Design and Implementation of a Smart Digital Door Lock Based on BBS PRNG

تصميم وتنفيذ قفل باب الكتروني ذكي اعتماداً على استخدام خوارزمية بلوم- بلوم- شاب- مولد الرقم المزيف

Zeina Waleed Abbas
University of Technology – Buildings and Constructions Department

Abstract:

Security in smart home considered as a major concern nowdays.In this proposal work, a new implementation of BBS PRNG (Blum BlumShub Pseudorandom Number Generator) to generate new PIN (Personal Identification Number) for digital door lock access. The normal PIN generated from combination of numeric keypad, and this PIN mostly consist of 4-digit and may one of most popular password such as "1234" which easy to break.

The proposal work is to design prototype of electronic circuit for digital door lock using ATmega32 to control the actuator of door, also, a bluetooth module wired to microcontroller to receive PIN from smartphone to lock/unlock the door. The PIN will be generated using BBS algorithm in Android (smartphone) environment and transmitted to digital door lock controller via Bluetooth. The proposed design can enhance the security of control digital door lock by using the PIN generated by BBS PRNG, and performance evaluation of attack both PINs, normal and BBS generated, by using Brute Force attack tools which comes with the BBS is harder and takes years to attack, where normal PIN takes minutes to attack.

Keywords: Smart door lock, PIN, BSS PRNG, Bluetooth, ATMEGA328, Android, Brute Force attack tool.

الملخص:

تعتبر الأنظمة الأمنية في البيوت الذكية احدى الاهتمامات المهمة في هذه الأيام. في هذا العمل المقترح، تم توظيف جديد لخوارزمية (بلوم بلوم شاب – مولد الرقم المزيف) لتوليد الرقم التعريفي الشخصي المستخدم لغرض التحكم بفتح وغلق قفل الباب الالكتروني. أن الرقم المتولد في حالته الاعتيادية يتكون من (4 ارقام) ويتم إدخالها من خلال لوحة المفاتيح الرقمية، وقد يكون من السهولة معرفة وخرق الأرقام المدخلة لبساطة تكوينها واختيارها مثلاً (1234).

في هذا المقترح تم تصميم دائرة الكترونية للسيطرة على قفل الباب الالكتروني باستخدام المتحكم الدقيق ATMEGA328 لغرض السيطرة على المشغل الميكانيكي في الباب، بالإضافة الى انه تم استخدام تقنية البلوتوث لغرض ارسال واستلام الرقم التعريفي الشخصي من جهاز الهاتف الذكي الى دائرة التحكم لقفل الباب الالكتروني. أن الرقم التعريفي الشخصي المقترح في هذا البحث يتم توليده باستخدام خوارزمية (BBS) وتم تصميم برنامج في بيئة أندرويد للأجهزة الهاتف الذكية. والغرض من هذا البحث هو تحسين الأمن للسيطرة على القفل الالكتروني وذلك بتوليد الرقم التعريفي الشخصي، وتم تقييم أداء العمل من خلال التعرف على الرقم السري الاعتيادي (4 أرقام) وعلى الرقم المتولد بطريقة الـ BBS باستخدام أداة (هجوم القوة العنيفة) والتي بالتالي تبين ان الرقم المتولد بطريقة الـ BBS أصعب وتأخذ فترة عدة سنوات لاختراقه في حين الرقم التعريفي الشخصي (4 أرقام) يستغرق دقائق لمعرفته.

1. Introduction

The Federal Bureau of Investigation (FBI) [1] shows in table for property crime included home burglaries, about 8 million property crimeshappened in 2015 in the United States, and about70 percent of which took place in residential homes. A study from the Alarm Industry Research and Educational Foundation (AIREF) in 2010, burglars spend less than 60 seconds for breaking into a home [2]. So, need to make a house harder to harder access, including home security systems, and smart digital door locks. These realities have let the development of many security systems for residential, commercial applications, and smart home take it in consideration during designs and implementations [3].

Specifically focus on the security of smart home technology, which developed, based on some suitability functionalities like door access authentication, reliability of controller circuit design, and secured data in communication medium during pass the key code via wire or wireless medium [4,5]. The digital door lock is one of the most common digital devices take place of conventional types of locks because of the utilize convenience and inexpensive. The digital door lock is an electronic locking system that works by the combination of digital key, security password or number codes sets higher secure protection with reliability over the conventional locking systems. Therefore, it is a good digital device appropriate for checking the access information and controlling the door on or off because everyone has to access to the door lock to go inside or out [6].

2. Related Works

Ismail et al. [7], they have designed method in smart home for door lock to serve the disabilities people to lock/unlock digital door lock via bluetooth. No security issued has implemented, in contrast to our work this approach can be break with short time while our work focused on generated 10-digits long.

Kader et al. [8], in this paper, a design digital door lock using fingerprint model is considered as method for authentication, in contrast to our work, this method need training data (fingerprint samples) and fingerprint model is cost compared to our method which is not need any sensor devices and database.

3. Proposed Smart Door Lock Design

The proposed work is consist of two main blocks, remote device and door lock electronic circuit as show in figure (1).

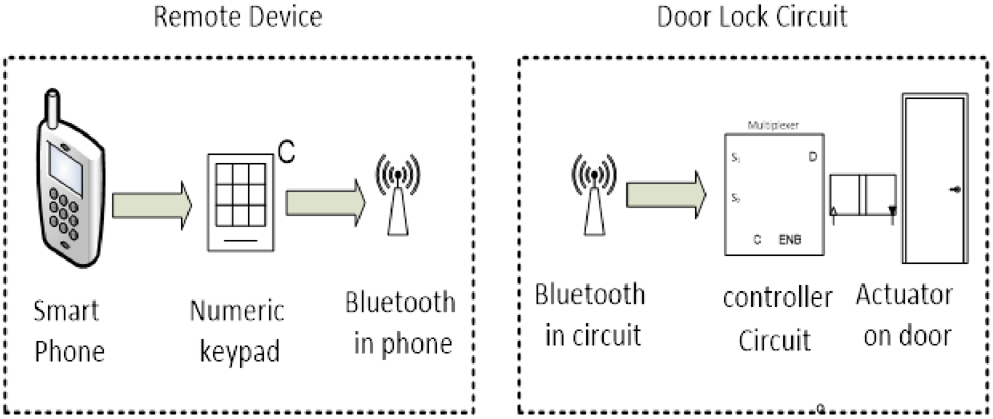


Figure (1): Conceptual Diagram of Proposed Work

4. Remote Device Design and Description

The smart phone is an interactive and integrated frameworks and is consists of several sensors and numerous wireless data communication such as Bluetooth and Wi-Fi [9]. In the proposed work, the programming environment of application design for remote device is Android OS using MIT App Inventor framework [10].

Bluetooth Procedure in Remote Device

The procedure of Bluetooth connection and data transceiver is explain in figure (2).

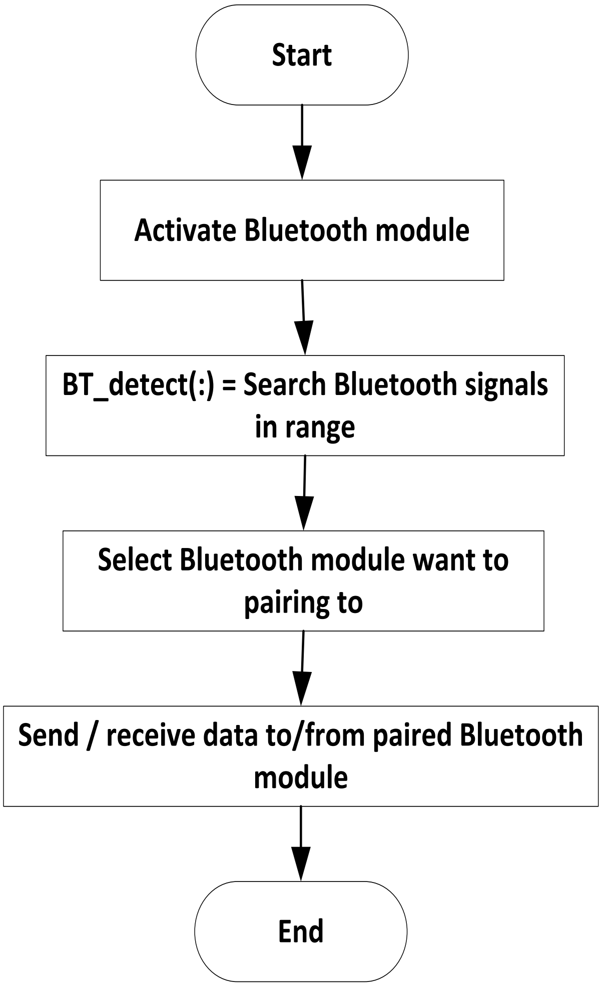
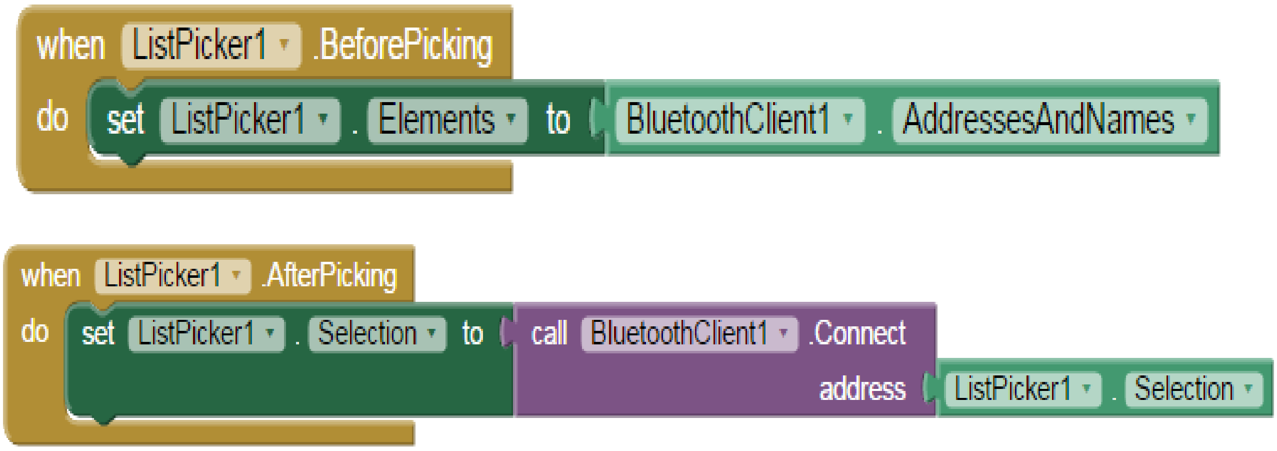

Start
Activate Bluetooth module
BT_detect(:) = Search Bluetooth signals in range
Select Bluetooth module want to pairing to
Send / receive data to/from paired Bluetooth module
End

Figure (2): Bluetooth connection and data transceiver procedure

The flow block diagram of Bluetooth procedure is showing in figure (3)



```
when ListPicker1 .BeforePicking
do set ListPicker1 . Elements to BluetoothClient1 . AddressesAndNames

when ListPicker1 .AfterPicking
do set ListPicker1 . Selection to call BluetoothClient1 .Connect
                                                   address ListPicker1 . Selection
```

Figure (3): Bluetooth flow code in MIT App Inventor

5. Controller Circuit Design and Description

The controller circuit has been designed based on ATMEGA328 microcontroller and Bluetooth modular used as communication medium, in addition, relay (5v) component used to switching the actuator (door lock driver) on/off. The schematic of controller circuit design is showing in the figure (4) below.

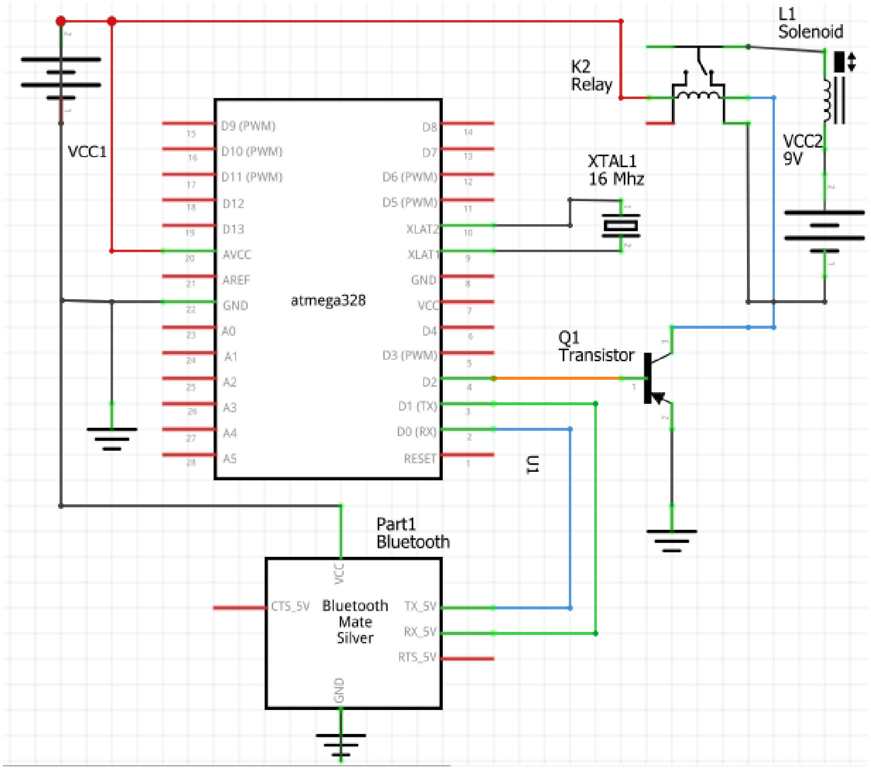


Figure (4): schematic of controller circuit design for proposal work

Controller Circuit Description

The electronic circuit operation has been describe in flow chart in figure (5) below.

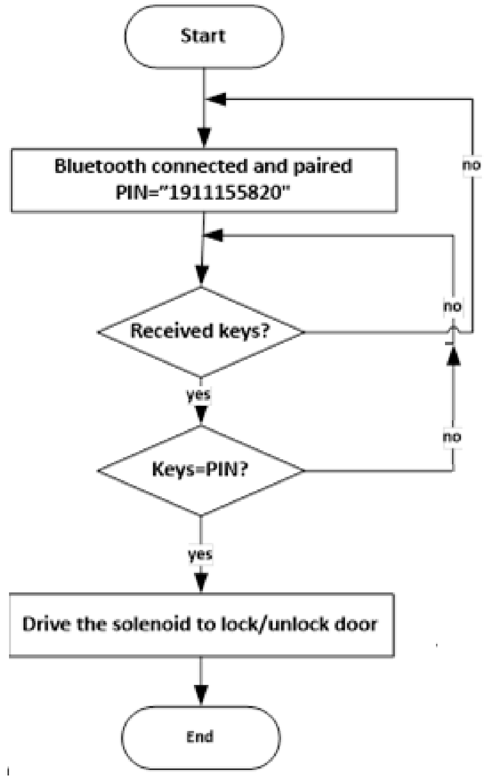

Start
Bluetooth connected and paired
PIN="1911155820"
Received keys?
no
no
yes
Keys=PIN?
no
yes
Drive the solenoid to lock/unlock door
End

Figure (5): Controller circuit operation

6.Implementation of BBS in Remote Device

Thenormal length of user code combination is 4-digits entered by using keypad. In proposed method in this step, after entering the key code, we have applying Blum BlumShub (BBS) algorithm, which is one of Pseudorandom Number Generator (PRNG) to generate complex code. by using BBS equation(1)[11]:

$$x_{n+1} = x_n^2 \, mod \, M \, \ldots\ldots (1)$$

Where M=PQ, P and Q are prime numbers.

The BBS algorithm is explain as showing in figure (6)

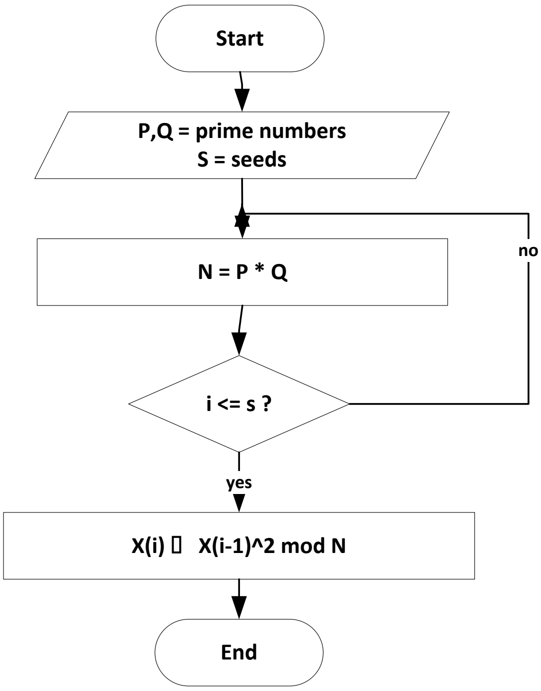


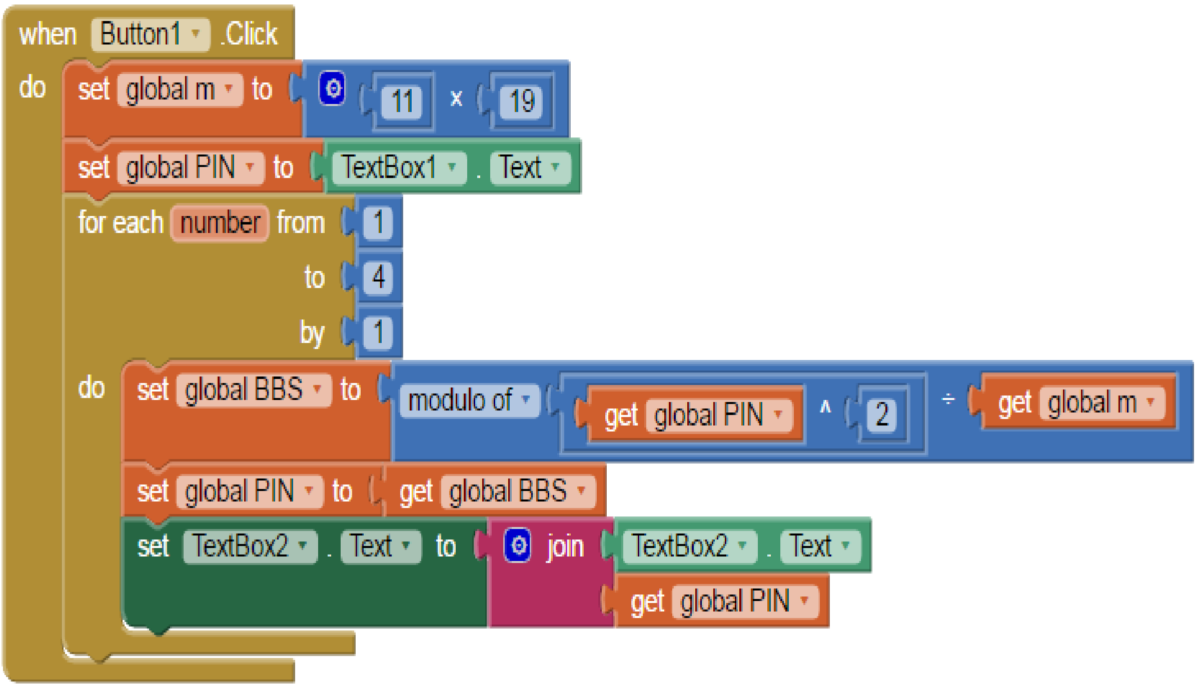
Figure (6): BBS algorithm Procedure

The x(i) is in our case is the digits of PIN number, for example, let the PIN #1234, P=11 and Q=19, N=19*11=209. X(1)=mod(1234 ^2, 209) =191, the second iteration is X(2)=mod(191 ^2, 209)=115, the third iteration is X(3)=mod(115 ^2, 209) =58, finally the X(4)=mod(58 ^2, 209) =20. Next step, we haveused feature fusion method.

The feature fusion is part of data fusion used to concatenated data/features into new set [12].

In this phase of proposed work, we have applied feature fusion method for grouping or combining the BSS results (191, 115, 58, and 20) as in example above, together in one new set (1911155820) to be send to lock/unlock door lock.

BBS algorithm in MIT App Inventor is showing in figure (7).



```
when Button1 .Click
do  set global m to 11 x 19
    set global PIN to TextBox1 . Text
    for each number from 1
                    to 4
                    by 1
    do  set global BBS to modulo of get global PIN ^ 2 ÷ get global m
        set global PIN to get global BBS
        set TextBox2 . Text to join TextBox2 . Text
                                    get global PIN
```

Figure (7): BBS algorithm in MIT App Inventor

The Bluetooth device in controller circuit waiting to pairing with another adapter (Bluetooth device) within the range of signal detection. After detected, need to exchange the passkey, default "1234", when this verified, the both Bluetooth paired now ready to exchange the information, in our work, the PIN number generated by BBS algorithm.

After Bluetooth device received the information, a program in microcontroller will check if the length of the information is matched with saved key, such as the length of BBS number generated is (10) digits if the PIN entered by user in his/her smart phone is (4 digits). The next step is checking PIN received with key saved in microcontroller flash memory if both matched or not.

Finally, if the key and PIN matched, a digital pin (D2) in ATMEGA328 will set HIGH (ON) and send this signal to the base of transistor to switches the load which drive the solenoid to lock/unlock the door.

7. Result Analysis

The main concept of the proposed work is enhancing security of the digital key access in digital door lock. There are two main subjects in the proposed work, the remote controller and the controller circuit.

The remote control, it is an application design based on Android OS for smart phones, used to enter the secured key (4 digits) by digital keypad and this key encrypted by BBS PRNG algorithm to generate complex key code. Then, the generated key transmitted via Bluetooth to the paired one, which attached to controller circuit. The application design of remote control shown in figure (8) below.

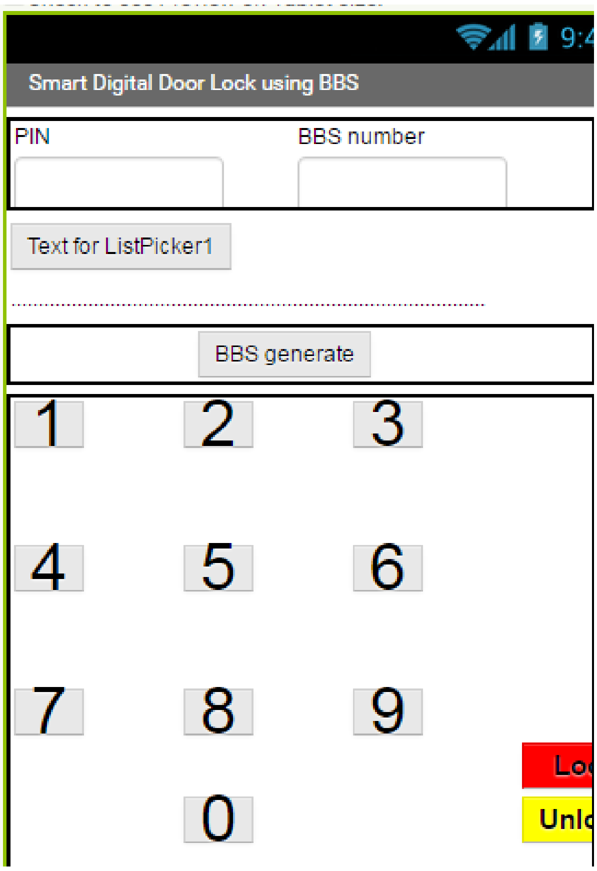


Figure (8): Remote control application design for Android OS

The application of remote control consists of following objects:

- PIN field: textbox used to enter the 4-digits combination key.
- BBS number: textbox used to display the result of generated new key using BBS PRNG algorithm.
- List Picker: a push button used to select a Bluetooth to pair and connect.
- BBS generate: a push button used to generate key using BBS PRNG algorithm.
- 0-9 keys: used to enter a PIN number.
- Lock/Unlock: a push button used to control the digital door lock.

The controller circuit has been design to control the door lock by driving relay to switch the solenoid on/off. In addition, this circuit has a microcontroller ATMEGA328P to control the Bluetooth for pairing and receiving the key, then comparing this key with stored key in flash memory of microcontroller. When the both of keys matched, a command be send to switch the transistor to drive the relay. The electronic components used in controller circuit design shown in figure (9) and described below.

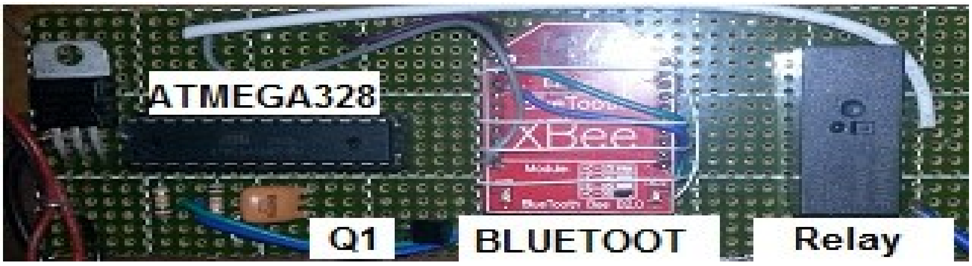


Figure (9): Circuit design for digital door lock controller

- ATMEGA328: a microcontroller has 32kB flash memory and 26 I/O pins, used in proposed work to read data received by Bluetooth and compared the key with stored one, and programmed to drive the solenoid to lock/unlock the digital door lock.
- Q1: transistor designed as switch to drive the relay.
- Relay: used to control the solenoid (on/off).

8. Conclusion

This paper focuses on the design and implementation of smart digital door lock using BBS as new PIN generator with Bluetooth technique as communication medium for transceiver data. The proposal work has two main parts, remote control (smart phone) and controller circuit.

We have evaluate the security of PIN code for digital door lock by applying BBS algorithm compared with standard 4-digits. The comparison evaluated by finding spent time to possible attacking PIN or each PINs using Brute Force attack online tool. The calculation has done for both length of key (4-digits) and key generated by BBS PRNG algorithm. In addition, the setting the delay time or speed of pass password per second is 0.40s considered as a Bluetooth transceiver delay. The experimental results show that the time spent to attack 4-digits is 42min, where the time spent to attack BBS PRNG is about 80 years.

References

[1] https://ucr.fbi.gov/crime-in-the-u.s/2015/crime-in-the-u.s.-2015/tables/table-1

[2] http://airef.org/burglars-confirm-value-of-alarms/

[3] Adnan I., AfhalParavath, and Aswin P., "GSM Based Digital Door Lock Security System", IEEE International Conference on PICC, 2015.

[4] Nagender K. and Subhas C., "Smart Homes, Design, Implementation and Issues", Springer publishing, 2015.

[5] Yong T., Pranesh S., and Jae Y., "Smart Digital Door Lock for the Home Automation", IEEE, 2009.

[6] Thomas Norman; "Electronic Access Control"; Elsevier Inc., 2012.

[7] Ismail, ZarinaTukiran; "Android-Based Home Door Locks Application Via Bluetooth for Disabled People"; IEEE international Conference on Control System, Computing and Engineering, 2014.

[8] M.A. Kader, YousufHaider, Rezaul Karim, Saiful Islam, Mohammad Mamun Uddin, "Design and implementation of a digital calling bell with door lock security system using fingerprint", IEEE, 2016.

[9] Kevin T. Carles C. and Robert D.; "Getting Started with Bluetooth Low Energy", O'REILLY media Inc.; 2014.

[10] Henk C.A van Tilborg; "Encyclopedia of Cryptography and Security"; Springer Sci+Business Media Inc.; 2014.

[11] David Wolber, Hal Abelson,EllenSpertus and Liz Looney; "App Inventor 2, create your own Android Apps"; O'REILLY; 2014.

[12] Koteswara R., Swarna K., and Hima D.; "Acoustic Modeling for Emotion Recognition"; Springer Briefs in Electrical and Computer Engineering, Speech Technology; 2015.