International Journal of Electrical, Energy and Power System Engineering (IJEEPSE)
e-ISSN: 2654-4644
Vol. 3, No. 2, pp. 35-39, June 2020
ijeepse.ejournal.unri.ac.id

Cryptography with Layered Algorithms for Text Security on Android

Ery Safrianti*
Electrical Engineering Department
Universitas Riau
Pekanbaru, Indonesia
esafriant@eng.unri.ac.id

Fernanda Fitriansyah
Electrical Engineering Department
Universitas Riau
Pekanbaru, Indonesia
fernanda.fitriyansah@gmail.com

**corresponding author: erysafrianti, esafrianti@eng.unri.ac.id*

***Abstract* — Android phone is one of the most widely used telecommunications devices today. The exchange of various forms of information ranging from text, sound, images, and video through this media is inseparable from the threat of criminal crime through digital data theft. Data security aspects are critical to be considered, one of which is data in the form of text. Text data is commonly used in short message services (SMS), chat in various Android applications, or the use of logins and passwords. This research will create an app on android for securing text data through cryptographic techniques with a layered algorithm using three types of algorithms, namely Caesar, Blowfish, and AES Algorithms (Advanced Standard Encryption). This application can run on Android 5.0 (Lollipop) or above, which can be used to encrypt and decrypt text messages. The test results show that the decryption process can safely return the original text's that were encoded through the encryption process without the slightest mistake with the original text. The encryption test for capital letters, numbers, and punctuation can be decrypted entirely.**

Keywords— android, cryptography, layered algorithm, text.

I. INTRODUCTION

Telecommunications technology is currently experiencing a very rapid increase in all aspects of technology, such as mobile device technology, telecommunications networks, applications, and software used. In terms of mobile phone technology, types of smartphone devices, android mobile is one of the most widely used. Android phones have many features and applications for exchanging information, ranging from text via SMS (Short Message Service) to multimedia information, multiplayer games, data transfers, video streaming, and others. The security of information exchanged is also essential to avoid things that are not desirable.

Currently, various kinds of social media applications are circulating among the public to facilitate communication and interaction of one individual to another individual or one individual to most individuals at once carried out in cyberspace. The more people communicate through social media, the more opportunities for actions that can be detrimental. Such as wiretapping, piracy, leakage of information through third parties, or other crimes. These actions will cause harm to the sender or recipient.

There are several techniques used to maintain the security of information and messages. One method of securing data and words is to use encryption and description of data, which are studied in the field of cryptography. Cryptography is the science and art of maintaining the confidentiality of messages or information that can be read. The word is usually called plaintext, and the result of encryption is called ciphertext. There are two types of cryptographic algorithms, namely the classic cryptographic algorithm and the modern cryptographic algorithm. In operation, classical cryptographic algorithms work using character modes such as Hill Cipher, Vigenere Cipher, Caesar Cipher, Affine Cipher, and others. In contrast, modern cryptographic algorithms work using bit modes such as AES (Advanced Encryption Standard), Blowfish, DES (Data Encryption Standard), IDEA (International Data Encryption Algorithm), RSA (Rivest Shamir Adleman) and others.

In overcoming these problems, this research will design an Android-based application for text security using cryptographic with a layered algorithm, namely Caesar, Blowfish, and AES. This application can encode relevant text into random text that will be sent or shared through social media communication services such as WhatsApp, Line, SMS, and others to protect the information from unauthorized parties. And random information or text can still be returned to its original form using the same keywords when encoding.

II. LITERATURE REVIEW

A. Cryptography

Cryptography comes from Greek, crypto and graphia. Crypto means secret and graphia means writing. Cryptography, according to its terminology, is a science and

Received: March 20, 2020 | Revised: May 17, 2020 | Accepted: May 26, 2020

art of maintaining message security when messages are sent from one place to another. In terms of cryptography is defined as science as well as art to maintain the confidentiality of messages in the form of data or information that has meaning or value by disguising (shuffling) into an incomprehensible form using a particular algorithm [1].

The cryptographic process begins by changing the data in the form of plaintext (writing or initial message that can be read) into ciphertext (writing or secret messages that can no longer be read easily) by using an algorithm that transposes (changes position) each character / bit in the plaintext and by substituting (replacing) each character / bit in the plaintext to produce writing or data that is completely different from the initial data. The method of converting plaintext to ciphertext at the place of sender or data maker is called the Encryption Method, using an encryption key. At the data receiver or reader, the ciphertext received is then converted back into a plaintext using the Decryption Method, which reverses the position or contents of the data received in an unreadable state, returning to data that is easy to read, using a decryption key [1].

In general, based on key similarities cryptographic algorithms can be divided into two, namely symmetric algorithms and asymmetric algorithms. The symmetric algorithm is an algorithm that uses the same encryption key as the decryption key, this algorithm is also called the single-key algorithm. Examples of symmetric algorithms are the DES, AES, Rijndael, Blowfish and others. While the asymmetric algorithm is an algorithm that has its own encryption and decryption key, which use public keys and private keys. Examples of asymmetric algorithms include RSA, El Gamal and Rabin [1].

B. Caesar

The template is used to format your paper and style the text. All margins, column widths, line spaces, and text fonts are prescribed; please do not alter them. You may note peculiarities. For example, the head margin in this template measures proportionately more than is customary. This measurement and others are deliberate, using specifications that anticipate your paper as one part of the entire proceedings, and not as an independent document. Please do not revise any of the current designations.

Caesar Cipher is one of the oldest and simplest methods that is widely used. This method was discovered in the 19th century by Julius Caesar. Where the way it works to shift the plaintext is replaced with other letters according to the number of shifts that remain in the alphabetical position [2].

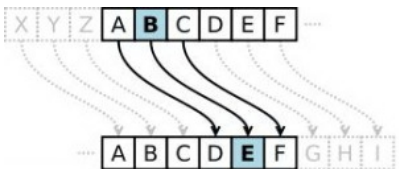

Fig 1. Illustration of shift 3 in the Caesar Cipher [2]

For example, if you want to encrypt plaintext which contains ELECTRO ENGINEERING with key 3, then the letter T is replaced by the letter W, the letter E is replaced by the letter H, the letter K is replaced by the letter N and so on. The cipher text result will contain WHNQLN HOHNWUR.

C. Blowfish

The Blowfish algorithm was created by Bruce Schneider, a Cryptanalyst and President of the Counterpane Internet Security, Inc. (a consulting firm on cryptography and computer security) and published in 1994. Created for use on computers that has large microprocessors (32-bit or more with large data caches). Blowfish is an algorithm that is not patented and is available for free for a variety of uses. Blowfish works by dividing messages into blocks of bits of equal size, that is, 64-bits with variable key lengths that encrypt data in 8 byte blocks. Messages that are not multiples of 8 bytes will be added additional bits (padding) so that the size for each block is the same [3].

Blowfish encryption is a Festal network that has 16 rounds. The input is a 64-bit (x) data element. To encrypt x, the encryption process can be done in the following way [3].

- First divide x in two 32-bit halves (XL) and (XR).
- After XL and XR continue to iterate (i) 1 to 16 then $XL = XL \oplus Pi$

  $XR = F(XL) \oplus XR$

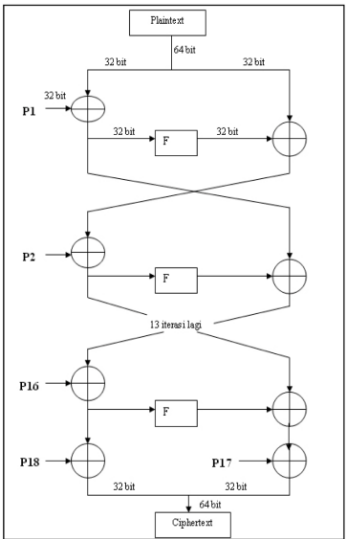

Fig 2. Block diagram of Blowfish encryption algorithm [3]

- Change XL and XR, continued from i =1 until i= 16
- Function F divided XL into four sections 8-bit: a, b, c and d, then it can be formulated
- F(XL)=((S1,a+s2,b mod 2^32)⊕S3,c)+S4,d mod 2^32
- After the 16th iteration, exchange XL and XR again to cancel the last exchange.

  $XR = XL \oplus P17$

  $XL = XL \oplus P18$

- Finally, recombine XL and XR to get the cipher text (the result of encryption). The encryption method above can also be explained in the block diagram of the Blowfish encryption algorithm, shown in Figure 2.

The decryption process has exactly the same steps as the encryption process, only the Pbox sequence is used in reverse order.

D. Advanced Encryption Standar (AES)

Advanced Encryption Standard (AES) was the winner in the search for a substitute for the DES algorithm which was considered to be no longer safe. The National Institute of Standards and Technology (NIST) has chosen the Rijndael encoding system developed by Joan Daemen and Vincent Rijment as the AES encoding system in 2000.

AES is still considered safe to use. One of the security systems AES caused by the use of large keys (128 bits, 192 bits, and 256 bits) when compared with DES systems that only use 64 bits. So the bruce attack on the AES 256 bit system has a key space of 2 ^ 256 which is a very large value.

AES is a non-Fiestel block encoding system because it uses components that always have an inverse with a 128-bit block length. AES keys can have 128, 192 and 256 bit key lengths. AES uses 5 units of data size, namely: bit, byte, word, block and state. Bits are the smallest data units, namely binary system digit values, 8-byte bytes, 4-byte (32-bit) words, 16-byte (128-bit) blocks, and state are the blocks that form 4x4-byte matrixes [1].

E. Android

Android is an operating system for cellular phones based on Linux. Android provides an open platform for developers to create their own applications so they can be used by a variety of mobile devices. Initially Google Inc. buy Android Inc. newcomers who make software for mobile phones. Then to develop Android in the form of the Open Handset Alliance which is a combination of 34 hardware, software and telecommunications companies including Google, HTC, Intel, Motorola, Qualcomm, TMobile, and Nvidia [4].

Since April 2009, the Android version has been developed with a code name named after dessert and sweets. Each version is released in alphabetical order. Here is a series of android trips [5]:

1. Android Beta (2007)
2. Android Version 1.0 Astro (2008)
3. Android Version 1.1 Bender (2009)
4. Android Version 1.5 Cupcake (2009)
5. Android Version 1.6 Donut (2009)
6. Android Version 2.0 / 2.1 Eclair (2009)
7. Android Version 2.2 Froyo (2010)
8. Android Version 2.3 Gingerbread (2010)
9. Android Version 3.0 Honeycomb (2011)
10. Android Version 4.0 ICS (2011)
11. Android Version 4.1-4.3 Jelly Bean (2013)
12. Android Version 4.4 KitKat (2013)
13. Android Version 5.0 Lollipop (2014)
14. Android Version 6.0 Marshmallow (2015)
15. Android Version 7.0 Nougat (2016)
16. Android Version 8.0 Oreo (2017)
17. Android Version 9.0 Pie (2018)

For Android security usually on a new Android device on the Sandbox media created by Google, where every time a user wants to install an application on the market, several permissions will appear that must be approved by the user before installing the application on his device.

III. METHODOLOGY

Application design method is using Android Studio software. Flow chart of design process is in Figure 3 where the general design workflow is explained. In the study of literature that is looking for and studying theories related to research. After that, proceed with preparing the software needed, here the software used is Android Studio and Android Emulator with Android operating system 5.0 or above. Next do the designer or form the desired appearance and program the display as desired. After the program is entered and finished it can be tested for text encryption and decryption. If there is an error or the desired result is not reached, the process will return when designing and reprogramming. If the desired results have been achieved then the application has been completed.

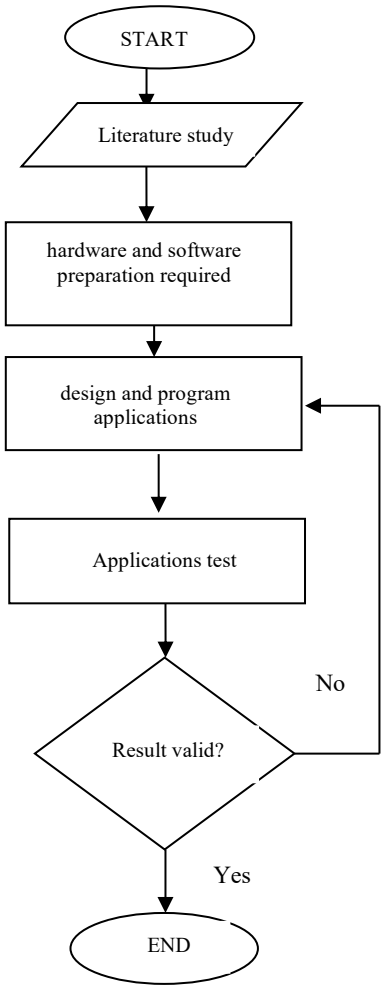

Fig 3. Flowchart of system design

Applications designed can only encrypt text messages with a caesarean algorithm, caesarean results will be encrypted again with the blowfish algorithm. And the blowfish results will be encrypted again with the AES algorithm which is the

final result of the application. To use the decryption process which is done almost the same as the decryption process, but do it in the opposite way, namely by doing an aes first, then blowfish and finally a caesarean. Caesarean results are original text messages that have not been encoded.

IV. Result and Discussion

The results of the application have 4 main views: main menu display, encryption display, decryption display and information display.

A. Main menu display

The main menu display is the initial display when the application is opened. In this main menu the user has 4 button options namely: encryption button, decryption button, information button, and exit button. In the display there are 4 button options that have functions:

- Encryption button that will call the encryption display.
- Decryption button will call the decryption view.
- Information button that will call up the information display.
- Exit button to exit the application.

B. Encryption Display

Encryption display is a display that will be called when the encryption button in the initial menu display is selected. Encryption display which is the display that will be called when the encryption button on the main menu is selected. In the encryption display the message will be processed for encryption. And in this view there are several text edits, text views and buttons that have functions:

- Two text editing entries, namely plain text input which is the text message to be encoded, key input which is the keyword for the message to be encoded.
- Text view here is the output which is the result of the encoded text message (text cipher).
- Three buttons to process messages, the encryption button here is a button to encode text messages including the encryption button has the function of making plain text input by caesarean method. Button encryption blfs has the function of making caesarean results with the blowfish method. Aes encryption button has the function of making the results of blowfish by the aes method.
- Share button to share encrypted messages through social media applications that are found on the user's smart phone.
- Copy button to copy a message that has been encoded and can be pasted again.
- Save button to save the encrypted message on the user's device in .txt format.
- Two buttons to return include the home button which will call the main menu display. Decryption button to call the decryption view.

C. Dencryption Display

Decryption view is a display that will be called when the decryption button in the initial menu display is selected. Encrypt view is a decryption view which is the display that will be called when the decryption button on the main menu is selected. In decryption view the encrypted message will be processed to be returned to its original form. And in this view there are several text edits, text views and buttons that have functions:

- Two text editing entries, namely the cipher text input which is an encrypted text message that will be returned as an original message, and the key input which is the key word for an encrypted message so that the message can be multiplied like the original message.
- Text view here is output that is the original text message (plain text) that has been returned from the encrypted message.
- Two for input, the button load that will load or open messages in the .txt form stored on the user's device. And the paste button will paste or paste the copied message.
- Three buttons to reproduce the message, the decryption button here is the button to restore the encoding of the encrypted text message, which is the AES encryption button has a function to restore the occurrence of the input cipher text with the AES method. The blfs encryption button has a function to restore the occurrence of AES results with the blowfish method. Button encryption has a function to restore the occurrence of blowfish by a caesarean method, so that it becomes an initial message that is not encrypted.
- Two buttons to return include the home button which will call the main menu display. Encryption button to call the encryption display.

D. Information Display

Information display is a display that will be called when the information button in the initial menu display is selected. Information Display is an information display which is a display that will be called when the information button on the main menu is selected. In this information display include details about the application and bio data of students who work on it.

E. Application Testing

Testing Android applications for text security using layered cryptography with a caesarean, blowfish, and AES algorithm is done by running on the android operating system and doing the encryption and decryption process. The encryption process can be done by first filling in the input from the picture we see the plain text input is "Electrical Engineering, Faculty of Engineering" and the keyword is "12345". The encryption process takes place with three layers of cryptographic algorithms namely caesarean, blowfish and AES. The caesarean process shifts plain text 3 times. The blowfis process transmits caesarean results by dividing the message bits and combining them again after mixing with a password. AES repeats the process 14 times after which the encryption results are obtained.

To start the decryption process, the text cipher message must be filled in first by typing manually, opening a saved file, or pasting a copied message. After the message is filled,

enter the same password as when encrypting. Example here the text cipher is entered by opening a file that has been saved and for the keyword is "12345". After testing the encryption results obtained in Table 1 and decryption in Table 2 follows:

TABLE 1. ENCRYPTION TEST RESULTS

Plain Texts	Keyword	Encription Result
Teknik Elektro, Fakultas Teknik	12345	ZppT0DyIG1KG0BhmsTUU5fA hckn 5z+5zP/qyuqkLIgMp2squ7qBj5y GQFiE6KwuI
aA bB cC dD eE fF gG hH iI jJ kK lL mM nN oO	abcd	bIakSC24GgX0ObxMqtpm+jRB RKsx X8KaEdmo5sJK49YmzRfJxX+V 0F+ +Opt2mePfPwRZjujSOMFtVtq+0 P46v+n5MOxiIpjQTjKuTqvAX2 U=
!@#$%^&*()_+ ~{}[]<>/?.,	++--?	61DWGhX0Y16FkCJNGqXEw5 1FFeyAG7wF+WK1AO0VA5OH vF6dXS505gXUOfcPHue8
NIM: 1307113463	1995	lYyuppOyApSBjutZzBlgJozHSqb /s0JSAzkZJDYXlFw=

TABLE 2. DECRYPTION TEST RESULTS

Cipher Text Input	Key words	Description Result	error
ZppT0DyIG1KG0BhmsT UU5fAhckn 5z+5zP/qyuqkLIgMp2squ7 qBj5yGQFiE6KwuI	12345	Teknik Elektro, Fakultas Teknik	-
bIakSC24GgX0ObxMqtp m+ jRBRKsxX8KaEdmo5sJK 49YmzRfJxX+V0F++Opt 2mePfPwRZjujSOMFtVtq +0P46v+n5MOxiIpjQTjKu TqvAX2U=	abcd	aA bB cC dD eE fF gG hH iI jJ kK lL mM nN oO	-
61DWGhX0Y16FkCJNGq XEw51FFeyAG7wF+WK 1AO0VA5OHvF6dXS505 gXUOfcPHue8	++--?	!@#$%^&* ()_+~{}[]< >/?.,	-
lYyuppOyApSBjutZzBlgJ ozHSqb/s0JSAzkZJDYXlF w=	1995	NIM: 130711346 3	-

Table 1 shows the encryption results and Table 2 shows the decryption results. Encryption is encryption and decryption is return. From these two tables it can be seen that the results of the initial text that was encoded can be safely returned to the original text as it was available without the slightest loss or lack. In the decryption process, there is no mistake, seen from the decryption of a message that has been encoded successfully returned to the same form as the original text, whether capital letters, numbers, and punctuation can be encrypted and decrypted perfectly. So after seeing these results it can be proven that the application has been running properly.

V. CONCLUSION

Android application designed text security successfully used and ran on the Android operating system 5.0 (Lollipop), and above for the version below, the app will error when installed. The encryption results test on the text security android application designed successfully encrypts three layers. It produces secret text; the decryption results test on the Android app designed text security triumphantly returns the encoded message to its original form before being encoded. The encryption on the Android security application designed text can only be decrypted with the same app; it cannot be decrypted with other applications except with the same Android Studio coding. The encryption and decryption can be done with different plaintexts, such as sharing capital letters, numbers, and punctuation that can be encrypted and decrypted without errors.

REFERENCES

[1] Basuki. A., Upik. P., Restu. H., "Perancangan Aplikasi Kriptografi Berlapis Menggunakan Algoritma Caesar, Transposisi, Vigenere, Dan Blok Chiper Berbasis Mobile", Seminar Nasional Teknologi Informasi dan Multimedia ISSN: 2302-3805, STMIK AMIKOM Yogyakarta, hal: 31-35, 2016.

[2] Putra. M.,E., " Perancangan Aplikasi Kriptografi Berlapis Menggunakan Algoritma Caesar, Transposisi, Vigenere,Dan Blok Chiper Berbasis Mobile**",** Jurnal Elektro dan Telekomunikasi Terapan, Vol. 4 No. 1, e-ISSN: 2442-4404, hal 495 – 503, 2017.

[3] Hasan. F., Indah. L., Dini. N, "Rancang Bangun Aplikasi Instant Messaging Client Terenkripsi Berbasis Android menggunakan Algoritma RSA", Jurnal Aksara Komputer Terapan Politeknik Caltex Riau Vol. 6, No. 2. Pekanbaru, hal: 30-38, 2017.

[4] Defni, Indri. R, "Enkripsi Sms (Short Message Service) Pada Telepon Selular Berbasis Android Dengan Metode Rc6", Jurnal Momentum Vol.16 No.1, Jurnal Momentum. ISSN: 1693-752X, Padang, hal: 63-73, 2014.

[5] Hendro. R. K, "Aplikasi Enkripsi Dan Dekripsi Sms Dengan Algoritma Zig Zag Cipher Pada Mobile Phone Berbasis Android", Pelita Informatika Budi Darma, Vol. x No. 3, ISSN: 2301-9425, Medan, hal: 1-6, 2015.

[6] Ariyus, D, "Pengantar Ilmu Kriptografi", Yogyakarta, Penerbit Andi, 2008.

[7] Roharjo, T., "Aplikasi Pengamanan Pesan Teks Menggunakan RC6 dan AES Berbasis Android", Universitas Mercu Buana, 2018.

[8] Ayu, T.K, "Aplikasi SMS Berbasis Android Dengan Enkripsi Vigenere Running Key", Universitas Sanata Dharma, Yogyakarta, 2014.

[9] Prasetiyo. B., Muslim. M.A., Susanto. H., "Penerapan Kriptografi Algoritma Blowfish pada Pengamanan Pesan Data Teks", Techno.COM, 16(4), 358–366, 2017.

[10] Developer. A., https://developer.android.com /studio, 2018.

Received: March 20, 2020 | Revised: May 17, 2020 | Accepted: May 26, 2020