International Journal of Advanced Computer Technology (IJACT)
ISSN:2319-7900

Smart Phone-Arduino based of Smart Door Lock/unlock using RC4 stream Cipher Implemented in Smart Home

Dr Abbas M. Al. Bakry, Rajaa D. Resan

Abstract: Security is considered as important issue especially in design smart home. In this paper, we've focused on an authentication problem in design smart door lock by using RC4 cipher stream for encryption/decryption smart-phone information which contains a unique data.

This work has contains two main parts, Android application (remote control) and control circuit using Arduino UNO, also the communication medium is Bluetooth technology used transceiver information and commands in this work.

The main purpose of the design smart door lock using RC4 algorithm is to enforce security based on personal smart-phone information, and the results shows more strength authentication for access in real-time.

Keywords: RC4, authentication, Arduino UNO, Android

1. Introduction

The modern design of smart homes has focused on smart controls and convert conventional switches to centralize control system [3]. The smart home technologies have focused on networking (wiring and wireless systems), controlling (remote control, smart phones, and web browsers), and smart devices (green, energy consumption, security, environment, and entertainment) [4,5,6,7]. An illustration of smart home technologies is shown in figure(1).

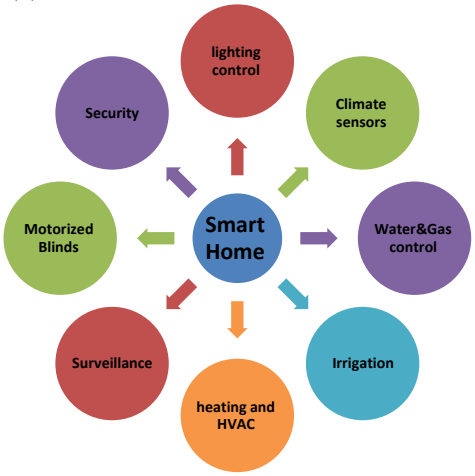


Figure (1) Category of smart home services

The remote controllers in smart have been used in various services such as home appliances control; reduce power consumption, communication and security. In this work, we've focus on implementation of the security issue in smart door lock [2].

Smart door lock is considered as a smart access control based on authenticated person to lock/unlock the door in smart home. One of the most advantage of design smart door lock is to control door open/close by an authentication person, other advantage is can be accessed using smart phone where the use normal key may be lost or stolen[1].

There are several challenges and approaches regarding security issues in smart door lock, using GSM technology to send SMS to door controller and receive message to the owner; GSM not secured enough and can operate the controller by other users [8], using Bluetooth to lock/unlock door by send normal commands [9], based on PIR (motion sensor) locking/unlocking the door; this approach has using authentication process [10], based on RFID as accessed, RFID can be damage when affected by magnetic field [11].

In this paper, the command send to controller has been collect the information of authenticated user's smart phone and these information encrypted by RC4 algorithm and the cell phone number has been chosen as the encrypted key. The connected between smart phone and door controller based on Bluetooth technology.

2. RC4 stream cipher

RC4 is considered as one of the popular and fast simple stream cipher algorithms and [12]. RC4 has two main components which are (Key Scheduling Algorithm -KSA- and Pseudo Random Generation Algorithm -PRGA-) [13]. Below, describing RC4 components operation in pseudo-code form.

KSA Input: stream, secret key K Output: S-box , S generated by K	PRGA Input: S-box, S of KSA Output: Random stream, z

for i=0,..N-1
S[i] = i;
next i
j=0;
	i=0, j=0;
	while TRUE
	i=i+1;
	j=j+S[i];

ISSN:2319-7900

for i=0, .., N-1 j=j+S[i] + K[i] swap (S[i], S[j]); next i	swap (S[i], S[j]); z=S[S[i] + S[j]];

KSA step is applied to scramble the array of password's character values and swapping current index with previous one.

The size of array S is same size of stream's character number N. First, the array S has entries with digits numbers through length of size of S. Then, S array contains the j-th entry by swapped entries as calculated in eq(1).

$$j = \lfloor j + S(i) + key[i \bmod k - length] \rfloor mod\ 256 \ldots . (1)$$

Where j is considered as the previous j value, and S[i] is value of current stream contain, key[i mode k-length] is return 0 or 1.

The next step in RC4 is PRGA generates the key-stream bytes of log2 N bits, then, XORed with the plaintext to produce ciphertext in final.

3. Proposed Work

The proposed work has focused on design hardware for smart door lock using Bluetooth technology and Android OS, besides the implementation of RC4 algorithm for authentication access. The phases of proposed design have been illustrated as shown in figure (2).

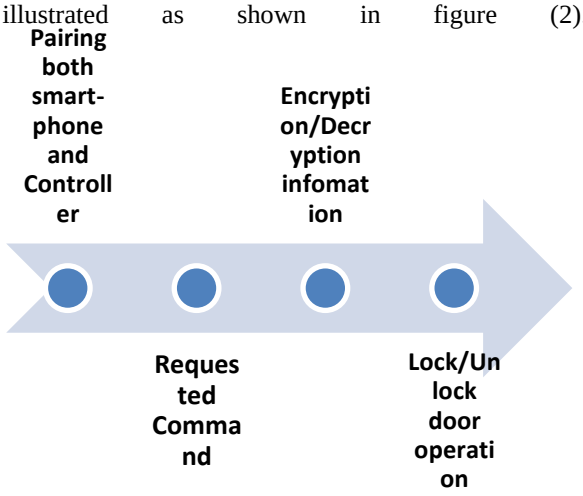


Figure (2) proposal work phases

In our design, we've design an application using smart-phone with Android platform as remote control. The Android platform has including Bluetooth APIs which provides to access to the Bluetooth functionalities. To create connection between remote control and electronic controller circuit for door lock, need to initialize the server and client socket on same channel. Then, the server side is listening to the request of client side, and the last one waiting for permission from server for accepting pair. The remote control application design is shown in figure (3).

Figure (3) remote control application designed in Android platform

The Bluetooth command in remote control application used to display list of Bluetooth devices within the range of detection. The procedure of Bluetooth API is shown in figure (4).

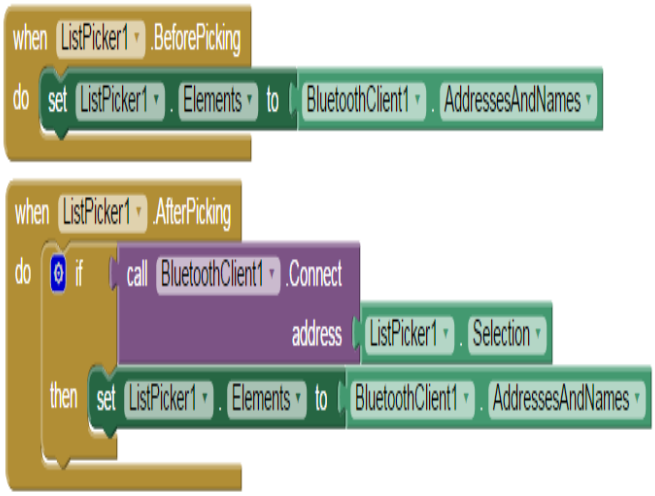


Figure (4) Bluetooth pairing step in client side

After the pairing step has done, the client has collecting the information of the device and select device ID. In the proposed work, device ID has considered as the plain stream because it is unique information and phone number is considered as the key-stream. The flow code of retrieving device information is shown in figure (5).

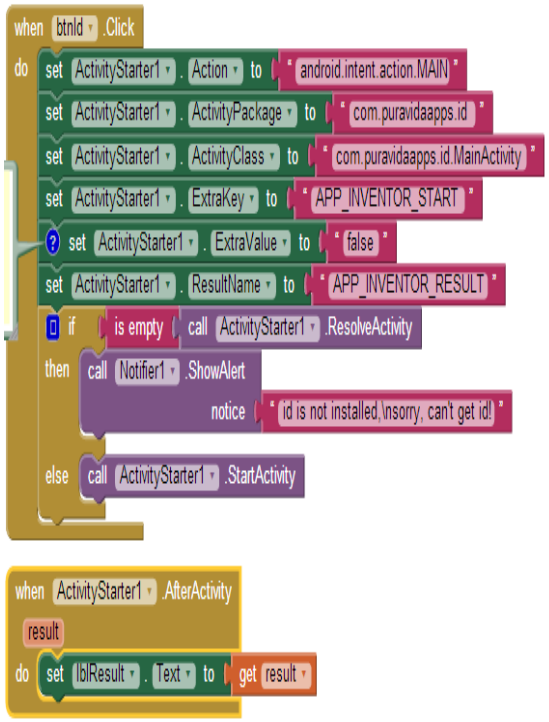


Figure (5) Procedure for retrieving device information

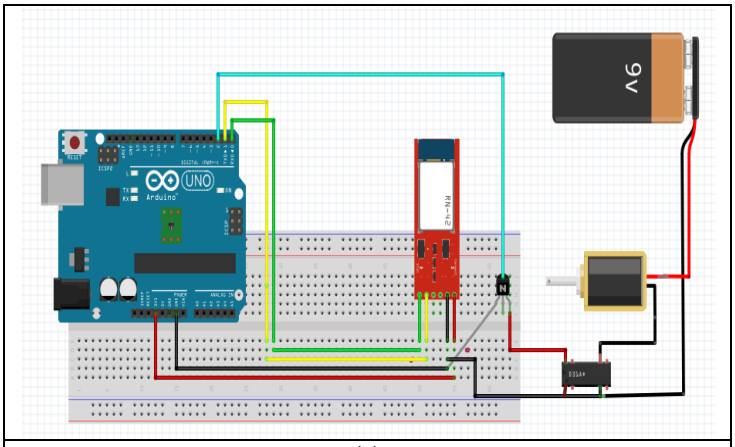
As notes from figure (3) there are two commands (On/Off) used to control door lock. Within each of these commands, RC4 stream cipher has been applied to encrypting the information before send it to the circuit control. The first step of RC4 is Appling KSA, this algorithm has two inputs (stream and k). The stream in this design has obtained from device ID, and k-stream has obtained from phone number. The results of encryption of RC4 by applying this information is described in table (1).

Table (1) RC4 encryption in client side (smart-phone)

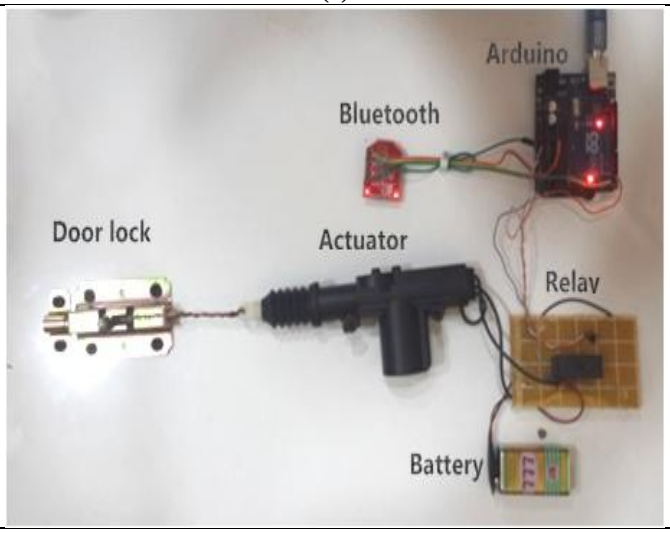
Device ID	Phone Number
13a24944c7bf6230	07709256291
RC4 Encryption	
pny9nf"0ZJfBPYX52"yV6a	

The control circuit received the encrypted plain text. The design of control circuit has using Arduino UNO kit as controller and Bluetooth module (HC-06), the whole hardware elements in proposed design is illustrated as schematic circuit and real design as shown in figure (6).

The Arduino UNO has contains microcontroller (ATMEGA328) which as USB connection, PWM, analogue, and digital feature. In the proposal work, Bluetooth module (HC-06) is connected to serial pins with microcontroller (TX and RX) and power with 3.3v as shown in figure (7).



(a)



(b)

Figure (6) proposed hardware design (a) schematic circuit, (b) real design

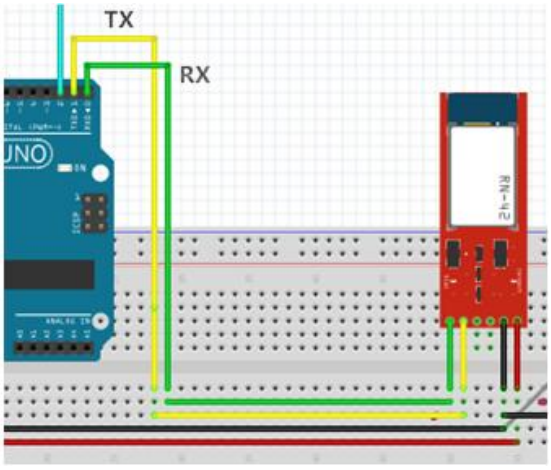


Figure (7) Schematic diagram of Bluetooth module connection to Arduino UNO

There has been using actuator (12v) mounted on door used to lock/unlock operation. The actuator has driven by driver circuit designed by using transistor as switching mode and relay (5v) connected

ISSN:2319-7900

to one of digital pin of Arduino UNO as shown in figure (8).

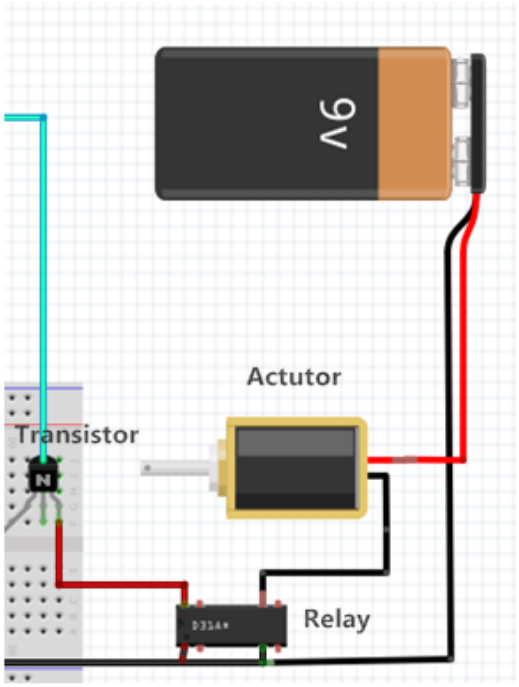
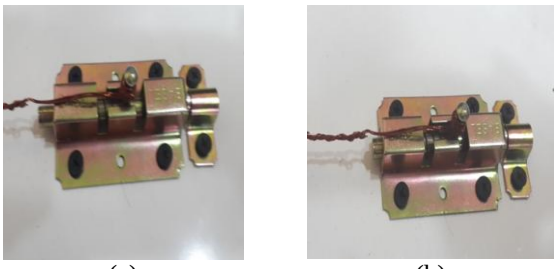


Figure (8) Actuator driver circuit design

Table (2) RC4 decryption in control circuit (Arduino UNO)

Encrypted plain text	Phone Number
pny9nf"0ZJfBPYX52"yV6a	07709256291
RC4 Decryption	
13a24944c7bf6230	

There are two states of actuator which are switch on and off depending on command sent by smart-phone. Each state of actuator has represented as shown in figure (9).



(a) (b)

Figure (9) Actuator states, (a) normally close, (b) open

4. Conclusions

Smart home technology is involved with various fields (security, power consumption, communication, etc). Security issue is becoming more important and developed day by day.

The suggestion in this paper is apply RC4 cipher stream to encrypt/decrypt phone information as an authentication for door access by lock/unlock the actuator mounted to door. The proposed design has focused on developing door lock using Android platform for design a remote control, and Arduino UNO as control circuit to receive encrypted information sent by personal smartphone, then decrypt the information and take decision to lock/unlock the actuator of door.

References

1. Ravindra Das; "Biometric Technology, Authentication, Biocryptography, and cloud-based Architecture", CRC press, 2015.
2. Rohit Kadam, Pranav Mahmauni, and Yash Parikh; "Smart Home System"; International Journal of Innovative research in Advanced Engineering (IJIRAE), Volume (2) issue (1), 2015.
3. Mustafijur Rahman, A. H. M. Zadildul Karim, sultanurNyeem, Faisal Khan, and GolamMatin; "Microcontroller Based Home Security and Load Controlling Using GSM Technology"; I. J. Computer Network and Information Security, 2015.
4. Rohit Kadam, Pranav Mahmauni, and Yash Parikh; "Smart Home System"; International Journal of Innovative research in Advanced Engineering (IJIRAE), Volume (2) issue (1), 2015.
5. NazrulAnuarNayan,Ili A. M. Ikhsan, and Yasuhiro Takahashi; "Using ZigBee Communication Technology in a Smart Home Wireless Sensor Network"; Proceedings of Second International Conference on Modern Trends in Science, Engineering and Technology, 2014.
6. Rajeev Piyare and Seong Ro Lee; "Smart Home Control and Monitoring System Using Smart Phone"; ICCA, Volume (24), 2013.
7. JayashriBAngali and ArvindShaligram; "Design and Implementation of Security Systems for Smart Home based on GSM Technology"; International Journal of Smart Home, Volume (7), issue (6), 2013.
8. F. Shawki, M. El-Shahat. Dessouki,"Microcontroller Based Smart Home With Security Using Gsm Technology", IJRET: International Journal of Research in Engineering and Technology, 2015.
9. Lia Kamelia, Alfin Noorhassan S.R, Mada Sanjaya and W.S., Edi Mulyana, "Door-Automation System Using Bluetooth-Based

ISSN:2319-7900

Android For Mobile Phone", ARPN Journal of Engineering and Applied Sciences, VOL. 9, NO. 10, OCTOBER 2014.

10. Ali Haktan Isilak, "Smart Home Applcations for disabled People by Using Wireless Sensor Network", Faculty of Engineering and Architecture, Departent of Computer Engineer, 2010.
11. Phillip Robinson, "RFID Smart Home: Access Control and Automated-Lighting System", Senior Design Project, 2008.
12. Subhamoy Maitra, Goutam Paul, and Sourav Sen Gupta; "Attack on Broadcast RC4 Revisited", International Association for Cryptologic Research, Springer Verlag Berline, 2011.
13. Sabnam S, Kunal D., and Gitosree K; "Emerging Trends in Computing and Communication", ETCC, Springer new Delhi, 2014.