Design and implementation of keycode encryption for electric door lock embedded system using cryptography algorithm

Y Ariyanto*, K S Batubulan, D K P Aji and N A Sutrisno

Information Technology Department, State Polytechnic of Malang, Malang, Indonesia

*yuri@polinema.ac.id

Abstract. In this digital era the usage of locks is no longer only relies on traditional key systems, but also relies on usage of electronic sensors that can improve security system. Now the threat to keyless locking system does not only come from physical sources but also come from non-physical or digital sources. This threat can be prevented by using cryptography to hide digital data in the system. In this research utilizing a raspberry pi and a servo motor as a locking device, a web server as a data storage center, a mobile device software application as a user interface. Raspberry pi is a mini computer that can be used for various needs. The password will be sent over internet from mobile device to web server and raspberry pi will give a command to the servo to unlock and lock. This study will compare between combination of RSA, 3DES, AES 128 bit, and 256bit AES algorithms to obtain an algorithm that could be operated optimally on the system based on encryption and decryption speed. The final result of this study is a method to implement cryptographic algorithms on smart key systems to obtain better security.

1. Introduction
The development of the use of data encryption systems at this time, experienced a good development. The need for security has become one of the community's needs. One form of fulfilling these security needs is the use of locks on the door to restrict access or prevent unwanted people from entering or accessing the main user area. To meet people's needs for security, various innovations were developed on door lock devices to create a variety of key opening and closing methods, ranging from the use of various physical keys to the use of various electronic sensors. Until the emergence of the smart key concept, which was the application of the principle of the internet to things on key devices. Internet of things (IoT) is the scope in which physical objects are integrated into information networks, where physical objects can become active participants in business processes. With the application of the Internet of things principle to key devices, a keyless locking concept has emerged in which the lock closure method no longer uses physical keys.

In this research, utilizing a raspberry pi and servo motor as a locking device. Then use the web server as the data storage center and process the data encryption algorithm process. In application users, the application interface is cellular based, making it easier for users to run the application on a mobile device.

In the system testing method, the password will be sent via the internet from the mobile device to the web server and raspberry pi will give the command to the servo to open and lock. Analysis of the results of system testing will produce a comparison between the combination of RSA, 3DES, AES 128 bit, and 256bit algorithms, to obtain an analysis of algorithm data that can be operated optimally on the system,
based on encryption and decryption speed. The final result of this research is a method for implementing cryptographic algorithms on smart key systems to get better security.

To support this research, knowledge and understanding of the theory is needed, about the data encryption algorithms used in the system. The supporting theory used by the system, as follows:

1.1. Cryptography
Cryptography is the science of secret writing with the aim of hiding the meaning of a message. Cryptography (Cryptography) comes from Greek, namely from the words Crypto and Graphia which means secret writing. Cryptography aims to maintain the confidentiality of information contained in the data so that the information cannot be known by unauthorized parties, the theory was expressed by Cristof Par and Jan Pelzl in 2010 [1-3].

1.2. RSA (Rivest-Shamir-Adleman) algorithm
The RSA algorithm was introduced by Ronald Rivest, Adishamir and Lonard Adleman [4]. RSA encrypts plaintexts x, where we consider the string of bits that represent x to be an element in \( Z_n = \{0,1,\ldots,n-1\} \). As a consequence, the binary value of plaintext x must be less than n [5]. The same applies to ciphertext [6]. Encryption with the public key and decryption with the private key are as shown in figure 1.

![RSA encryption decryption system](image1)

**Figure 1.** RSA encryption decryption system.

In figure 1, it shows how the RSA algorithm is applied, where x, y, n and d are very long numbers, usually 1024 bits or more. Value e is sometimes referred to as an encryption exponent or public exponent, and private key d is sometimes called an exponent decryption or private exponent. If Alice wants to send an encrypted message to Bob, Alice needs to have a public key \((n, e)\), and Bob decrypts it with the private key d.

1.3. AES (Advanced Encryption System) algorithm
The AES algorithm is almost identical to the Rijndael cipher block. The Rijndael algorithm is a cipher block and the key size varies between 128, 192 and 256 bits. However, the AES standard only requires a 128-bit block size [7]. Therefore, only the 128-bit block length Rijndael algorithm is known as the AES algorithm, shown in figure 2.

![Overview of the AES algorithm](image2)

**Figure 2.** Overview of the AES algorithm.
1.4. Triple Data Encryption Standard (3DES) algorithm

3DES cryptography method is the result of the development of the DES (Data Encryption Standard) cryptography method, where the DES method in development is still insecure in encoding data. In both these algorithms have differences, namely 3DES algorithm uses tripling steps in the DES process, which is used in the encryption process and the decryption process by using three key combinations [8]. In addition, the effective length of the key used by the 3DES algorithm, for the encryption process and decryption process uses 168 bits, where the three sub-keys each have 56 bits, while the DES cryptography algorithm, the method used with key length 56 bit [9].

1.5. Raspberry Pi

The Raspberry Pi is open hardware, with the exception of the main chip on the Raspberry Pi, the Broadcom SoC (System on Chip), which runs many of the main components of the CPU-board, graphics, memory, USB controller, etc. Many projects made with the Raspberry Pi are open and well documented and is something you can build and modify yourself [10].

2. Methodology

2.1. Methodology

In this research, using research methods in the following stages, shows in figure 3.
In figure 3 is shown, at the flowchart, it is explained that the user needs to enter a device identity and password to unlock the smart key that is locked. After the user enters the device id and the application password on the smartphone will send a session request to the web service and will get the session identity and public key which will be used at the RSA encryption stage. Then the application will encrypt the password with the AES algorithm and will generate AES and AES cipher keys. The key generated from the operation of the AES algorithm will then be encrypted using the RSA algorithm using the public key previously received from the web service. After the encryption process is complete the application on the smart phone will send the device identity, session identity, CERTEX AES, and RSA chipertext to the web service and then decrypt it and match the device identity database along with the password, if the combination is correct then the smart key device will open.

2.2. System design
For the implementation of keycode encryption for electric door lock embedded systems [11-13], using RSA and AES, shown in figure 4.

![Figure 4. System design.](image)

In figure 4. it is shown explained that the application on smart phones sends data that has been previously encrypted to the web service and raspberry pi communicates with the web service on the internet through build-in Wi-Fi on raspberry pi. The Raspberry pi is connected to a servo which will act as a lock. Wiring on smart key devices is as follows, shows in table 1.

| Pin Servo | Pin GPIO |
|-----------|----------|
| Ground    | 6        |
| Positive  | 2        |
| Signal    | 7        |

2.3. Hardware and software specification
The design results obtained are the implementation of RSA and AES cryptography on electric door lock embedded system based on raspberry pi. The following are system requirements which include:

- The software specifications used in making this application are as follows: Microsoft windows 7, apache, MySQL, visual studio code, android studio, raspbian pixel, python
- Hardware requirements pc, raspberry pi 3 b, servo, jumper cable.
3. Results and discussion
In the encryption and decryption speed test, the encryption and decryption speed of cryptography used and other cryptography tests that have similar paths with cryptography are used. In this test Cryptography from RSA and AES 128bit will be compared with 3DES and AES 256bit using the same plaintext, shows in table 2.

Table 2. Speed test results.

| No. | Testing Plaintext          | Times (ms) |
|-----|---------------------------|------------|
| 1   | Plaintext : 1234567890123456  |            |
|     | RSA + 3DES               | 611 ms     |
|     | RSA + AES 128 bit        | 422 ms     |
|     | RSA + AES 256 bit        | 822 ms     |
| 2   | Plaintext : abedefghijklmnop |            |
|     | RSA + 3DES               | 732 ms     |
|     | RSA + AES 128 bit        | 455 ms     |
|     | RSA + AES 256 bit        | 864 ms     |
| 3   | Plaintext : abedefgh12345678 |            |
|     | RSA + 3DES               | 745 ms     |
|     | RSA + AES 128 bit        | 537 ms     |
|     | RSA + AES 256 bit        | 788 ms     |
| 4   | Plaintext : 12345678abcd efgh |            |
|     | RSA + 3DES               | 734 ms     |
|     | RSA + AES 128 bit        | 572 ms     |
|     | RSA + AES 256 bit        | 776 ms     |

4. Conclusions
From the test results it can be concluded, that the speed in encryption and description of data, the combination of keycode in the application of the RSA algorithm with AES 128bit produces the fastest time, when compared with the RSA algorithm keycode combination with 3DES. For future research, it can be tested on other cryptographic algorithms, so that a combination of keycode is secure, with the best time results in the encryption and description process.

Acknowledgment
The authors would like to thank to Director and Head of Research, State Polytechnic of Malang who have supported this research project.

References
[1] Weber R H and Weber R 2010 Internet of Things Legal Perspectives (Berlin, German : Springer-Verlag)
[2] Paar C and Pelzl J 2010 Understanding Cryptography (Berlin, Jeman : Springer–Verlag)
[3] Qingxian W 2005 The application of elliptic curves cryptography in embedded systems Second International Conference on Embedded Software and Systems (ICESS’05)
[4] Rivest R L, Shamir A and Adleman L 1978 A method for obtaining digital signatures and public–key cryptosystems Communications of the ACM 21(2) 120-126
[5] Dongjiang L, Honghe C and Yandan W 2012 The research on key generation in RSA public– key cryptosystem 2012 Fourth International Conference on Computational and Information Sciences, IEEE, Chongqing, China
[6] Sadikin M A, Wardhani R W 2016 Implementation Of Rsa 2048-Bit And Aes 256-Bit With Digital Signature For Secure Electronic Health Record Application Communication & Information Technology Journal 10(2)
[7] Floissac N E and L’Hyver Y 201 From AES-128 to AES-192 and AES-256,How to Adapt Differential Fault AnalysisAttacks on KeyExpansion, 2011 Workshop on Fault Diagnosis and
Tolerance in Cryptography

[8] Rao S 2015 Performance Analysis of DES and Triple DES *International Journal of Computer Applications* **130**(14)

[9] Mathur M and Kesarwani A 2013 Comparison Between DES, 3DES, RC2, RC6, BLOWFISH and AES *Proceedings of National Conference on New Horizons in IT*

[10] Raspberry Pi *Featured Products* [Online] Retrieved from https://www.raspberrypi.org/products/

[11] Richardson L and Ruby S 2007 *RESTful Web Services* (Sebastopol, California, United States of America: O’Reilly Media, Inc.)

[12] Mahmod R 2014 An Experimental Study of Cryptography Capability using Chained Key Exchange Scheme for Embedded Devices *World Congress on Engineering 2014* I

[13] Meier R 2009 *Professional Android™ Application Development* (Indianapolis, Indiana, Canada: Wiley Publishing, Inc. Communication Technology)