ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 6, Issue 7, July 2019

Cryptographic Based Secured Communication between Army Stations

[1] T.Sivasakthi, [2]S. Priyanka, [3]V. Swathi Priya, [4]P. Mathuvanthi
[1] Assistant Professor
[1][2][3][4] Department of Electronics and Communication, Sri Sairam Engineering College, Chennai, India

***Abstract* – Small embedded devices such as microcontrollers have been widely used for identification, authentication, securing and storing confidential information. In all these applications, the security and privacy of the microcontrollers are of crucial importance. To provide strong security to protect data, these devices depend on cryptographic algorithms to ensure confidentiality and integrity of data. Moreover, many algorithms have been proposed,**
with each one having its strength and weaknesses. This paper presents the implementation of Advanced Encryption Standard(AES) running inside a PIC16F877A microcontroller.

Index Terms: AES, Encryption, Authentication, Decryption, Cryptographic

I. INTRODUCTION

The objective of the project is to design and provide an effective communication between two army stations so that the transfer of crucial information is secured using zigbee wireless communication technologies .The algorithm used is the Advanced Encryption Standard (AES), the most popular and widely adopted symmetric encryption algorithm to encrypt and decrypt the information. AES algorithm is effective since it is accessed by the receiver only when they are aware of the data transmission.

II. CRYPTOGRAPHY BASICS

Cryptography or cryptology (is the practice and study of techniques for secure communication in the presence of third parties called adversaries More generally, cryptography is about constructing and analyzing protocols that prevent third parties or the public from reading private messages; various aspects in information security such as data confidentiality, data integrity, authentication, non-repudiation are central to modern cryptography. Modern cryptography exists at the intersection of the disciplines of mathematics, computer science, electrical engineering, communication science, and physics. Applications of cryptography include electronic commerce, chip-based payment cards, digital currencies, computer passwords, and military communications .

The basic principles include :

1. Encryption
In a simplest form, encryption is to convert the data in some unreadable form. This helps in protecting the privacy while sending the data from sender to receiver. On the receiver side, the data can be decrypted and can be brought back to its original form. The reverse of encryption is called as decryption. The concept of encryption and decryption requires some extra information for encrypting and decrypting the data. This information is known as key. There may be cases when same key can be used for both encryption and decryption while in certain cases, encryption and decryption may require different keys.

2. Authentication
This is another important principle of cryptography. In a layman's term, authentication ensures that the message was originated from the originator claimed in the message. Now, one may think how to make it possible? Suppose, Alice sends a message to Bob and now Bob wants proof that the message has been indeed sent by Alice. This can be made possible if Alice performs some action on message that Bob knows only Alice can do. Well, this forms the basic fundamental of Authentication.

3. Integrity
Now, one problem that a communication system can face is the loss of integrity of messages being sent from sender to receiver. This means that Cryptography should ensure that the messages that are received by the receiver are not

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 6, Issue 7, July 2019

altered anywhere on the communication path. This can be achieved by using the concept of cryptographic hash.

4. Non Repudiation

What happens if Alice sends a message to Bob but denies that she has actually sent the message? Cases like these may happen and cryptography should prevent the originator or sender to act this way. One popular way to achieve this is through the use of digital signatures.

III. LITERATURE REVIEW

Bogdan Groza in 2008 presented an idea by Implementing cryptography on devices with low computational power. It is a necessity as they became involved in communications over public networks. Even more, these devices became ubiquitous and are used in a large area of applications, from home-office systems to industrial control systems. We deal with the design and implementation of a cryptographic protocol that can be used to assure the authenticity of the information broadcasted over UDP from an 8051 based system-on-a-chip to a large number of receivers. The protocol that we use is similar to the well known TESLA protocol that was used in sensor networks, and by using such a protocol information can be broadcasted to a large number of receivers without requiring secret shared keys or expensive public key operations. Some implementation details and experimental results are presented as well, and they show that implementing a cryptographic authentication protocol is feasible even in a constrained environment as offered by the 8051 microcontroller[1].

Xueying Zhang presented an energy cost analysis for session key establishment in a wireless sensor network (WSN). A session key is used to encrypt the data between two nodes and it should be established before the start of their secure data communication. In a WSN, the session key establishment is an important process in constructing a secure data communication and is preferably undertaken to minimize the energy drain on the energy-constrained sensor node. In our study, we examine the energy cost of session key establishment using a symmetric-key based protocol in a WSN. We make use of an energy consumption model for the sensor node that considers the communication cost and computational cost for implementing the protocol on a microcontroller-based sensor node. In particular, we explore the effects of session key establishment to the overall energy cost in a sensor node, especially considering the frequency of key establishment and the quality of communication channel[2].

Jeremy H.-F. Constantin and Andreas P. Bur investigated the benefits of instruction set extensions (ISEs) on a 16-bit microcontroller architecture for software implementations of cryptographic hash functions, using the example of the five SHA-3 final round candidates. We identify the general algorithm bottlenecks, taking into account memory footprints and cycle counts of our optimized reference assembly implementations. We show that our target applications benefit from algorithm-specific ISEs based on finite state machines for address generation, lookup table integration, and extension of computational units through microcoded instructions. The gains in throughput, memory consumption, and the area overhead are assessed, by implementing the modified cores and applications utilizing the developed ISEs. Our results show that with less than 10% additional core area, it is possible to increase the execution speed on average by 172% (ranging from 21% to 703%), while reducing memory requirements on average by more than 40%[3].

Markus Vogt proposed that the RFID technology in combination with cryptographic algorithms and protocols is discussed widely as a promising solution against product counterfeiting. Usually the discussion is focussed on passive low-cost RFID-tags, which have harsh power constraints. 4-Bit microcontrollers have very low-power characteristics (5-60 µA) and are therefore an interesting platform for active and passive low-cost RFID-tags. To the best of our knowledge there are no implementations of cryptographic algorithms on a 4-bit microcontroller published so far. Therefore, the main contribution of this work is to demonstrate that cryptography is feasible on these ultra-constrained devices and to close this gap. Our implementation draws a current of 6.7µA at a supply voltage of 1.8V and a frequency of 500 KHz and requires less than 200 ms for the processing of one data block[4].

Often overlooked, microcontrollers are the central component in embedded systems which drive the evolution toward the Internet of Things (IoT). They are small, easy to handle, low cost, and with myriads of pervasive applications. An increasing number of microcontroller-equipped systems are security and safety critical. In this tutorial, we take a critical look at the security aspects of today's microcontrollers. We demonstrate why the implementation of sensitive applications on a standard microcontroller can lead to severe security problems. To this end, we summarize various threats to microcontroller-based systems, including side-channel analysis and different methods for extracting embedded code. In two case studies, we demonstrate the relevance of these techniques in real-world applications: Both analyzed systems, a widely used

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 6, Issue 7, July 2019

digital locking system and the onetime password generator, turned out to be susceptible to attacks against the actual implementations, allowing an adversary to extract the cryptographic keys which, in turn, leads to a total collapse of the system security[5].

IV. METHODOLOGY

A. Introduction

Encryption is the process of encoding messages (or information) in such a way that third parties cannot read it, but only authorized parties can. Encryption doesn't prevent hacking but it prevents the hacker from reading the data that is encrypted. In an encryption scheme, the message or information (referred to as plaintext) is encrypted using an AES algorithm, turning it into an unreadable cipher text.

Here we use PIC microcontroller to transfer and receive data. If the sent data from the transmitter is word and the transferred data is encrypted into a numeric value assigned to each of the letters to that word. On the other side the receiver gets the numeric values of that particular data into the PIC and it is decrypted to the data which was sent by the transmitter.

This is usually done with the use of an encryption key as a numeric value, which specifies how the message is to be encoded. Any adversary that can see the cipher text should not be able to determine anything about the original message. As a result the Cryptography is the best method for security of data. The AES algorithm 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.

B. Block diagram

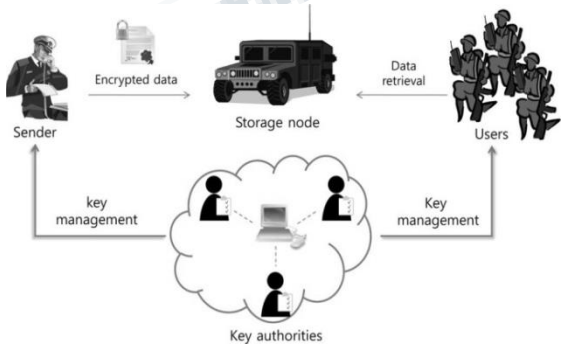

Fig. 1 Encryption and Decryption Process

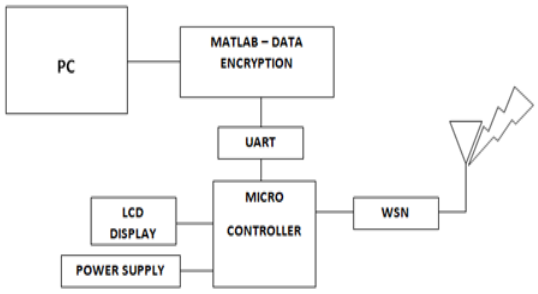

Fig. 2 Transmitter section

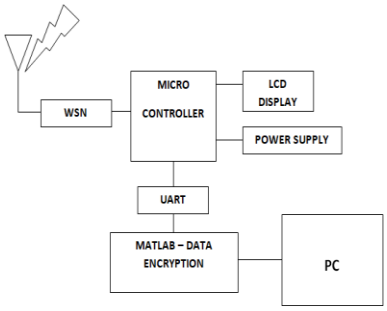

Fig.3 Receiver Section

C. Existing system and problem

Cryptography is art of writing how to secure information from unauthorized person. Basic knowledge of information processing during communication between two entities. More generally, it is regard to a group of rules for construction and analyzing correct behavior in the presence of adversary. These are threatening to different form of information security like data confidentiality, integrity and authentication. Present and recent cryptography consists of applied mathematics computer and science. The use of cryptography includes Teller Machine , user name and passwords for e-commerce and system.

The Cryptosystem consists of keys, algorithms of encryption and decryption are part of cryptosystems to each key. Keys are play major role, as a convert plain text to ciphers with specific order knowledge of the generation of cipher therefore to protect message from third party. Network security issues are removed using cryptography which is based on a science and mathematical character. There are two cryptography algorithms based on keys: symmetric key and asymmetric key cryptography algorithms.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 6, Issue 7, July 2019

In symmetric key cryptography method the same key is used to sending and receiving entities. The sender and receiver are being used for an encrypt/decrypt information with same key.
In asymmetric key , two keys are private and public. The private key is retained in sender side and public key is announced to the public. In public key encryption/decryption, the private used for encrypt while public for decrypt methods
In symmetric key cryptography ciphers are generated by substitution and transposition methods, but these ciphers can be obtained by recursive methods applied by introducer.
These algorithms faces problems of man in the middle attack and protection of keys generated at the sender and receiver sides. Authentication is one of the major characteristics in networks to protect data from the adversaries.

D. Proposed methodology

In this digital age of communication, private and confidential data is exchanged over internet and stored in digital mediums. This data is constantly under increasing threat. Encryption is one of the techniques to protect sensitive data. Small embedded devices such as microcontrollers have been widely used for identification, authentication, securing and storing confidential information. In all these applications, the security and privacy of the microcontrollers are of crucial importance. This project presents attack on hardware implementations of Advanced Encryption Standard (AES) running inside a PIC16F877A microcontroller. AES is considered to be one of most capable encryption algorithm in cryptography and can be implemented in hardware or software. Hardware implementation would be faster and secure as compared to software implementation.

E . Algorithm

AES is based on a design principle known as a substitution–permutation network, and is efficient in both software and hardware.Unlike its predecessor DES, AES does not use a Feistel network. AES is a variant of Rijndael which has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits. By contrast, Rijndael per se is specified with block and key sizes that may be any multiple of 32 bits, with a minimum of 128 and a maximum of 256 bits. The algorithm described by AES is a symmetric-key algorithm, meaning the same key is used for both encrypting and decrypting the data. The more popular and widely adopted symmetric encryption algorithm likely to be encountered nowadays is the Advanced Encryption Standard (AES). It is found at least six time faster than triple DES.
A replacement for DES was needed as its key size was too small. With increasing computing power, it was considered vulnerable against exhaustive key search attack. Triple DES was designed to overcome this drawback but it was found slow.
In present day cryptography, AES is widely adopted and supported in both hardware and software. Till date, no practical cryptanalytic attacks against AES has been discovered. Additionally, AES has built-in flexibility of key length, which allows a degree of 'future-proofing' against progress in the ability to perform exhaustive key searches.
However, just as for DES, the AES security is assured only if it is correctly implemented and good key management is employed.

Encryption Algorithm
Step 1 : convert input data into binary
Step 2: binary data into A,T,G AND C letters
Step 3 : Key value from server
Step 4 : apply complementary rules step 2 and 3
Step 5: Apply XOR operation between output from step 4
Step 6: Convert into Binary format (cipher data)
Decryption Algorithm
Step 1: Convert cipher data (binary format) into ASCII Binary sequence
Step 2: Convert binary into TEXT
Step 3: Key value from server
Step 4: apply complementary rule for step 3 and 4
Step5: XOR operation between step3 and step4 after step5
Step 6: original binary format after step 5
In the binary format, 0 complement is 1and 1 complement is 0 . hence 00 and 11 are complement to each. 01 and 10 are also complement. Here A is 00 T is 11
G is 01 C is 10 and ASCII value of G is71 C is 67 A is 65 T is 84.
Encryption Algorithm example
Binary data: 10111010 A=00 T =11
G=01 C=10
Step2: 10 11 10 10
C T C C
Step 3: T T G A (key value)
Step 4: G A G G
A A C T
Step 5: 01000101
00001011
01001110
Step 6: G A T C

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 6, Issue 7, July 2019

Step 7 : ASCII values Binary format

A	65	1000001
T	84	1010100
G	71	1000111
C	67	1000011

71 65 84 67

Step 8: Convert into Binary from output step 7

1000111 1000001 1010100 1000011 This is cipher text of binary 10111010

Decryption: Apply decryption steps to get original data

VI. CONCLUSION

The proposed method uses AES encryption standard to provide maximum security. As we are using AES algorithm, in which the data transfer process is possible only if the authorized user at receiver wants to access the information and information is securedly transferred from the transmitter to the receiver. Hence the possibility of hacking is minimal compared to other algorithms. We show that our proposed system can provide significant secret code generation thereby enabling reduced energy consumption, in addition to substantial memory reduction.

VII. FUTURE SCOPE

The experiment shows that our method is secure, imperceptible and can be used for effective transfer of information. In the future, more powerful encryption standards can be used along with Cryptography to improve security. In this proposed system, information transfer between army stations is done only if the authorized person enters the password at receiver. In future, fingerprint of the authorized person can be used in addition to password, so that transferring of information is more secure

VIII. REFERENCES

[1] Bogdan Groza , Pal-Stefan Murvay , Ioan Silea , Tiberiu Ionica, Member, IEEE, " Cryptographic authentication on the communication from an 8051 based development board over UDP", june 2008.

[2] Xueying Zhang, H.M. Heys, and Cheng Li, Member, IEEE, "Energy Cost of Cryptographic Session Key Establishment in a Wireless Sensor Network", August 2011.

[3] Jeremy H.-F. Constantin and Andreas P. Bur, Member, IEEE, "Instruction Set Extensions for Cryptographic Hash Functions on a Microcontroller Architecture", July 2012.

[4] Markus Vogt, Axel Poschmann, Christof Paar, "Cryptography is Feasible on 4-Bit Microcontrollers - A Proof of Concept", April 2009.

[5] Daehyun Strobel, David Oswald, Bastian Richter, Falk Schellenberg, and Christof Paar, Member, IEEE, "Microcontrollers as (In)Security Devices for Pervasive Computing Applications", August 2014.