc. Embedded technology uses pc or a controller to do the specified task and the programming is done using assembly language programming.
In our project our main aim is to do secured navigation of military guns.

Encryption is the process of transforming information (referred to as plain text) using an algorithm (called cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key. The result of the process is encrypted information (in cryptography, referred to as cipher text). In many contexts, the word encryption also implicitly refers to the reverse process, decryption (e.g. “software for encryption” can typically also perform decryption), to make the encrypted information readable again (i.e. To make it unencrypted).

Encryption/decryption is especially important in wireless communications. This is because wireless circuits are easier to “tap” than their hard-wired counterparts.

Nevertheless, encryption/decryption is a good idea when carrying out any kind of sensitive transaction, such as a credit-card purchase on line, or the discussion of a company secret between different departments in the organization. The stronger the cipher – that is, the harder it is for unauthorized people to break it – the better, in general. However, as the strength of encryption/decryption increases, so does the cost.

Encryption has long been used by militaries and governments to facilitate secret communication. Encryption is now used in protecting information within many kinds of civilian systems, such as, computer networks.

II. PROBLEM DEFINATION

The military applications are requires to increased protection of a confidential data including access control methods. In many cases, it is a desirable to provide a differentiated access services that a Data access policies are defined over a user attributes or a roles, which are managed by the key authorities.

III. RELATED WORKS:

A study in [1] is conducted for different secret key algorithms such as DES, 3DES, AES, and Blowfish. They were implemented, and their performance was compared by encrypting input files of varying contents and sizes. The algorithms were tested on two different hardware platforms, to compare their performance. They had conducted it on two different machines: P-II 266 MHz and P-4 2.4 GHz. The results showed that Blowfish had a very good performance compared to other algorithms. Also it showed that AES had a better performance than 3DES and DES. It also shows that 3DES has almost 1/3 throughput of DES, or in other words it needs 3 times than DES to process the same amount of data.

A study in [2] is conducted for different popular secret key algorithms such as RC4, AES, and XOR. They were implemented, and their performance was compared by encrypting for real time video streaming of varying contents. The results showed; encryption delay overhead using AES is less than the overhead using RC4 and XOR algorithm. Therefore, AES is a feasible solution to secure real time video transmissions.

In the present work[3]the authors introduced a new symmetric key cryptographic method for both encryption and decryption of any file such as binary file text file etc. They considered the size of key matrix as 65536 and in each cell they stored two character patterns instead of one character with the introduction of a square key matrix of size 256x256.

In this paper[4], various techniques of security of data and one the algorithm using Polyalphabetic substitution cipher are discussed. Security of data in army stations is an important issue. In early systems, at the time of information transmission between two army stations, it can be hacked by terrorists, spies and enemies. Cryptography is a very important system employed for this purpose.

There are various types of algorithms available for encryption and decryption of data and new algorithms are evolving. Polyalphabetic substitution cipher is a strong algorithm used for security of data in army stations.

The algorithm [5] is designed using combination of two symmetric cryptographic techniques. These two primitives can be achieved with the help of Advanced Encryption Standard (AES) and Data Encryption Standard (DES). This new hybrid cryptographic algorithm has been designed for better security with integrity.

The security [6] is provided based on the AES prototype cryptographic algorithm. An advanced key management scheme is used to enhance the security of the system. The paper presents [7] an approach to develop a Hybrid Cryptographic algorithm using combination of two symmetric cryptographic techniques which are AES and DES.

In this paper [8] ,Encryption algorithms and methods are among those technologies that are less apparent to casual or business users, but are central to virtually every fund transfer, business to business transfer or internal International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE) ISSN: 0976-1353 Volume 13 Issue 4 –MARCH 2015. 274 company data input and output today. This paper examines evolution and economic significance of NIST's Data Encryption Standard (DES) program. In this paper[9] a block encryption standard for transfer of data is proposed to achieve the different goals of security that is availability confidentiality and integrity. The algorithm is based on symmetric key encryption approach .

In this paper[10] the advanced encryption standard is used for error detection in an efficient manner .hardware implementation can be done in the most efficient and appropriate manner.

IV. SYSTEM DESIGN:

The operation of the whole system can be seen through the block diagram. The Fig. 1 below shows the project block Diagram.

A.Transmitter section:

In a transmitter section, the data to be transferred to a remote location is entered using hyperterminal in PC , and the data is sent to a microcontroller. The Microcontroller – after receiving the data, based on its program – transfers the data to a MAX232 wherein the TTL data is converted into a serial data. This serial encrypted data is then transmitted to the receiver section by a Zigbee module .

The Crystal circuit plays a key role in the microcontroller operation. This Crystal circuit generates clock pulses so that the internal operation gets synchronized .When the reset pin is high, the microcontroller returns to a power on state, by leaving the currently executing program. RESET operation is performed by holding the RST pin.

B.Receiver section:

At the receiver end, the Zigbee receiver module receives the data through air and the microcontroller decrypts the encrypted data. Finally the data is converted into the original data so that a user can read it and the decrypted data makes its way to the LCD display to get displayed there. Thus data can be protected at both the ends while transmitting and receiving.

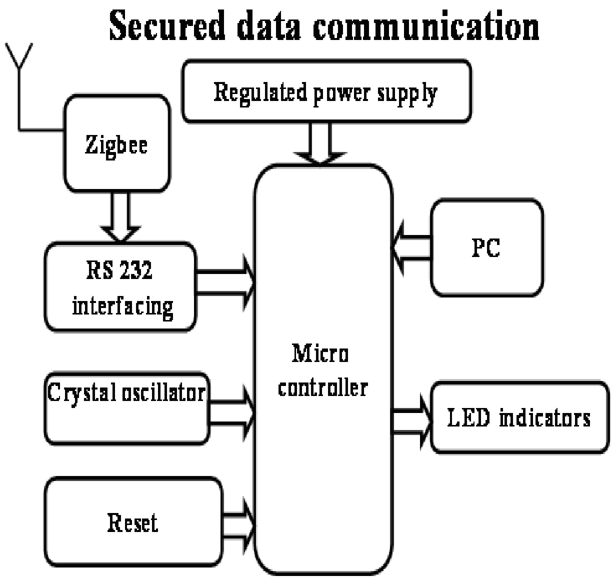

FIG (i): Block diagram of transmitter section

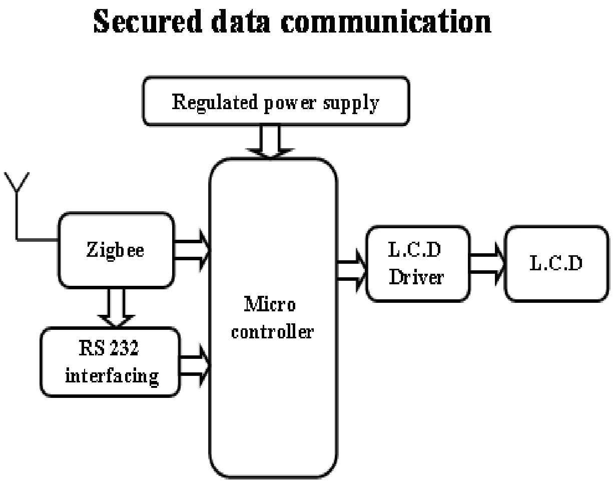

FIG :(ii): Block diagram of receiver section

Encryption: Initial1y plain text is split into blocks, having equal length after x-or operation with key which is send by the user. Then we take each distinct block and all the distinct blocks according to their sequence of appearance are kept in private key. The content after x-or operation is converted into binary form which is nothing but stream of bit which is decomposed into N number of blocks of equal length; say L bits where L is an integer. It may be happened that after decomposition of total source-stream of bit into some L-bit blocks, a blocks, less than L bits is left at last, say ML (means length of ML< L) which is kept unchanged during encryption. So here N should be less or equal to 2L (N ≤2L). For the encryption we need to generate replaced code, named Identification

Marks for each distinct block. Send each split blocks with recently generated corresponding identification marks. Let us consider the two consecutive identification marks and replace with identification marks which are generated on and onwards with the 2nd level regeneration process the replacement process will be continued up to D level .Now ML is appended at beginning with the output hence the encrypted text will be generated.

Decryption: Collecting all distinct blocks, identification marks for each block is assigned. This identification mark is same as first level of identification mark. From the beginning of the encrypted text, unchanged block (ML) is collected, length of which is defined in to the key. Then every identification marks is replaced into identification marks. In that process we find two different identification marks against each distinct block .Now we repeat finding identification marks up to D level in inverse manner. Repeat the same procedure to identification marks up to Dang will get the data back .Replace the all identification marks into its binary form with the help of key. Now we collected the entire bit-stream-blocks are merge together. After this merging, UB is attached at last of the recently generated decrypted bit of stream.

V. CONCLUSION

Cryptography is the best method for security of data. The proposed RSA shows a better result when compared with the previous works. It will take less time and it is impossible to break the encryption algorithm without knowing the exact key value. This algorithm can be applied for data encryption and decryption in any type of public applications for sending confidential data.

VI. REFERENCES

[1] "A Performance Comparison of Data Encryption Algorithms," IEEE [Information and Communication Technologies, 2005. ICICT 2005. First International Conference ,2006-02-27, PP. 84-89.

[2] W.S.Elkilani, H.m.Abdul-Kader, "Performance of Encryption Techniques for Real Time Video Streaming, IBIMA Conference, Jan 2009, PP 1846-1850.

[3] Dripto Chatterjee, Joyshree Nath, Suvadeep Dasgupta, Asoke Nath "A new Symmetric key Cryptography Algorithm using extended MSA method: DJSA symmetric key algorithm" published in 2011 International Conference on Communication Systems and Network Technologies, 978-0-7695-4437-3/11 $26.00 © 2011 IEEE

[4] Dnyanda Namdeo Hire, "Secured Wireless Data Communication", International Journal of Computer applications(09758887),Volume54no1,September 2012.

[5] Wang Tianfu, K. Ramesh Babu , VIT University, TamilNadu,India."Design of a Hybrid Cryptographic Algorithm".K Ramesh Babu, International Journal of Computer Science & Communication Networks, ISSN:2249-5789 , Vol 2(2), 277-283 277

[6] Nikolaos Doukas,Nikolaos G.Bardis, wseas transactions on information science & applications, "Design and Development of a Secure Military Communication based on AES Prototype Crypto Algorithm and Advanced Key Management Scheme",ISSN: 1790-0832, Issue 10, Volume 5, October 2008

[7] Jigar Chauhan, Neekhil Dedhia, Bhagyashri Kulkarni, University of Mumbai. "Enhancing Data Security by using Hybrid Cryptographic algorithm", International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 2, Issue 3, May 2013

[8] D. Coppersmith, "The Data Encryption Standard (DES) and Its Strength against Attacks." IBM Journal of Research and Development,May 1994, pp. 243 -250.

[9] Akhil Kaushik, Manoj Bamela, AnantKumar, ” Block Encryption Standard for Transfer of Data”, International Conference on Networking and Information Technology- 2010.

[10] H. Yen, B. F. Wu,“Simple error detection methods for hardware implementation of advanced encryption standard”,IEEE Trans. Computers, Vol. 55, No. 6, pp. 720- 731, June2006.