Journal of Information Engineering and Applications
ISSN 2224-5782 (print) ISSN 2225-0506 (online)
Vol.8, No.1, 2018

RSA Public Key Cipher Implementation using Microcontroller

Waleed Noori Hussein[*1] Dhuha Habeeb Mutasher [*2] Ethar Habeeb Jasem[*1] Liqaa Nabeel Sabeeh[2]
1.Department of Computer Techniques Engineering , Iraq University College, Basra, Iraq
2.Department of Computer Engineering , Iraq University College, Basra, Iraq

Abstract
Cryptography is an important part of modern world network security which makes the world of computing a safer place. The RSA algorithm is extensively used in the popular implementations of Public Key Infrastructures. This research discusses the cryptography concept. This research aims to examine and implement a GUI for RSA algorithm to cipher text with Arduino which consists of three stages: key generation, encryption, and decryption. The connection between LCD, keypad, Arduino and mobile are further presented.
Keywords: Cryptography, RSA, Arduino, Security.

1. Introduction

Today Cryptography is a powerful tool used to protect the information in computer systems. Network Security & Cryptography is a concept to protect the network and data transmission over a wireless network. The fast development of technology, the transmission of confidential data in a secure way gets a big deal of attention. The conventional methods of encryption can only maintain the data security (Masram, Shahare et al. 2014). Information may be reached by malicious hacker's .therefore, it is important to provide an effective encoding and decoding method to make sure all data are enhanced and secured. The authorization of accessing data in a network is involved with Network security, which is handled by the network administrator. Clients provide with or are assigned an ID and password or any other authenticating information which provide them access to any data and programs within their authority (Stallings 2006). Network security includes many different types of computer networks, which include public and private, they are used in every network security providing transactions and communications between businesses, government agencies, and individuals. Networks may be private, same as within an enterprise, and others which may be open to public access.

Nowadays, cryptography plays a major role in protecting the information of technology applications. Cryptography actually means secret writing, even the ancient human desired to keep and store secrets (Miano 1999, Pianykh 2009, Dhakar, Gupta et al. 2012). In ancient days, cryptography was available only to generals and Emperors, but today it is nearly used by everyone, every day, every time when a credit card transaction is done, a phone call is made, secure website is used; there is a use of cryptography. In cryptography original message is basically encoded in some non-readable format. This process is called encryption. The only person who knows how to decode the message can get the original information (Aleisa 2015). This process is called decryption. Figure 1 shows the process of cryptography.

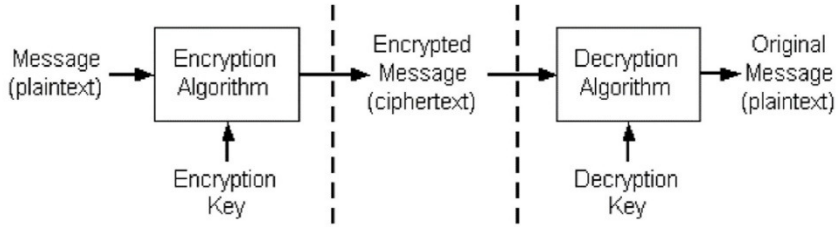

Figure 1: Cryptography process

This research examines and implements a GUI for RSA algorithm with Arduino which consists of three stages: key generation, encryption, and decryption. As well as the connection between LCD, keypad, Arduino, and mobile.

2. Cryptography Concept

Cryptography is a science which investigates methods of protecting information. Protection of information is an activity (or a set of activities) for providing security of the information; in its turn, information security is such a property of the information environment, which implies the presence of at least one of the following attributes (factors) of the information (depending on the requirements) (Mckay 2005, Chandramouli, Bapatla et al. 2006):

1. Confidentiality a possibility to access the information only by its sender and addressees;
2. Integrity an ability for the receiver of the information to discover the fact of modification of the information if any by third parties after the information has been sent by its sender;
3. Authenticity an ability for the receiver of the information to determine the real sender of the information.

3. The Rsa Algorithm

RSA is founded in 1977 is a public key cryptosystem. RSA is an asymmetric cryptographic algorithm named after its founders Rivest, Shamir &Adelman. It generates two keys: a public key for encryption and private key to decrypt the message (Preetha and Nithya 2013). RSA algorithm consist of three steps, step one is key generation which is to be used as key to encrypt and decrypt data, step two is encryption, where actual process of conversion of plaintext to cipher text is being carried out and the third step is decryption, where encrypted text is converted into plain text at other side's is based on factoring problem of finding product of two large prime numbers. Key size is 1024 to 4096 bits (Boneh and Shacham 2002, Preetha and Nithya 2013).

4. Software Implementation

The GUI application was developed using visual basic 6, our application consists of three stages: key generation, encryption, and decryption. The first part (key generation) allows us to know the public and private key. The second part (Encryption) contains two fields (Plain text and Ciphertext).The third part (Decryption) works reversibly to the second part (Decryption).

5. Screenshots Of The Application

Figure 2 shows the main window of our RSA GUI encryption:

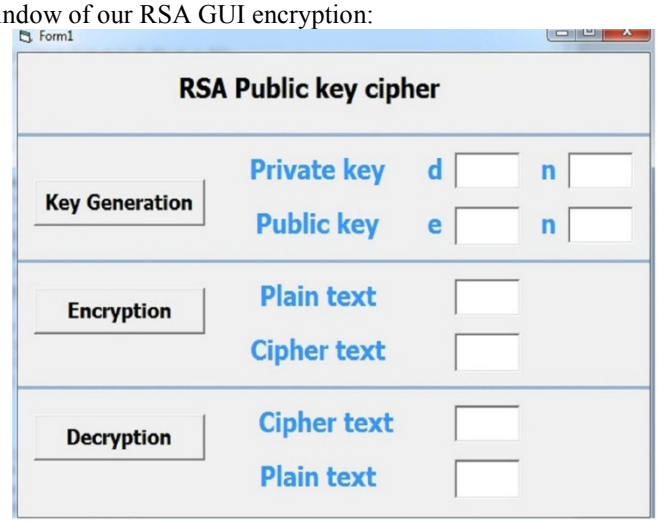

Figure 2: RSA Encryption

When the user clicks on key generation, two keys will be generated a public and private key. Clicking on encryption will give us the cipher text, and clicking decryption will return the original text

6. Hardware Implementation

The connection that has been implemented in this research are presented with the use of Arduino. An Arduino board consists of an Atmel 8-bit AVR microcontroller with complementary components that facilitate programming and incorporation into other circuits. Four connection methods have been established in this research:

6.1 The connection between Arduino and keypad

The keypad (4*4) that contains 8 output wires was connected to the Arduino (mega 2560) pins from pin 2 to pin 9 as shown in Figure 3. The code of keypad was written in the Arduino program.

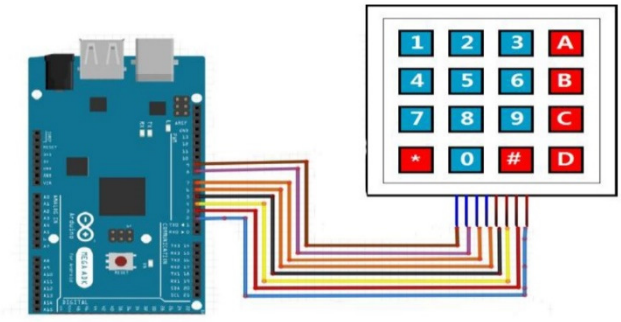

Figure 3: Arduino and keypad connection

Keypad wire 1 to digital pin 2(D2)
Keypad wire 2 to digital pin 3(D3)
Keypad wire 3 to digital pin 4(D4)
Keypad wire 4 to digital pin 5(D5)
Keypad wire 5 to digital pin 6(D6)
Keypad wire 6 to digital pin 7(D7)
Keypad wire 7 to digital pin 8(D8)
Keypad wire 8 to digital pin 9(D9)
Arduino power to computer USB port.

6.2 The connection of LCD

This connection has been accomplished by using a keypad, LCD, breadboard as shown in Figure 4 below. This sketch print "Hello World!" to the LCD and uses the display () and no Display () functions to turn on and off the display.

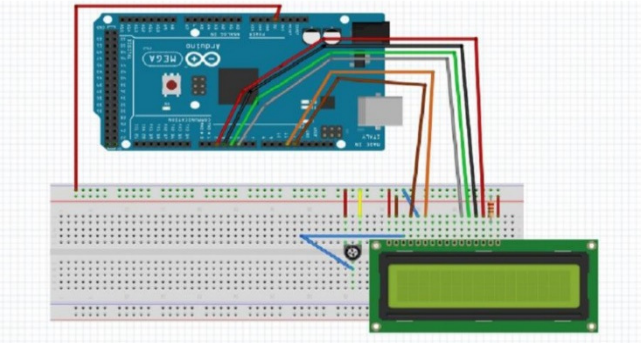

Figure 4: LCD connection

The Circuit:
LCD RS pin to digital pin 12
LCD Enable pin to digital pin 11
LCD D4 pin to digital pin 5
LCD D5 pin to digital pin 4
LCD D6 pin to digital pin 3
LCD D7 pin to digital pin 2
LCD R/W pin to ground
10K Resistor:
Ends to +5V and ground
Wiper to LCD VO pin (pin 3)
When the connection takes place, then the code is written within the Arduino program for verification.

6.3 The connection of keypad and LCD

The connection is established by connecting the Arduino, keypad, and LCD together, and then the code of ciphering was written in Arduino software, this sketch print two choices: "Encryption “and" Decryption" to the LCD. We choose what we want to do by using the keypad as shown in Figure 5.
The circuit:

- Keypad wire 1 to digital pin 6(D6)
- Keypad wire 2 to digital pin 7(D7)
- Keypad wire 3 to digital pin 8(D8)
- Keypad wire 4 to digital pin 9(D9)
- Keypad wire 5 to digital pin 2(D2)
- Keypad wire 6 to digital pin 3(D3)
- Keypad wire 7 to digital pin 4(D4)
- Keypad wire 8 to digital pin 5(D5)
- LCD pin K to negative part
- LCD pin D7 to Arduino pin 22
- LCD pin D6 to Arduino pin 24
- LCD pin D5 to Arduino pin 26

- LCD pin D4 to Arduino pin 28
- LCD pin E to Arduino pin 11
- LCD pin D6 to Arduino pin 24
- LCD pin RW to Negative part
- LCD pin VO to transistor
- LCD pin VDD to positive part
- LCD pin VSS to negative part
- Arduino pin 5V to positive part
- Arduino pin GND to negative part.

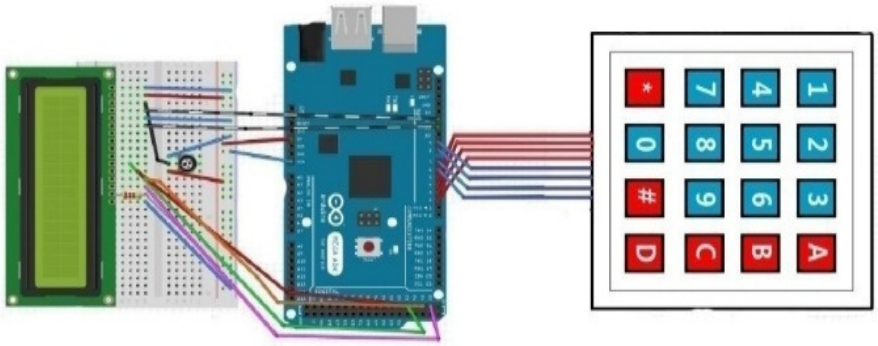

Figure 5: Keypad and LCD connection

6.4 The connection between LCD, keypad, and mobile

The connection of the mobile with Arduino, keypad, and LCD is provided, so users can cipher text by using the mobile, the code is written in Arduino software, then, the mobile will display two choices: 1 Encryption, 2 Decryption. The first (Encryption) will request to enter: a) public key, b) N, c) text 1+ text 2. The second (Decryption) will request to enter: a) private key, b) N, c) ctext1+ctext. We use the public key, private key and the N from the RSA Encryption program that it exists in the computer as shown in Figure 6.

The circuit:

- Keypad wire 1 to digital pin 6(D6)
- Keypad wire 2 to digital pin 7(D7)
- Keypad wire 3 to digital pin 8(D8)
- Keypad wire 4 to digital pin 9(D9)
- Keypad wire 5 to digital pin 2(D2)
- Keypad wire 6 to digital pin 3(D3)
- Keypad wire 7 to digital pin 4(D4)
- Keypad wire 8 to digital pin 5(D5)
- LCD pin K to negative part
- LCD pin D7 to Arduino pin 22
- LCD pin D6 to Arduino pin 24
- LCD pin D5 to Arduino pin 26
- LCD pin D4 to Arduino pin 28
- LCD pin E to Arduino pin 11
- LCD pin D6 to Arduino pin 24

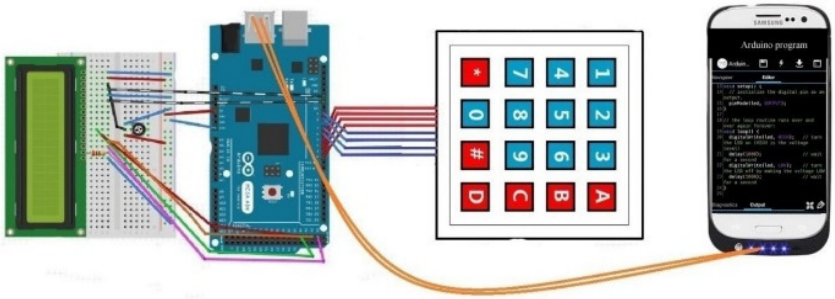

Figure 6: LCD, keypad and mobile connection

7. Conclusion

In this research paper we have discussed the concept of cryptography .We have also discussed the software and hardware implementation. In his paper RSA algorithm was used for key generation, encryption and decryption. A GUI for RSA algorithm was designed to cipher text with Arduino. The encryption and decryption were done in two stages, in the first stage we cipher text by using Arduino only, and the second stage we cipher text by using Arduino and mobile. For future implementation, encryption can be achieved by using RSA algorithm with Adriano to cipher images and voices between two Arduino and two mobile.

References

Aleisa, N. (2015). "A Comparison of the 3DES and AES Encryption Standards." International Journal of Security and Its Applications **9**(7): 241-246.

Boneh, D. and H. Shacham (2002). "Fast variants of RSA." CryptoBytes **5**(1): 1-9.

Chandramouli, R., S. Bapatla, K. Subbalakshmi and R. Uma (2006). "Battery power-aware encryption." ACM Transactions on Information and System Security (TISSEC) **9**(2): 162-180.

Dhakar, R. S., A. K. Gupta and P. Sharma (2012). Modified RSA encryption algorithm (MREA). Advanced Computing & Communication Technologies (ACCT), 2012 Second International Conference on, IEEE.

Masram, R., V. Shahare, J. Abraham and R. Moona (2014). "Analysis and comparison of symmetric key cryptographic algorithms based on various file features." International Journal of Network Security & Its Applications **6**(4): 43.

Mckay, K. (2005). "Trade-offs between Energy and Security in Wireless Networks Thesis."

Miano, J. (1999). Compressed image file formats: Jpeg, png, gif, xbm, bmp, Addison-Wesley Professional.

Pianykh, O. S. (2009). Digital imaging and communications in medicine (DICOM): a practical introduction and survival guide, Springer Science & Business Media.

Preetha, M. and M. Nithya (2013). "A study and Performance Analysis of RSA Algorithm." IJCSMC **2**: 126-139.

Stallings, W. (2006). Cryptography and network security: principles and practices, Pearson Education India.