International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 03 | Mar 2019 www.irjet.net p-ISSN: 2395-0072

CRYPTOGRAPHIC EFFICIENT DATA TRANSMISSION IN DEFENCE STATIONS USING LORA

Nishakar Kankalla[1], Kasireddygari Anirudh Reddy[2], Nimmagadda Haripriya[3]

[1]Associate Professor, Department of ECE, St. Martin's Engg. College, Medchal, Telangana, India
[2]Bachelor of Technology, Department of ECE, St. Martin's Engg. College, Medchal, Telangana, India.
[3]Bachelor of Technology, Department of ECE, St. Martin's Engg. College, Medchal, Telangana, India.

----------****----------

Abstract: *Nowadays in many multinational companies, military departments, intelligence and surveillance departments etc., confidential data transfer is a crucial task. 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. Cryptography [4] is a one of the technique which can be used for secured transmission of data. There are numerous algorithms available for encrypting and decrypting data and many algorithms are being discovered. Poly alphabetic cipher algorithm is one of the strongest algorithms used for securing data in army stations. In this paper, poly alphabetic cipher algorithm is discussed for wireless data transmission between army stations using PIC Microcontroller. In the proposed system transfer of the cipher text is obtained from Poly alphabetic cipher Algorithm directly from base station to soldiers, thereby minimizing the time consumed. In addition to it an alert system is also being provided to the soldier.*

Keywords: *Cryptography, Cipher Algorithm, Encryption, Decryption, LED, LoRa, USB-TTL.*

1 .INTRODUCTION

The paper examines in implementing a cryptographic data transmission. We can implement this technology in defence and military areas. Here LoRa [1, 3] technology is employed because it provides higher level of security (Cryptography).

Cryptography is the science of information security. The word is derived from the Greek *kryptos*, meaning hidden. In recent times, cryptography has turned into a battleground of some of the world's best mathematicians and computer scientists. The ability to securely store and transfer sensitive information has proved a critical factor in success in war and business. LoRa technology employs higher level of encryption before sending the data.
This paper consists of an on board computer, which consists of number of input and output ports. These on board computers are commonly termed as micro controllers. The input and output port of the controller are interfaced with different input and output modules depending on the requirements. In other words micro controller acts as a communication medium for all the modules involved in the paper.

Technological advancements are happening day-by-day. Hence, there is a possibility of leaking secret information that may seriously damage any organization or a national security. Especially, at the war time the terrorists and spies tries to get the information by leaking our hi-tech security systems so that they can capture the important information useful to win the war. In the Business field too, security plays an important role.

Military cryptographic systems must meet number of practical considerations:
1) An ideal cryptographic system for military purposes is a single all-purpose system which is practical for use from the highest headquarters to the individual soldier on the battlefield. It is secure no matter how much message traffic is sent using the system. It is easy to use without special training. It presents no logistics problems in keeping the users supplied with the system's keys. It operates under all weather conditions, on all means of communication, and in the dark.
2) Cryptographic system selection for military use depends on much more than its degree of security. While protecting information from unfriendly eyes, a system must still allow communications to take place rapidly, to be reliable and to be usable by all who need to communicate. It must be usable under all conditions. For example, a system requiring an hour of pains-taking encryption would go unused by a combat military force on the move.
3) A system that has no tolerance for errors in its use would be inappropriate for soldiers under fire in severe weather conditions.
4) A system that only supports a low volume of messages would be inappropriate for a major message centre handling thousands of messages daily.
5) A system that requires expensive, sophisticated equipment would be inappropriate for a military force that can barely afford to buy ammunition. No single system meets all the requirements of security, speed, reliability, and cost.

2. BLOCK DIAGRAM

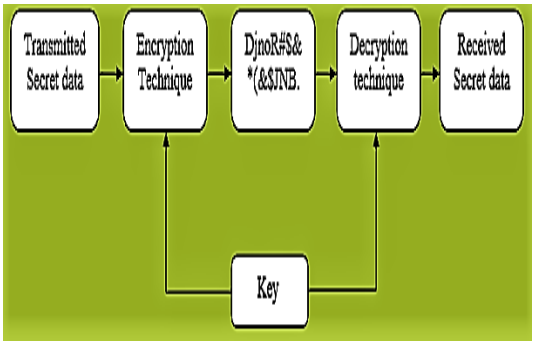

Fig.1: Cryptographic Technique

3. WORKING

Basically there are many security features in the data transmission where many multinational companies and various remote army stations utilise.
First of all the data which is to be sent is prepared from the end of variant and if any threat from the border occurs immediate reaction should be taken from first end source. The controller plays a vital role in functioning the process by loaded the program using Embedded "C" [6, 9].

Data that is transmitted should not be visible to the hackers or third party from another end. In order to satisfy those conditions cryptography is used to secure the transmitted data so that every processes can be assured in secured manner.

Every data needs to be transmitted with the help of any wired or wireless communications methods. So in this paper the source used for transmitting data is LoRa, which is the acronym of Long Range, this source is named for wireless communication which is placed at both the ends. From the transmitter end the data transmitted is disclosed using cryptographic technique known as encryption where a dummy data is displaced on the screen so that no one except the officials can understand. The dummy data (cipher text) looks like garbage value where it displays other characters other than alphabets.

Similarly on the other station the data received can be displayed using symmetric key where only two parties knows for decrypting the data using that key. This technique is also another cryptographic[1] technique. The received data can be displayed on high standard where it can vast at a distance of 10-12 km range from one station to another station.

4. HARDWARE DESCRIPTION

4.1 Transmitter Station: The below schematic diagram of Transmitter explains the interfacing section of each component to the micro controller in the transmitting section. Here a USB-TTL convertor is connected to the pc where the power is gained to the whole section. Initially the USB-TTL convertor provides 230 V AC to the transmitter section, in order to convert the power as per the requirement an RPS section is built such that the required amount of power is enabled.

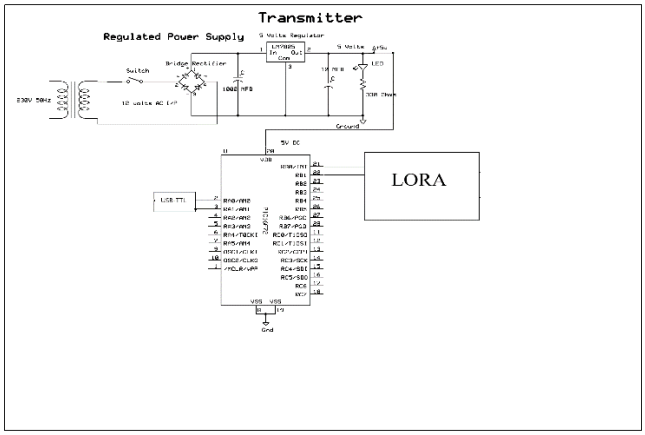

Fig.2: Transmitter section

In the RPS section firstly a step down transformer is placed such that it converts high voltages into low voltages. Here the provided 230 V AC is converted into 12 V AC. The device which converts an AC current to pulsating DC is called as a rectifier. In order to convert the AC power to DC power a bridge rectifier is place after the step down transformer, this converts 12 V AC to 12 V DC. A switch is placed between the transformer and the rectifier, this acts as reset button. The output from the rectifier results with some noise, in order to rectify that a capacitor is placed so that it acts as a filter and reduce the noise gained after the process of rectification. Decoupling capacitors are placed after the filter because sometimes there may be power fluctuations this harms the micro controller. So these decoupling capacitors are places in series such that these acts as an avoider to the micro controller from damage. Now a regulator is placed and the filter is connected to this. This regulator converts 12V DC to 5V DC as per the requirement.

The power supply is connected to the 20 pin of the PIC micro controller. To the pins 2, 3 USB-TTL converter is connected. A crystal oscillator is placed between the pins 9 and 10, which generates clock pulses as per the requirement and also this plays a major role in transmitting the data i.e., speed is increased. LED's [2] are provided to check the condition of the components whether working or not. Pins 20 and 21 are connected to the LORA module through which the provided data is transmitted.

The data which is to be transmitted is entered in the pc using HyperTerminal software which is encrypted and is transmitted through the LoRa module.

4.2 Receiver Station: The below schematic diagram of Receiver explains the interfacing section of each component with microcontroller [5] in the receiving section. Here a USB-TTL convertor is connected to the pc where the power is gained to the whole section. Initially the USB-TTL convertor provides 230 V AC to the receiver section, in order to convert the power as per the requirement an RPS section is built such that the required amount of power is enabled.

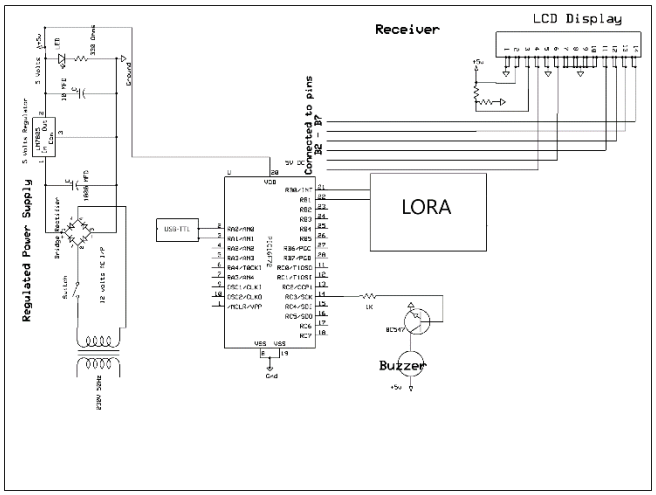

Fig.3: Receiver section

In the RPS section firstly a step down transformer is placed such that it converts high voltages into low voltages. Here the provided 230 V AC is converted into 12 V AC. The device which converts an AC current to pulsating DC is called as a rectifier. In order to convert the AC power to DC power a bridge rectifier is place after the step down transformer, this converts 12 V AC to 12 V DC. A switch is placed between the transformer and the rectifier, this acts as reset button. The output from the rectifier results with some noise, in order to rectify that a capacitor is placed so that it acts as a filter and reduce the noise gained after the process of rectification. Decoupling capacitors are placed after the filter because sometimes there may be power fluctuations this harms the micro controller. So these decoupling capacitors are places in series such that these acts as an avoider to the micro controller from damage. Now a regulator is placed and the filter is connected to this. This regulator converts 12 V DC to 5 V DC as per the requirement.

The power supply is connected to the 20 pin of the PIC micro controller. To the pins 2, 3 USB-TTL converter is connected. A crystal oscillator is placed between the pins 9 and 10, which generates clock pulses as per the requirement and also this plays a major role in receiving the data i.e., speed is increased. LED's are provided to check the condition of the components whether working or not. Pins 20 and 21 are connected to the LoRa module through which the provided data is received. From the pins 22 to 28 it is connected to the LCD display where the external display about the data reception and the password access or the denied is displayed. Also a buzzer is placed and is provided with the buzzer driver and is connected to the pin 14, a buzzer is provided such that if an unauthorized uses the password in the receiving section and if the password is wrong the buzzer beeps continuously where it acts as an alarm system. The data which is received in the receiving section from the LoRa module will be displayed in the HyperTerminal software in the pc only when the provided data is correct. Before giving the password the LCD display shows the notification that the data is received and the dummy data is displayed. When the correct password is provided the data is decrypted and the original data is displayed.

5. CRYPTOGRAPHY

Cryptography is associated with the process of converting ordinary plain text into unintelligible text and vice-versa. It is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. Cryptography not only protects data from theft or alteration, but can also be used for user authentication. Earlier cryptography was effectively synonymous with encryption but nowadays cryptography[1] is mainly based on mathematical theory and computer science practice. Cryptographic technique which is used to encrypt the data using encryption algorithm. Symmetric, i.e. same key is used here for encryption & decryption purpose. Cryptography technique is mainly classified into two categories as follows: Symmetric key algorithm: In symmetric key algorithm, same key is used for encryption and decryption of the same data on both sides. Asymmetric key algorithm: Asymmetric key algorithm uses different keys for encrypting and decrypting the same data on both transmitter's & receiver's side.

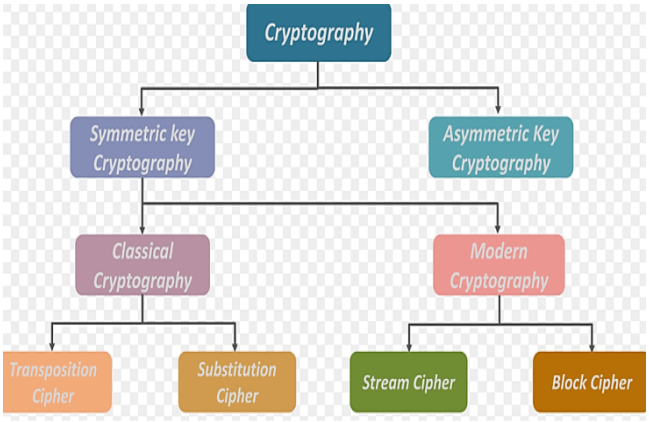

Fig.4: Various types of Cryptographic techniques

Among these two algorithms the polyalphabetic substitution cipher algorithm is more advantageous and used in various applications.

Mono alphabetic substitution cipher: In this type of substitution, a character in the plaintext is always substituted by some other character in the cipher text regardless of its position in the text. Here each plaintext character is shifted down by 3.

Polyalphabetic substitution cipher: This algorithm is widely used due to its following advantages:

1) Provides more security than mono alphabetic cipher.
2) Easy to implement.
3) Replacement of same characters repeated in algorithm can be done using different characters.

5.1 Encryption:

It is the process of encoding a message or information in such a way that only authorized parties can access it and those who are not authorized cannot. Encryption does not itself prevent

Interference, but denies the intelligible content to a would-be interceptor. Initial1y plain text is split into blocks, having equal length after x-or operation with key which is send by the user.

5.2 Decryption:

Decryption is the process of taking encoded or encrypted text or other data and converting it back into text that you or the computer can read and understand. This term could be used to describe a method of unencrypting the data manually or unencrypting the data using the proper codes or keys.

6. POLY ALPHABETIC CIPHER ALGORITHM

In this technique, we have simply used the number system to encrypt the data. The flowchart shown explains the detailed process of encrypting and decrypting the information to be transmitted.

6.1 Algorithm for Encryption:

1. START.

2. Represent the message to be transmitted in numeric form (i.e. a:'0', b:'1', z:'25').

3. Add corresponding key to the cipher text.

4. Subtract 26 from the addition.

5. Write corresponding letter of above numbers & amp; Repeat the procedure till the end of text.

6.2 Algorithm for decryption:

1. START.

2. Represent the message received in numeric form (i.e. a:'0', b:'1'... z:'25').

3. Add 26 to this numeric form.

4. Subtract corresponding key from the above addition.

5. Write corresponding letter of above numbers & Repeat the procedure till the end of text.

7. DIFFERENT MODULES

7.1 PIC [8]

The 16f72 micro controller is powerful (200 nanosecond instruction execution) yet easy-to-program (only 35 single word instructions) CMOS FLASH-based 8-bit microcontroller. The PIC 16F72 is a 28 pin IC in the physical structure with 3 ports like port A (6 pins), port B (8 pins), port C (8 pins) excluding the supply pins (4 pins). Microcontrollers are also used in scientific, high technology, and aerospace projects.

PIC is a family of Harvard architecture microcontrollers made by Microchip Technology, derived from the PIC1640 originally developed by General Instrument's Microelectronics Division. The name PIC initially referred to & quote; Peripheral Interface Controller & quote; A PIC' instructions vary from about 35 instructions for the low-end PICs to over 80 instructions for the high-end PICs. The instruction set includes instructions to perform a variety of operations on registers directly, the accumulator and a literal constant or the accumulator and a register, as well as for conditional execution, and program branching. Microcontrollers are designed for small or dedicated applications.

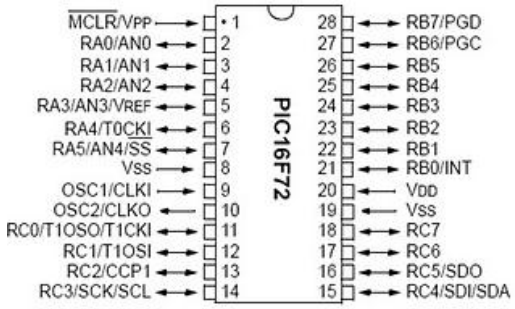

Fig.5: Pin diagram of PIC Microcontroller

7.2 LoRa [3, 4]

LoRa stands for Long Range. LoRa is the physical layer or the wireless modulation utilized to create the long range communication link. LoRa is based on chirp spread spectrum modulation, which maintains the same low power characteristics as FSK modulation but significantly increases the communication range. Chirp spread spectrum has been used in military and space communication for decades due to the long communication distances that can be achieved and robustness to interference, but LoRa is the first low cost implementation for commercial usage. Frequency range is of different types such as 433 MHZ, 868 MHZ, 915 MHZ. In this paper basic frequency type that is 433 MHZ is used which can transmit the data up to 10-12 Km range.

Long Range (LoRa) the advantage of LoRa is in the technology's long range capability. A single gateway or base station can cover entire cities or hundreds of square kilometres. Range highly depends on the environment or obstructions in a given location, but LoRa and LoRa WAN have a link budget greater than any other standardized communication technology. LoRa WAN defines the communication protocol and system architecture for the network while the LoRa physical layer enables the long-range communication link.

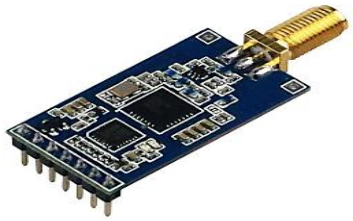

Fig.6: LORA Module

7.3 USB-TTL

The CP2102 is a highly-integrated USB-to-UART Bridge Controller providing a simple solution for updating RS-232 designs to USB using a minimum of components and PCB space[7]. The CP2102 includes a USB 2.0 full-speed function controller, USB transceiver, oscillator, EEPROM, and asynchronous serial data bus (UART) with full modem control signals in a compact 5 x 5 mm MLP-28 package. No other external USB components are required.

Fig.7: USB-TTL Module

7.4 CRYSTAL OSCILLATOR[2]

Crystal oscillator[2] is basically a tuned oscillator that works on the basis of piezoelectric effect i.e. when voltage is applied to crystal it vibrates at frequency of applied voltage or when mechanical pressure is applied it generates an Ac voltage. Generally quartz is used for crystal oscillator which is more stiff compare to Rochelle salt. Quartz is inexpensive and readily available in nature. Crystal can be represented by electrical model if it is suitably cut and mounted between two metal plates.

A **crystal oscillator** is an electronic circuit that produces a repetitive Electronic signal, often a sine wave or a square wave. PIC micro controller internally having 4 MHz clock frequency. We are giving the 20 MHz clock frequency as an external source for increasing the system performance.

Fig.8: Crystal Oscillator

8. SOFTWARE DESCRIPTION

HyperTerminal is an application that connects a computer to other remote systems. These systems include other computers, bulletin board systems, servers, Telnet sites, and online services. However, a modem, an Ethernet

connection, or a null modem cable is needed before HyperTerminal can be used. IT professionals and users can work with HyperTerminal to set up a dial-up connection to another computer through the internal modem using Telnet or to access a bulletin board system in another computer.

They can use HyperTerminal to set up a connection for data transfers between two computers, such as a desktop computer and a portable computer, using the serial ports. HyperTerminal can also allow IT to take serial-port control of external devices or systems such as scientific instruments, robots or radio communications stations. They also use HyperTerminal to troubleshoot any issues when setting up and using a modem. IT can send commands through HyperTerminal to make sure the modem is properly connected.

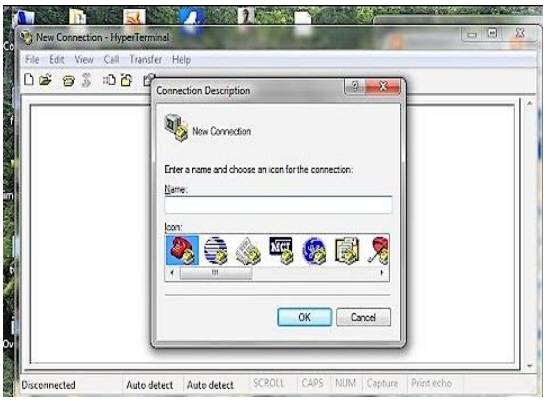

Fig.9: HyperTerminal Display

9. ADVANTAGES

Confidentiality– Encryption technique can guard the information and communication from unauthorized revelation and access of information.
Authentication – The cryptographic techniques such as MAC and digital signatures can protect information against spoofing and forgeries.
Data Integrity- The cryptographic hash functions are playing vital role in assuring the users about the data integrity.
Non-repudiation- The digital signature provides the non-repudiation service to guard against the dispute that may arise due to denial of passing message by the sender.
Highly efficient and user friendly design
Easy to operate.
Low power consumption
Efficient design

10. CONCLUSION

Integrating features of all the hardware components used have been developed in it. Presence of every module has been reasoned out and placed carefully, thus contributing to the best working of the unit. Secondly, using highly advanced IC's with the help of growing technology, the paper has been successfully implemented. Thus the project has been successfully designed and tested. Cryptography is indeed, the best method for data security. Among the various types of cryptographic[1] techniques, Polyalphabetic Substitution cipher is the best method. This paper will help to maintain the privacy and to prevent any unauthorized person from extracting the information from the communication channel. So using this small concept, we will try to implement the algorithm for secured wireless communication over a long distance. This algorithm will help in obtaining the higher degree of security from terrorists, spies or any other harmful person. So this system can be practically used to obtain important information from source to destination using wireless communication.

11. REFERENCES

[1] Ramon Sanchez-Iborra; Jesus Sanchez-Gomez; Juan Ballesta-Viñas; Maria-Dolores Cano; Antonio F. Skarmeta (2018). "Performance Evaluation of LoRa Considering Scenario Conditions".

[2] Marrison, Warren (1948). "The Evolution of the Quartz Crystal Clock"

[3] Bankov, D.; Khorov, E.; Lyakhov, A. (November 2016). "On the Limits of LoRaWAN Channel Access"

[4] Behrouz A. Forouzan, ed. SIE Cryptography and Network Security

[5] Raj Kamal: Microcontrollers Architecture, Programming, Interfacing and System Design.

[6] Mazidi and Mazidi –Embedded Systems.

[7] PCB Design Tutorial –David.L.Jones.

[8] PIC Microcontroller Manual – Microchip.

[9] Embedded C –Michael.J.Pont

AUTHORS

Mr.Nishakar Kankalla, completed his B.Tech and M.Tech from Jawaharlal Technological University (JNTUH), Hyderabad, Telangana. Currently pursuing Ph.D. from Utkal University, Bhubaneswar, Odisha. are Image Processing, Embedded Systems and Wireless Communications. He has total 10 years of teaching experience in reputed institutions. He has published total 7 papers in National and Internationals conferences and journals. Currently working as Associate Professor in Department Electronics and Communication Engineering, St. Martin's Engineering College, Hyderabad.

Mr Kasireddygari Anirudh Reddy is pursuing IV Year Batchelor of Technology in Department of Electronics and Communication Engineering, St. Martin's Engineering College, Dulapally, Medchal, India. His area of interest in Advance digital signal processing & Linear Electromagnetics (Electronics) and also in Radar systems and Satellite communications.

Ms Haripriya Nimmagadda is pursuing IV Year Batchelor of Technology in Department of Electronics and Communication Engineering, St. Martin's Engineering College, Dulapally, Medchal, India. Her area of interest in Practical Electronics, Digital control system Engineering and also in Telecommunications and Wireless communication networks.