Smart Home Security Design Applying One Time PAD Algorithm

G Gunawan¹, A R Lubis¹, Soeharwinto², Naemah Mubarakah², Deny Jollyta³, and Syahril Effendi⁴

¹Department of Computer Engineering and Informatics, Politeknik Negeri Medan, Indonesia
²Department of Electrical Engineering, Universitas Sumatera Utara, Medan, Indonesia
³Department of Informatics Technology, STIKOM Pelita Indonesia, Pekanbaru, Indonesia
⁴Department of Computer Science and Informatics Technology, Universitas Sumatera Utara, Medan, Indonesia

*gunawan@polmed.ac.id

Abstract. Smart Home Security is a smart system for securing a house or building equipped with a security system applying the One Time Pad (OTP) algorithm. The background of this research is that the system that has been used recently do not use an adequate security algorithm so that it can still be broken by criminals or irresponsible parties. The system designed is intended to reduce or minimize home burglary against the part of the system applied in certain homes or rooms. Due to the imitation of passwords that are always the same or static, they are inputted when performing active or didactive security systems. Besides, to increase the level of security in the security section because of the application of the OTP (One Time Pad) method. The stages of the method are to implement the OTP algorithm and test its reliability and implement it on smart home security.

1. Introduction

Technological advancements especially Home Security System will provide enormous benefits for the security of the house itself, because practically this technology will become a consumption or personal and universal secondary needs so that the users can more easily do the outdoor activities without worrying about valuables things in the abandoned house [1]. Not only as a security system [2], technology that is in this scope can also be applied as a medium that can facilitate daily activities. The house is a basic human need for a place to live and a place to store valuables.

A house has a high risk of being burglarized when the owner is not at home and with the development of technology, it is possible for the house to be broken without the owner’s recognition. Based on this fact, a sophisticated security is required in accordance with technological developments. In this study, researchers will use Arduino as a media to control password encryption which will output via SMS by requesting input from the keypad, this encryption method is called one-time pad. The module of the circuit is that the Arduino mega and with a series of PIR and Magnetic Switch as a sensor that will be used for indoor detection.

Algorithm that will be applied in this research is One Time Pad which is an algorithm for encrypting data and information that is relatively simple and easy to use but is quite safe in ensuring the confidentiality of information or data that you want to send. In this research, the one-time pad algorithm is suitable to be used because the word or password that will be encrypted is not long, consisting of only 6 to 20 characters.
2. Literature Review

All home security systems work with the same basic principles to secure entry points, such as doors and windows, and interior rooms that contain valuable items such as art, computers, jewellery, and money.

The most basic definition of any security system is found in its name. Literally this is a means or method used to secure something through a system of components and interworking devices. In this example, we are talking about a home security system, which is a network of integrated electronic devices that work together with a central control panel to protect against burglars and other potential home intruders. [3] A typical home security system includes:

1. Control panel, which is the main controller of home security systems
2. Door and window sensors
3. Motion sensors, both interior and exterior
4. Wired or wireless security camera
5. Sirens or alarms

A. One Time Pad (OTP)

In the world of cryptography is known as a very strong encoding method that is not easily broken, namely the One Time Pad (OTP) encoding method. The OTP encoding method was first introduced by Gilbert Vernam in the first world war. The OTP encoding method is one of the variations of the substitution encoding method by giving special conditions to the key used, made of random characters / letters (random keys or pad), and it does not use certain formulas. If the key is completely random, used only once, and properly maintained its confidentiality, then this OTP encoding method is very strong and cannot be broken. In classical cryptography i.e. ancient cryptography known as paper and pencil cryptography, the password of the OTP encoding method was obtained by adding or subtracting the original text from the key. The use of this key only and must only be used once. Whereas to retrieve the original text, there is a reduction and addition of the password to the key, as opposed to the encoding process. [4]

B. Encryption dan Description

In cryptography we recognize two processes, namely:

1. Encryption is the process of changing the readable sentences (plaintext) into random messages or messages that have been given a password (ciphertext). The encryption process can be expressed in mathematical notation:
   \[ E (P) = C \]
   Where E is the encryption, P is plaintext and C is ciphertext.

2. Description is the process of returning a text cipher to plaintext. The description process can be expressed in mathematical notation:
   \[ D (C) = P \]
   Where D is a description.

Because the encryption process changes the message then the description translates it and changes to its original form, therefore the encryption and description relationship can be notified as:

\[ D (E (P)) = P \]

In OTP cryptography, the number of keys is equal to the number of plaintexts. If you want the ciphertext to be difficult to solve then the key usage should be:
• Do not use repetitive keys
• Choose a random key
The use of One Time Pad is applied on a series of alphabets A..Z by giving alphabetical values namely A = 0, B = 1, C = 2, D = 3, E = 4 ... until Z.

The formula for doing One Time Pad is:
Encryption: Ei = (Pi + Ki) mod26
Decryption: Pi = (Ei − Ki) mod26

Or the hardware usually applies XOR (⊕) with binary data (plaintext and key are converted into binary formats). This operation is certainly faster on hardware:

Encryption: Ei=Pi⊕Ki
Description : Pi=Ei⊕Ki

C. Arduino Mega
Arduino Mega 2560 is an Arduino-based microcontroller development board using the ATmega2560 chip. This board has a lot of I/O pins, 54 digital I/O pins (15 of which are PWM), 16 analog input pins, 4 UART pins (hardware serial port). Arduino Mega 2560 is equipped with a 16 Mhz oscillator, a USB port, DC power jack, ICSP header, and a reset button [5]. This board is very complete, possess everything required for a microcontroller. Arduino is stated as a platform of physical computing that is open source. Firstly, it should be understood that the word "platform" here is the right choice of words. Arduino is not just a development tool, but it is a combination of hardware, sophisticated programming languages and Integrated Development Environment (IDE).

IDE is a software that is very instrumental in writing a program, compiling it into binary code and uploading it into microcontroller memory. There are many projects and tools developed by academics and professionals using Arduino, besides there are also many supporting modules (sensors, displays, drivers and so on) made by other parties to be able to connect with Arduino. It evolved into a platform because it became the choice and reference for many practitioners.

One of the factors making Arduino attract many people is because of its open source, both for hardware and software [6]. The Arduino electronic circuit diagram is free to everyone. You can freely download the image, buy the components, make the PCB and assemble it yourself without having to pay the Arduino makers. Similarly, the Arduino IDE can be downloaded and installed on a computer for free. We should thank the Arduino team who are very generous distributing the luxury of their hard work to everyone. I personally am truly amazed by the hardware design, the Arduino IDE and programming languages which are high quality and very classy [7].

3. Result And Discussion
Tests carried out include the input, process and output, with the aim of knowing whether each block and the whole can work as expected.

The equipment used is:
1. Arduino serves as the center of the process of the system.
2. The 12V adapter functions as a power source for every installed component.
3. The PIR sensor functions as a detection of body movements and temperature.
4. Magnetic sensor serves as a detector of movement at the door.
5. SIM module 800l serves to send messages.
6. The buzzer functions as an alarm.
After being designed, testing is required to ensure that the designed system can run as planned. The parts that will be tested are Active System, Deactive System, and OTP Password. The followings are the appearance and explanation of the results of the test.

1. **Active System**

   This test aims to determine whether the PIR and Magnetic sensor can detect motion properly. PIR sensors are placed in the room to detect whether there is a movement that occurs when the homeowner is not at home. Magnetic sensors are placed on the door to detect if someone is forcibly opening on the door. If the PIR sensor detects movement and magnetic sensors on the door is open, the buzzer will sound and the LED Strip light will turn on to indicate something happens inside the house, Sim800L will automatically send an SMS notification to the homeowner.

   Active system and active sensor can be seen from the led indicator light or lock picture on the LCD screen. If the System is Active, the LED lights will be red and the lock image on the LCD will be locked.

   ![Figure 1. Led system active turns red](image-url)
2. Deactive System

In a deactive system, both sensors will stop working temporarily, the indicator light will turn green and the open lock image on the LCD will open. The deactive system occurs if the homeowner is at home, this goal functions so that the homeowner is not detected by the sensor.
3. **OTP Password**

In this test will be done when doing Active System and Deactive System. When deactivating the Active and Deactive System, a password that has been made randomly is required so that every time the homeowner wants to activate or deactivate the system, the password will always change and remain the same. To enter the System Active press the "A" button on the keypad then Sim800L will send the password to the homeowner, and for the Deactive System, press the "B" button on the keypad then Sim800L will send a new password.

![Figure 6. LED system deactive turns green](image)

![Figure 7. Password Input](image)

![Figure 8. Result of OTP password](image)
4. Conclusion

Home security system applying the one-time pad method designed to secure the condition of the room when the owner leaves or is not at home, and so that the homeowner knows the condition in the house. One-time pad method is required in the security section so that the password used is not easy to imitate by recording passwords when entering the password input process.

References

[1] A. R. Lubis, F. Fachrizal and M. Lubis, "The Effect of Social Media to Cultural Homecoming Tradition of Computer Students in Medan," in The 4th Information Systems International Conference (ISICO 2017), Bali, 2017.
[2] Safewise (2015). What is Security System?. https://www.safewise.com/home-securityfaq/howdo-security-systems-work
[3] Hadiwibowo, (April 2007). Metode penyandian One Time Pad. https://hadiwibowo.wordpress.com/2007/04/02/metode-penyandian-one-time-pad/
[4] Khoirum, Muslihah. (Juni 2015). Pengertian Cara Kerja Sensor PIR http://khoirummuslihah.blogspot.com/2015/06/pengertian-dan-cara-kerja-sensor-pir.html access: 2 Agustus 2018
[5] https://www.maretron.com/support/manuals/Magnetic%20Switches%20Installation%20Instructions%201.2.html
[6] J. F. Fachrizal, H. A. Adam, Y. Fatmi and A. R. Lubis, "Security of Data Communications Between," in The First International Confrence on Informatics and Computing (ICIC 2017), Jayapura, 2017.
[7] Maretron, LLP . (2018). Installation Instructions MS-1035, MS-1055-N, MS-1075, MS-1085-N Magnetic Switches.