Dogo Rangsang Research Journal
ISSN : 2347-7180

UGC Care Group I Journal
Vol-12, Issue-12, No. 01, December 2022

Software and hardware security using advanced encryption and decryption methods in IOT network

[1]D. PAVAN KUMAR,
Research scholar,
Department of ECE,
Jogaiah Institutes of Technology and Sciences

[2]Mr. G.Ramesh Babu,
Research Supervisor & Asst.Professor,
Department of ECE,
Jogaiah Institutes of Technology and Sciences

Abstract

RSA Cryptography is a well-known example of public key cryptographic algorithms that involves robust encryption/decryption processes. In this paper, a microcontroller based RSA is designed and proposed. Arduino Mega2560R3 microcontroller supported with external memory and a screen touch LCD as well as a double keypad has been used under the programming of C language to implement the proposed RSA coprocessor with 32 bits. It was found that the trade of between message size and the encryption time can be drawn as a liner relationship according to the block size of the encryption phase. However, such design with a MCU provided with a small solar cell (and off course with a backup battery) as well as small block sizes is considered useful for the use in wireless sensor network (WSN) applications due to the ease of connecting the MCU to the WSN which as well avoid the processing time of encryption/decryption processes that could be executed by the MCU instead of the life limited sensors.

Keywords: Information Security; Cryptography; RSA Design; Arduino Microcontroller.

1. Introduction

The rapid advances in communication networks impose the fact of transferring information worldwide every second. Considerable part of this information might need protection against fraud, modification and different types of intrusion. The secure communication scheme is shown in figure 1 [2].

Cryptographic engineering has contributed to such cases with several algorithms to provide different levels of security for the substantial information ranges from the classical cryptosystems [7] to elliptic curves cryptography [2]. Such science is categorized in two groups; namely: Symmetric Key Cryptography and Public Key Cryptography. Oppositely, the cryptanalysis is the study of deciphering the encrypted data without taking the permission of the encrypter. This refers to predicting the weakness of the design and implementation of the cryptosystem [1]. Since, a cryptosystem is any computer system that involved in cryptography, it can be classified as a combination of three major elements. These are encryption engine, keying information and operational procedure. All in all, modern cryptography intersects the disciplines of mathematics, computer science, and electrical engineering.

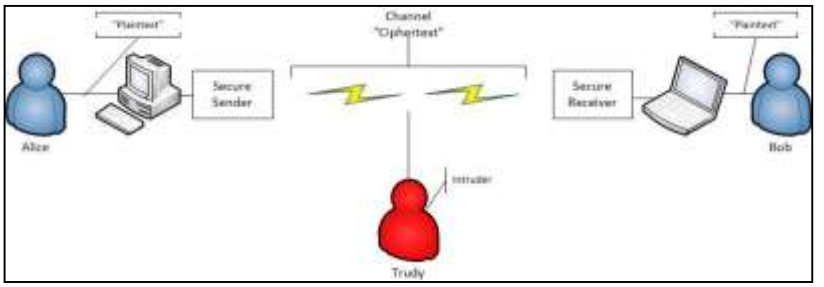

Figure 1: Scheme of Secure Communications

This paper proposes an efficient hardware design and architecture for RSA Cryptosystem using ARDUINO Microcontroller [4]. As a public key cryptography, Rivest-Shamir-Adelman (RSA) Cryptosystem is well known to be the first practicable secure algorithm that can be used to protect information during the transmission [1]. Such cryptosystem will have two different keys to accomplish a secure communication between two parties where one of them called encryption key and made public while the other called decryption key and made private. The implementation of RSA Cryptosystem is heavily based on modular arithmetic and exponentiation involving large prime numbers [2].

1.1. Problem statement

The data transmission over the public networks differs in its needs of security; some situations as in banks, hostile environments, companies, hospitals, and at the personal level too-require the channel to be very secure, so that the secure transmission is on demands. The process of designing systems that are concerned with the study of communications over non-secure channels is called cryptography.

RSA Cryptography is a well known example of public key cryptographic algorithms with robust encryption/decryption processes. The objective of this paper is to design and implement RSA Cryptoprocessor.

1.2. Work Motivation

Because most of banks, governments, organizations, and companies are extremely claim for securing their database. Also, this field of research is so unique and has critical engineering point of view. As an example, the database of Saudi Aramco has been attacked. The attacker used a computer virus known as Shamoon, which infected workstations in Aug. 15, 2012. The company shut its main internal network for more than a week [3]. Also, as a code of ethics for electrical engineers, we were interested to choose this design because it has some beneficial services for the community as well as the world. In addition, it is one of the motivating challenges between cryptographers and intruders.

1.3. Work Flow

Cryptography is simply a mathematical tool used to secure information between two parties: the sender and receiver using certain algorithm. This is done by converting a plaintext into Ciphertext using such encryption methods. Then the Ciphertext will be conveyed in distrusted channel, so that the intruder cannot either understand the content or alter it. Hence, the receiver can decrypt the Ciphertext using the assigned key. The workflow of this work will follow this scenario as in figure 2.

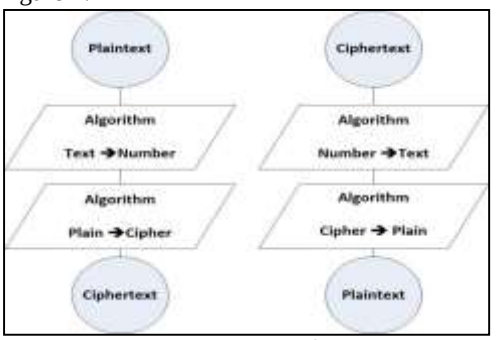

Figure 2: The Flowchart of The proposed work

1.4. RSA Algorithm by Example

We will explain and review RSA algorithm through the following numerical example given in table 1.

Table 1. Numerical example of RSA

Sender	Trudy	Receiver
Select P & G; P:prime, G:primitive root of P, P>G		
P=11, G=7		
Send P & G to the receiver	P=11, G=7	P=11, G=7
Sender select a random value A=6, which is private		Sender select a random value B=9, which is private
Apply $X = 7^6 \bmod 11$ $X = 4$		Apply $Y = 7^9 \bmod 11$ $Y = 8$
Send X to the receiver	X=4, Y=8	Send Y to the Sender
Receive Y = 8		Receive X = 4
Finding the secret key: $K_A = 8^6 \bmod 11 = 3$		Finding the secret key: $K_B = 4^9 \bmod 11 = 3$

2. Simulation Environment

This work aims to implement and verify the 32-bit RSA cryptosystem using programmable microcontroller unit (MCU). MCU [5, 6] is a single chip contains CPU, ROM, RAM, I/O control unit, Registers, and program counter. The microcontroller can be either programmable or nonprogrammable chip where the nonprogrammable chips are used for specific application and can be configured only one time by the manufacturer. On the other hand, programmable microcontrollers can be programmed for several applications. The microcontrollers can be programmed by assembly language, but nowadays the high level programming languages are commonly used such as C, C++, Verilog or VHDL. The role of the compiler is to translate the high level language to the assembly language. Then the assembler converts the assembly language to the machine language.

Figure 3: Arduino Mega2560R3 microcontroller

The microcontroller [6] is used in many control systems for several advantages such as the flexibility, ease of use, cost and size. The microcontroller can be reprogrammed at any time which makes it more flexible. Also, the microcontrollers are small in size and cost efficient compared to other controller technology. Microcontrollers are usually manufactured in two categories: single chip platform or printed board platform. For example PIC 16F688 is a chip platform, and Arduino Uno is printed board platform. Arduino is a microcontroller family which has three main types: Mega 2560, Uno, and Nano. More information about the Arduino microcontrollers can be found in [3]. In this paper, we have used Arduino Mega2560R3 microcontroller as shown in figure 4.

Figure 4: Arduino IDE

Actually, Arduino is an open source microcontroller board [6] which can be programmed using free development software. The Arduino uses a simplified version of C/C++ programming language. With Arduino board, we can write a program to control physical systems by read and write analog/digital signal. Therefore, some analog sensors are needed to be connected to the Arduino to read analog signals, and the ADC (Analog to Digital Converter) is the responsible to convert these signals to digital signals.

To program and configure the Arduino, we have used the Integrated Development Environment (IDE) software which we show it's GUI in figure 5. However, this software can be downloaded from the official website of Arduino free. The Arduino is easy-to-use since the only thing you need to do after install the IDE software is to connect the

Arduino to the computer using A to B USB cable shown in figure 6, then write the program code on the IDE, and finally upload it to the Arduino.

Using hardware programs to build up a real application is proved to be satisfactory and promising in terms of speed, versatility and security. Arduino is one of the most popular microcontrollers. It can be used in applications to provide many security features. Due to the limited processing power and memory of Arduino, it yields in a pretty poor performance especially when RSA algorithm is involved. By integrating Java card, the efficiency of RSA encryption and decryption computation on Arduino has been nicely accelerated. In figure 7, we show how Arduino Microcontroller could be used to implement RSA Algorithm.

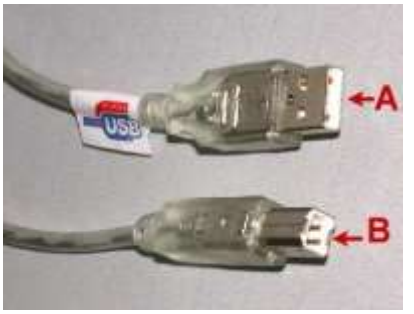

Figure 5: A-B USB cable

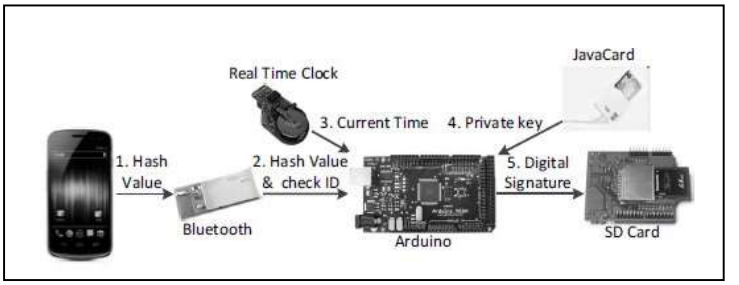

Figure 6: The required components for the proposed Hardware Platform

3. System Design and Evaluation

The proposed crypto-architecture of RSA is shown in figure 9. The flowchart shows the complete design stages which starts by generating two large prime numbers (p, q) through the random number generator unit along with primality testing unit and ends by encryption/decryption processes. We have included the text-number conversions which implemented using the ASCII Coding/Decoding tables with extended lists which includes 255 different codes (8-bits coding). We have implemented this system on Arduino Integrated Development Environment MEGA 2560 with external touch LCD as shown in figure 8. Furthermore, we added two 4x4 keypads to messages of encryption and decryption where we combined them all in one cabinet to get the final product (THE RSA MCU) shown in figure 10.

Figure 7: Arduino MEGA with SainSmart C46 LCD kit

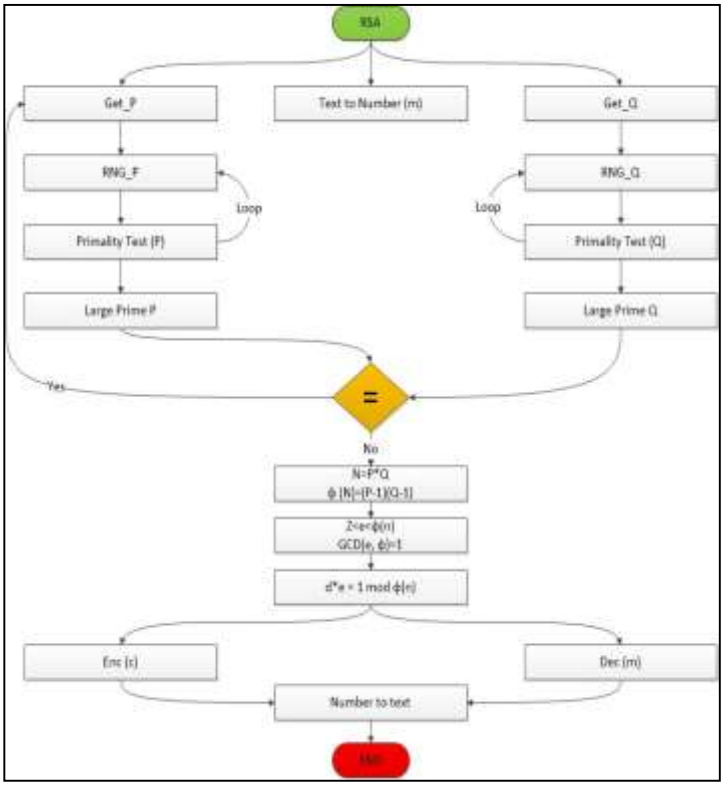

Figure 8: Flowchart Parallel RSA- All stages

The experimental evaluation is a functional technique that commonly used in measuring the performance characteristic and the efficiency of such a cryptosystem design. Therefore, after developing our design and implement it, we analyze and evaluate the result that we found, in order to improve our cryptosystem. Typically, various parameters are involved in calculating the numerical evaluation for our design. However, our cryptosystem implemented in several design environments in order to insure higher security levels for different applications. Figure 11 shows the evaluation life cycle of the proposed design.

Figure 10: Evaluation Diagram

Finally, we have tested the other implemented version of our 32 bit RSA Cryptoprocessor which is based in Arduino Microcontroller. Table 2 and figure 12 show the timing delay in encrypt different size of messages.

Table 2. Time characteristic of encryption using Arduino Microcontroller

Size (Kbyte)	10	25	50	80
Time (ms)	420	936	1698	2592

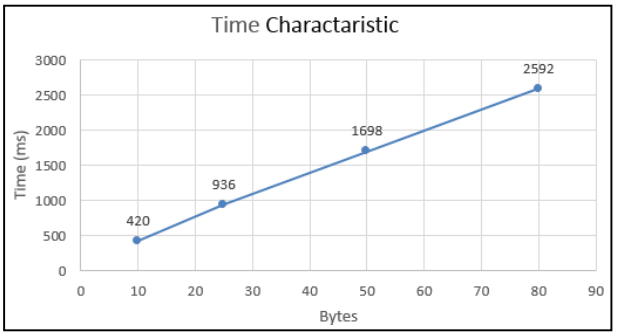

Figure 11: Time characteristic of encryption using Arduino Microcontroller

As seen from figure 12, the relation between the message size and the time required is liner due to the block size of the encryption that used in this version. Such results are useful in some applications of wireless sensor networks where the amount of communicated data is very small.

4. Conclusions and Future works

A tiny RSA crypto-controller has been successfully implemented and verified using Arduino MCU along with double keypad and screen touch. The design is reconfigurable in terms of key sizes; however we have tested the design for 32-bit encryption and decryption keys which considered as a small key size to infrastructure networks. Therefore, such security system is considered useful for the Adhoc distributed sensory network as it can be connected near to the sink especially if it is supported with rechargeable battery along with a small solar cell (12 volts). In future, this design can be stretched out to higher encryption and decryption bit-size by revising and modification of the utilized algorithms. Also, several public and symmetric key cryptographic algorithms could be designed and verified using the design sets mentioned in this paper; such as: El-Gamal Cryptosystem, Diffie-Helman Key exchange system, Data Encryption Standard (DES), Advanced Encryption Standards (AES), and many others.

Acknowledgements

Authors appreciate the publication support of College of Engineering at King Faisal University (KFU). Special Thanks due to Prof. Amjad Omar (Chairman of EE Department) and Mr. Ibrahim Al-Daej (Administrator of Financial Affairs) for their support and help.

References

1. Richard A.Mollin. An Introduction to Cryptography: 2nd edition. *Chapman and Hall/CRC*, ISBN-10: 1584886181, 2006 pp 37-39.
2. Qasem Abu Al-Haija and A. Al-Badawi. Cost-Effective Design for Binary Edwards Elliptic Curves Cryptoprocessor Over GF (2N) Using Parallel Multipliers & Architectures. *International Journal of Information & Computer Security (IJICS)*, Inderscience, V.5 (3) 2013.
3. REUTERS. Aramco Says Cyberattack Was Aimed at Production. *Saudi Aramco Company*, December 9, 2012, http://www.nytimes.com/2012/12/10/business/global/saudi-aramco-says-hackers-took-aim-at-its-production.html.
4. Echo P. Zhang. A Simple and Efficient Way to Combine Microcontrollers with RSA Cryptography. *The World Congress on Engineering and Computer Science* (2013) Vol I, ISBN: 978-988-19252-3-7.
5. M. Riley. Programming Your Home: Automate with Arduino, Android, and Your Computer. *The Pragmatic Programmers*, 2012.
6. Arduino manual. Arduino Microcontroller. *Arduino website*, 14 Dec 2013. [Online]. Available: http://arduino.cc/en/Reference/HomePage.
7. Q. Abu Al-Haija, et. al. Hardware and Software Simulation for Classical Cryptosystems. *4th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN-13)*, Ontario, Niagara Falls, Canada, 21-24, Oct-2013