Arduino UNO and Android Based Digital Lock Using Combination of Vigenere Cipher and XOR Cipher

MA Budiman¹, JT Tarigan¹, AS Winata¹
¹Departemen Ilmu Komputer, Fakultas Ilmu Komputer dan Teknologi Informasi, Universitas Sumatera Utara, Jl. Universitas No. 9-A, Kampus USU, Medan 20155, Indonesia

Email: mandrib@usu.ac.id, jostarigan@usu.ac.id, agussuryawinata062@gmail.com

Abstract. Data security becomes an important thing in the computer era nowadays, especially in digital lock. Because of easy to use, there is a lot of digital locks connected to Android smartphone. However, the security of digital lock is lower if commands and passwords exchange is unprotected. That is why algorithm combination concept is important to be applied. Vigenere Cipher and XOR Cipher algorithm combination is simple to be applied, where both are symmetric cryptography algorithm which has advantage in short calculation time, so the plaintext processing can run quickly. To implement the cryptography algorithm combination concept, a digital lock prototype is also needed. One of the best microcontroller for prototyping is Arduino UNO. It can communicate with other devices through Bluetooth connection especially Android smartphone if connected to Bluetooth module. The Arduino UNO based digital lock will communicate with Android smartphone via an application in the smartphone. It is found that Vigenere Cipher and XOR Cipher algorithm combination, and also other support algorithms can improve the secrecy of communication between devices in the digital lock system.

1. Introduction
Digital lock becomes very popular in this modern era, and slowly replace the old mechanic lock. The digital lock is popular for the elite that use technology as a security facility for their properties. The digital locks have various operation method, from the keypad input to the biometric scanning.

However, the development of hacking technique becomes a serious problem faced by the modern digital lock. Some of the digital locks maybe not yet have a secure command communication system, so the sniffing on devices communication can crack the password easily by the sniffer because the communication is not strongly protected.

Cryptography is a science and art of using mathematic techniques to improve message secrecy, that relevant to data and information security aspects [3]. Cryptography is very important in digital security system development. Without strong cryptosystem, the digital security system can be hacked easily by hackers.

Vigenere Cipher is a classic cryptography algorithm based on polyalphabetic substitution, that formulated to revise the weakness of a single substitution algorithm [1]. This algorithm can be implemented easily in various communication media. The use of a single algorithm and simple key weaken the security of a simple cryptography algorithm. So, algorithm combination is very important to improve the digital security system.
XOR Cipher is a strong modern cryptography algorithm that uses exclusive-or logic function to transform every bit in plaintext into ciphertext or vice versa. XOR Cipher commonly used as an additional cipher in a cryptosystem to improve the security of the system [13].

Arduino is an open source electronic circuit that includes an AVR microcontroller as main component, that very popular for electronic devices prototyping because it is easy to use. Android as a Linux based operation system that developed for mobile devices, especially smartphones and tablets. Android smartphone is a very popular device that used as pair device of Arduino in prototyping. Bluetooth is a wireless communication technology that commonly used as media between Arduino and Android communication. Data in Bluetooth communication between Arduino and Android usually has small size and the done in small range between devices. Additional encryption in Bluetooth must be efficient and consume less resource [8].

In this research, we will implement a combination of Vigenere Cipher and XOR Cipher to improve the security of digital lock prototype based on Bluetooth communication between Arduino UNO and Android smartphone.

2. Theories and Methods
This research use an algorithm combination of Vigenere Cipher and XOR Cipher to improve Arduino and Android based digital lock security.

2.1. Vigenere Cipher
Vigenere Cipher is a simple form of polyalphabetic substitution encryption technique, that using chains of different Caesar Cipher based on every single letter in cipher key [9]. Vigenere Cipher is an asymmetric cryptography algorithm. The encryption and decryption Vigenere Cipher algorithm can be formulated as follows:

\[ C_i = (P_i + K_i) \mod 26 \] \hspace{1cm} (1)

\[ P_i = (C_i - K_i) \mod 26 \] \hspace{1cm} (2)

Which \( C_i \) is the character at sequence \( i \) in the ciphertext, \( P_i \) is the character at sequence \( i \) in the plaintext, and \( K_i \) is the character at sequence \( i \) in the cipher key. However, in modern era, electronic message exchange is not just only use 26 alphabet characters, it also includes numbers, punctuations, and also lowercase and uppercase letters. Vigenere Cipher must be expanded using printable ASCII character set. This expansion changes the classic formula of Vigenere Cipher. The encryption and decryption of modified Vigenere Cipher algorithm describes as follows:

\[ C_i = ((P_i - 32) + (K_i - 32)) \mod 95 + 32 \] \hspace{1cm} (3)

\[ P_i = (((C_i - 32) - (K_i - 32)) \mod 95) + 32 \] \hspace{1cm} (4)

2.2. XOR Cipher
Basically, XOR Cipher is a Boolean Exclusive-OR logic function that implemented on binary bits. XOR Cipher is a symmetric cryptography algorithm. Security of XOR Cipher depends on the length and characteristic of the ciphertext. Long ciphertext improve uncertainty and can repel brute-force attack[6]. The encryption and decryption of XOR Cipher algorithm describes as follows:

\[ C_i = P_i \oplus K_i \] \hspace{1cm} (5)

\[ P_i = C_i \oplus K_i \] \hspace{1cm} (6)

Which \( C_i \) is the byte value of the character at sequence \( i \) in the ciphertext, \( P_i \) is the byte value of character at sequence \( i \) in the plaintext, and \( K_i \) is the byte value of character at sequence \( i \) in the cipherkey.

2.3. Three-Pass Protocol
Three-Pass Protocol is a cryptography protocol that allows an encrypted message to be sent securely without cipherkey exchange. That is possible because the sender and receiver have their own cipherkeys for encryption and decryption. The protocol is called so because there are three message exchanges before the message decrypted to the original message. To improve the reliability, this protocol is combined with various cryptography algorithms.

\[ x_{i+1} = x_i^2 \mod n \] ........................ (7)

Which \( x_{i+1} \) is the next result, \( x_i \) is the current result, and \( n \) is a special modulus. Variable \( n \) is a Blum Integer that is the result of multiplication of two prime \( p \) and \( q \); both must result in three if modulated by four, known as Blum Prime. Because \( \rightarrow x \) for lowest-order bit is \( x_i \), lowest-order bits in \( x_i \) becomes impossible to be determined with 50% possibility[4].

2.5. Support Algorithms
There are also many algorithms that support this digital lock system, such as combining and separating functions for manipulating an array of plaintext and transmission string data, cipher key generator function, and primality test function. In the system, we use the Sieve of Eratosthenes algorithm in the primality test function, which is very important for cipher key generator function.

2.6. Arduino UNO
Arduino is an open-source electronic circuit board that includes an AVR microcontroller from Atmel as the main component. Arduino becomes a popular microcontroller that used as a physical computing platform because of easy programming and various support library from its IDE software. Arduino UNO is an ATMega328p based microcontroller board that becomes the one of the best boards for prototyping. Besides reliability, the price is also not expensive[11].

There is also some module that compatible to Arduino that we used to complete the system. They are Bluetooth module for Arduino and Android communication, real-time clock module to support...
cipher key generator function, solenoid lock as the mechanic lock, and Voltage Regulator. The Voltage regulator regulates the voltage between the Arduino, the solenoid lock, and the battery used in the system.

2.7. Android
Android is a Linux based operating system for mobile device developed by Google. Android is especially designed for touchscreen mobile devices such as smartphones and tablets. Android provides open source platform for programmers that develop their applications on various Android devices [5]. We use Android Studio for program the digital lock application. Android Studio is an official IDE (Integrated Development Environment) for Android programming that developed by Google. Android Studio was developed using JetBrains IntelliJ IDEA, and designed for Android applications software development.[12].

3. Result and Discussion
Digital lock system that we developed would be tested based on the main process in the system, the communication between devices. The program in the system would be modified so each device can display the communication data. The communication data would be displayed at toast message in Android and serial monitor in Arduino IDE.

The communication between devices test is purposed to test if the application and the device can run the communication or not. In the test, we find an error that the string length is not consistent in the communication data. Example of the communication error detection displayed as follows.

![Figure 2. Inconsistent communication data length detection](image)

After we tried to find the cause of the error, it was found that byte with value 0 in the string caused the error. Byte with value zero caused error in string based XOR Cipher implementation in Arduino. The error shown as follows.
Figure 3. The effect of byte with value zero in string

Which $P$ is the input plaintext, $K_1$ is the first cipherkey, $K_2$ is the second cipherkey, $C_1$ is the first ciphertext, $C_2$ is the second ciphertext, $C_3$ is the third ciphertext, and $P'$ is the output plaintext in the framework of Three-Pass Protocol communication. We try to solve the error by modifying the functions that return string in the system to functions that return arrays of bytes. The solution works pretty good in Android programming, but cannot be implemented in Arduino IDE because the IDE does not support the function that return array of bytes. We solve this problem by modifying the generated cipherkey value range to minimize the existence of byte with value zero in system communication data. This solution minimizes the system error, but not completely avoid the problem. The example of implementation of the solution shown as follows.

Figure 4. The cipherkey value range modification
Although there is some problem in the digital lock system, the security of the system can be considered good because always results random output and also has good cipherkey management. Example of communication data of the system shown as follows.

**Figure 5.** Communication data when displayed in the application (Lock Opening)

**Figure 6.** Communication data when displayed in Arduino IDE’s serial monitor (Lock Opening)
Which in the term of Three-Pass Protocol, first ciphertext represented by Str1, second ciphertext represented by Str2, and third ciphertext represented by Str3 in the communication data shown above. The three ciphertexts are the communication data that maintain the plaintext secrecy from the application to the device.

Besides being affected by the time, the cipher key also always would be reset for every communication between devices is done. Cipherkey will be reset after the system completes the decryption process, so the cipher key secrecy more guaranteed.

4. Conclusion
According to the result of analysis, design, and testing of the encrypted digital lock, one may conclude that:
- Vigenere Cipher and XOR Cipher algorithm combination implementation is effective to maintain the secrecy of devices communication in the digital lock system, although both are the simple algorithm.
• Real Time Clock-based Blum Blum Shub algorithm implementation as cipher key generator improve the security of digital lock system because it improves the randomness of devices communication data.
• Three-Pass Protocol is pretty good to be implemented in Bluetooth communication between Arduino and Android. The protocol is effective to maintain cipherkeys secrecy, that generated by each device, especially the lock device.

References
[1] Ariska B, Suroso, Endri J 2018 Seminar Nasional Inovasi dan Aplikasi Teknologi di Industri (SENIATI).
[2] Budiman MA, Amalia, Chayanie NI 2017 Journal of Physics: Conference Series 978:1 pp 12086.
[3] Efrandi, Asnawati, Yupiyanti 2014 Jurnal Media Infotama 10:2 pp 120-128.
[4] Kneusel RT 2018 Random Numbers and Computers (Thornton: Springer).
[5] MukherjeeS, Prakash J, Kumar D 2015 International Journal of Computer Science and Mobile Computing 4:3 pp 714-719.
[6] Natsheh QN, Li B, Gale AG 2016 International Conference on Medical Imaging Understanding and Analysis Procedia Computer Science 90:2016 pp 175-181.
[7] Rachmawati D, Budiman MA, Aulya L 2018 10th International Conference Numerical Analysis in Engineering 308 012003.
[8] Ramdhansya AF, Ariyanto E, Nuha HH 2014 Seminar Nasional Informatika (SemnastIF).
[9] Sinaga D, Umam C, Setiadi DRIM, Rachmawanto EH 2018 Dinamika Rekayasa 141 pp 57-64.
[10] Subandi A, Meiayanti R, Sandy CLM, Sembiring RW 2017 Advances in Science, Technology and Engineering Systems Journal 2:5 pp 1-5.
[11] Syahwill M 2013 Paduan Mudah Simulasi dan Praktik Mikrokontroler Arduino (Yogyakarta: Andi Offset).
[12] Verma N, Kansal S, Malvi H 2018 Int. J. of Applied Engineering Res. 13 6 pp 12527-12530.
[13] Yeng, PK, Panford JK, Acquah JBH, Twum F 2016 Int. Res. J. of Eng. and Tech. 3 15 pp 1713-1732.