Scientific Journal of Informatics
Vol. 5, No. 1, May 2018
p-ISSN 2407-7658 http://journal.unnes.ac.id/nju/index.php/sji e-ISSN 2460-0040

A Hybrid Security Algorithm AES and Blowfish for Authentication in Mobile Applications

Aji Purwinarko[1], Wahyu Hardyanto [2]

[1]Computer Science Departement, FMIPA, Universitas Negeri Semarang
[2]Physics Departement, FMIPA, Universitas Negeri Semarang
Email: [1] aji.purwinarko@mail.unnes.ac.id, [2]hardy@mail.unnes.ac.id

Abstract

Nowadays, everything is within our grasp and with the mobile phones become easier. Its use is not limited to calls and SMS but has become a tool that can be used to serve business transactions, banking, academic of data through mobile applications. Tus, the security of authentication in the mobile application needs to be improved to avoid a hacker attack. This article presents an authentication in the mobile application to the server using a hybrid of cryptographic algorithm Advanced Encryption Standard (AES) and Blowfish. AES and Blowfish is a symmetric key algorithm is very fast and powerful. With the utilization of a large block size of AES and Blowfish to encrypt keys, AES security will be much more robust and complicated to attacked. So, it will be difficult for hackers to perform Man in the Middle (MitM) attacks.

Keywords: AES, Blowfish, Man in the Middle attacks.

1. INTRODUCTION

Something very surprising to us that cryptography introduced thousands of years ago by the Egyptians used symbols, is believed to be the first use of cryptography [1]. Cryptography has grown, not only paper, but it has become more involved by utilizing equipment and techniques are more complicated.

Cryptography is very desirable, and data security becomes incomplete without accompanying cryptographic methods. The cryptographic method consists of two methods; one is symmetric, and another is an asymmetric process. In the symmetric key cryptography, requires the same key to encrypt and decrypt a message [2].

In this paper, we will learn the basic algorithms of common AES and Blowfish. Both are encrypted using a symmetric key algorithm using a block cipher. AES and Blowfish are the most efficient and secure algorithms [3]. The server receives the username and password had encrypted using AES and Blowfish algorithm. Applications developed using the Java Programming Language, while the recipient's server using PHP Language to perform user description and password.

2. METHODS

Cryptographic algorithms have classified as the symmetric and asymmetric method.

Symmetric

Symmetric methods such as AES and Blowfish are using a same secret key for encryption and decryption. They have the strength and fast encryption or decryption [4]. Encryption and decryption process of the symmetric method shown in Figure 1.

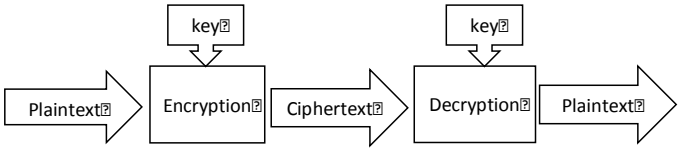


Figure 1. Symmetric Method Process

Asymmetric

Asymmetric methods use the public key for encryption and decryption need private key [4]. Everyone may know the public key; the sender's public key obtained from the receiver and use it to encrypt text into ciphertext. The receiver uses a private key to decrypt ciphertext into plaintext [1]. Encryption and decryption process of the symmetric method shown in Figure 2.

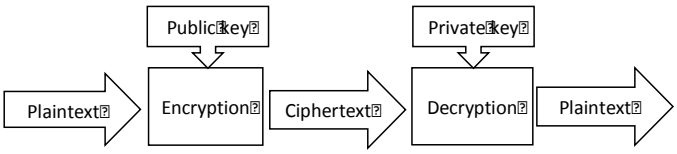
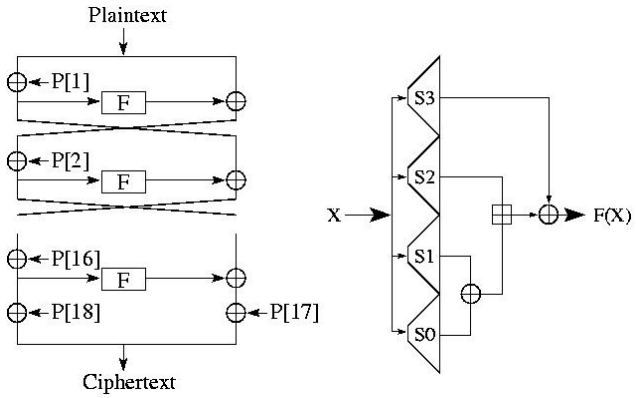


Figure 2. Asymmetric Method Process

In this paper, I will use multiple encryption algorithms, i.e. Blowfish and AES show in figure 3.

Blowfish



(source [11])

Figure 3. Blowfish Algorithm

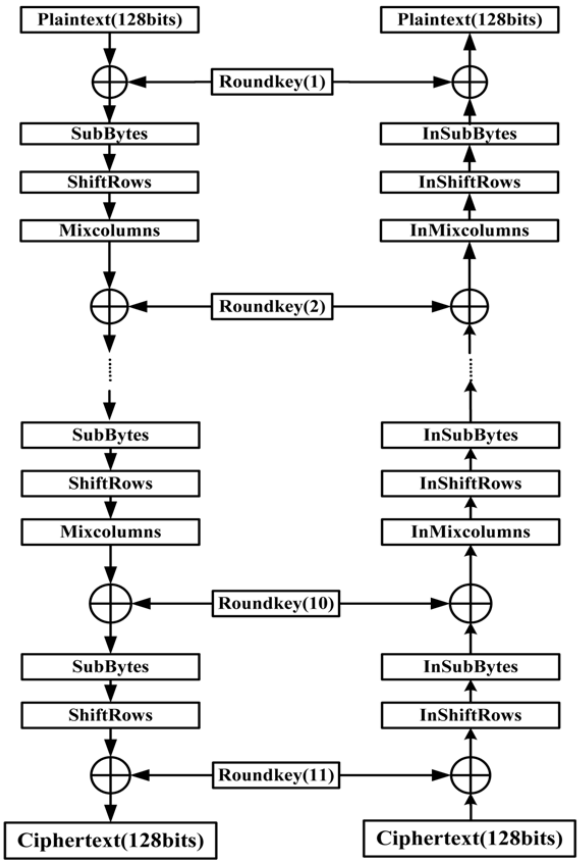
Blowfish encryption algorithm is the most efficient in processing time and power consumption compared with another symmetric algorithm [3], [9]. Blowfish algorithm was designed in 1993 by Bruce Schneier to achieve goals like 1) Speed, 2) compactness, 3) Simplicity and 4) Flexibility of key size [10]. Hardware applications can optimize Blowfish algorithm [11].

Figure 3 shows the Blowfish algorithm that consists of two parts, the key expansion and data encryption section. Extension key lock switches 448 bits into several subkey

arrays totaling 4168 bytes. Data encryption occurs via a 16-round Feistel network. Each round consists of permutations depending lock and key and the data substitution. All operations using XOR and addition on 32-bit words.

AES

Unoptimized encryption and decryption flowchart of AES show in Figure 4.



(source [7])

Figure 4. Unoptimized encryption and decryption flowchart of AES

The Advanced Encryption Standard (AES) is the United States Government's Federal Information Processing Standard for symmetric encryption, and original Rijndael algorithm to be substantially [5]. AES is a combination of robust algorithms and secure keys. This algorithm has a variable key length, such as 128, 192, and 256 resulting in a level of speed and various security [1].

Although the AES algorithm is secure, still needs to be improved using a hybrid with other algorithms, to avoid attacks the which occur due to the vulnerability of the S-box in AES algorithm [3]. AES is a symmetric block cipher with 10 rounds for 128-

bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys [6]. Figure 4 shows the flowchart unoptimized encryption and decryption of AES with 11 rounds [7].

Every round has several processing steps, which are Byte Sub, Shift Row, Mix Column and Add Round Key [8].

3. RESULT AND DISCUSSION

Author developing authentication application for evaluating two symmetric encryption techniques which are AES and Blowfish. It has been developed using a Java Programming Language by Sun Microsystems. Almost all mobile phones include this programming platform. The authentication application was created using Android Studio. The official Android IDE from Google to build Android apps.

Users enter a username and password into the application then encrypted by authentication application uses the AES algorithm with a key that has been encrypted by Blowfish algorithm to produce ciphertext. The destination server receives ciphertext; then the server performs decryption using the AES algorithm with a key that is encrypted by Blowfish algorithm. Figure 5 shows the encryption process is carried out by the application and decryption are done by the recipient server.

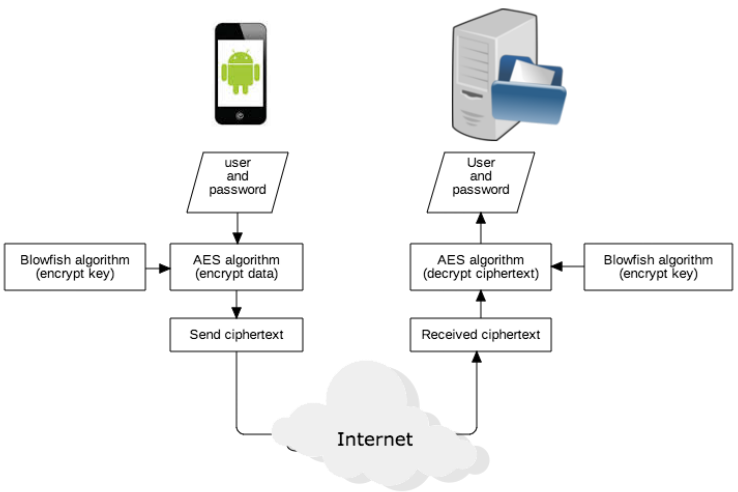


Figure 5. Encryption and decryption flowchart

4. CONCLUSION

A hybrid security algorithm AES and Blowfish for authentication implemented on Android and the receiver server. Build it in the software, and it works quickly and efficiently, even on small devices such as smartphones. With a big block size and longer keys using 128-bit blocks and with 128, 192, and 256-bit keys, AES will provide more security in the long term. A hybrid security algorithm AES and Blowfish for authentication can prevent hackers to perform Man in the Middle (MitM) attacks.

5. REFERENCES

[1] Aleisa, N. (2015). A Comparison of the 3DES and AES Encryption Standards. *International Journal of Security and Its Applications*, *9*(7), 241-246.

[2] Bansal, V. P., & Singh, S. (2015, December). A hybrid data encryption technique using rsa and blowfish for cloud computing on fpgas. In *Recent Advances in Engineering & Computational Sciences (RAECS), 2015 2nd International Conference on* (pp. 1-5). IEEE.

[3] Verma, A., Guha, P., & Mishra, S. (2016). Comparative Study of Different Cryptographic Algorithms. *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)*, *5*(2), 58-63.

[4] Yadav, R. K. (2013). Cryptography on Android Message Applications-A Review. *International Journal on Computer Science and Engineering*, *5*(5), 362.

[5] Uskov, A., Byerly, A., & Heinemann, C. (2016). Advanced Encryption Standard Analysis with Multimedia Data on Intel® AES-NI Architecture. *IJCSA*, *13*(2), 89-105.

[6] Bhanot, R., & Hans, R. (2015). A review and comparative analysis of various encryption algorithms. *International Journal of Security and Its Applications*, *9*(4), 289-306.

[7] Cai, X., Sun, R., & Liu, J. (2013, September). An ultrahigh speed AES processor method based on FPGA. In *Intelligent Networking and Collaborative Systems (INCoS), 2013 5th International Conference on* (pp. 633-636). IEEE.

[8] Cui, J., Chen, L., Zhang, Y., Xie, Z., & Zhong, H. (2014). A Secret Sharing Scheme Based on AES. *International Journal of Security and Its Applications*, *8*(6), 295-302.

[9] Mandal, P. C. (2012). Superiority of Blowfish algorithm. *International Journal of Advanced Research in Computer Science and Software Engineering*, *2*(9), 196-201.

[10] Patel, P., Patel, R., & Patel, N. (2016). Integrated ECC and Blowfish for smartphone security. *Procedia Computer Science*, *78*, 210-216.

[11] Nie, T., & Zhang, T. (2009, January). A study of DES and Blowfish encryption algorithm. In *Tencon 2009-2009 IEEE Region 10 Conference* (pp. 1-4). IEEE.