One Time Password (OTP) Based on Advanced Encrypted Standard (AES) and Linear Congruential Generator(LCG)

Imamah
Faculty of Engineering
University of Trunojoyo Madura
Bangkalan, Indonesia
i2m@trunojoyo.ac.id

***Abstract*— Security is a major issue when using internet services. Double-factor authentication is most used at this time to protect user's account. One example of double factor authentication is One Time Password (OTP). OTP is a password that is valid for only one login session. In this research OTP generated from plaintext which is a combination of username, handphone's number and access time. The Plaintext will be encrypted using Advanced Encrypted Standard (AES) and then taken 6 characters randomly using a Linear Congruential Generator (LCG). The results of this study indicate that OTP which is generated using LCG is not repetitive and the randomization is not easy to guess. This proposed method also capable to defend from sniffing attack.**

Keywords— One Time Password(OTP), Plaintext, Enkripsi, AES, LCG.

I. INTRODUCTION

Technology is growing very fast and has significant influence in the field of security. A lot of research involved with network and authentication security. One of the most widely used authentication methods is the text password. Text password is used to authenticate users to online services. Text password is a combination between characters, numbers and symbols[1].

Static password authentication is one of the simplest and most efficient authentication technologies; however, it is not highly secure because the password constantly remains the same. Static password authentication cannot resist replay attacks, password leakage, guessing attacks,or exhaustive attacks [2]. To overcome this problem, in 1981 Lamport initially proposed a one-time password (OTP) authentication scheme using hash functions [3].

One Time Password (OTP) is a security technique that used as a second layer of security. OTP password can only be used one time and with a short time limit, if not used immediately, then the password will expire and cannot be used again. This is the reason why OTP Applies to various web and Android-based systems.

One-time password authentication schemes are usually evaluated based on three aspects, i.e., simplicity, security and efficiency. Simplicity denotes how simple it is to realize the one-time password authentication scheme. Moreover, it is related to the implementation cost, and whether the scheme is easy to use. Simplicity could additionally influence the practicality of the scheme. Security involves how difficult it is for an attacker to break the scheme and obtain the private information. Efficiency describes the computational or communication cost of the scheme [5].

This study aims to develop a method for generating OTP that the evaluated is compatible with security aspects as proposed by Dongdong Zhao[5]. To increase security aspects in this research, Advanced Encrypted Standard (AES) algorithm is used for encryption and Linear Congruential Generator (LCG) is used for a method to take 6 characters randomly as the value of OTP.

II. RELATED WORK

This section provides a review of articles mainly studying application of one-time password. In 2014, Shally dan Gagangget Singh Aujla proposed a review about authentication method using OTP via SMS. In this research is not explained clearly about the comparison between the three authentication methods discussed, but it can be seen that the use of One Time Password authentication via SMS has a weakness that is the occurrence of wireless interception or Trojan mobile phone [4].

Zhao proposed OTP scheme based on the negative database(NDB) which involve a user password and random number are converted to an NDB before they are transmitted in the network. The security level of the proposed scheme is not ess than the OTP based on the encryption algorithm and one-way hash function [5].

Chang-Seop Park proposed OTP addresses the weaknesses of Lamport's OTP while preserving its advantages. In this paper, a new hash chain is designed and constructed for infinite OTP generation without a pre-shared secret between two parties (prover and verifier). Instead of a single long hash chain as in Lamport's OTP, the hash chain in the proposed OTP consists of multiple short hash chains [6].

III. PROPOSED WORK

A. Advanced Encrypted Algorithm (AES).

AES is adopted from National Institute of Standards and Technology (NIST) as a replacement for the Data Encryption Standards(DES). This is done because the key used on the DES algorithm si too short (56-bit) and so it cannot guarantee a high level of data security needed today.

The AES algorithm performs operations on 128-bit plaintext and uses identical key for encryption as well as decryption. The AES algorithm processes facts obstruct of 128-bit parts and performs 10, 12 and 14 rounds of operations employing a cipher secret of duration 128-bits, 192-bits and 256-bits respectively. The algorithm operates on data block comprised of a 4 × 4 byte matrix known as the

state. The essential procedures of AES algorithm are carried out on the state [7].

In the AES encryption process performed following four transformations nine times, namely SubBytes, ShiftRows, MixColumns, and AddRoundKey.

At the beginning of the encryption process, the input that has been copied into the state will undergo byte transformation AddRoundKey. After that, the state will undergo repeated transformations of SubBytes, ShiftRows, MixColumns, and AddRoundKey as much as Nr. [10].

a. AddRoundKey

In the encryption and decryption process, *AddRoundKey* process is the same, a *round-key* is added to the state with *XOR* operation. Each *round-key* consists of *Nb word* where each *word* will be summed with the corresponding *word* or column of state. The transforms *of AddRoundKey* in the first encryption process is set *round* = 0 for the next *round* = *round* + 1.

b. SubBytes

SubBytes is a byte transformation where every element in a state will be mapped using a substitution table (S-Box). For each byte of the *state array*, let *S[r, c] = xy*, in which case *xy* is the hexadecimal digit of *S [r, c]*, the substituted value, denoted by *S '[r, c]*, is the element in the substitution table which is the intersection of row *x* with column *y*.

c. Shiftrows

Transformation Shiftrows is basically a process of bit shift where the leftmost bit is moved to the far right bit (bit rotation).

d. Mix Column

The Mix Columns transformation operates at the column level; it transforms each column of the state to a new column.

B. *Linear Congruential Generator (LCG)*

Linear Congruential Generator (LCG) is a popular and most used method to generate random number. LCG was invented by D.H Lehmer. LCG utilizes a linear model to generate a random number defined as follows:

$$X_{n+1}=(aX_n + c) \bmod m \quad (1)$$

where *a* is the multiplier, *c* is the increment factor and m is the modulus. Parameters *a, c* and *m* have to be chosen carefully in order to avoid repetition of similar numbers before *m* [8].

The modulus m should be a large prime integer, while multiplier a must be an integer in the range 2,3,…,*m*-1. The cycle length of LCG would never exceed the modulus *m*, but it could be maximized using the three following conditions [8]:

a. *c* is relatively prime to modulus m;
b. Multiplier *a*-1 is a multiple of every dividing modulus *m*;
c. Multiplier *a*-1 is multiple of four when the modulus *m* is a multiple of four too.

C. *OTP based on AES*

The first step of OTP technology is OTP calculation, which is the algorithm to generate a unique passcode for every authentication[9]. In this study, unique passcode or OTP is generated based on Fig 1.

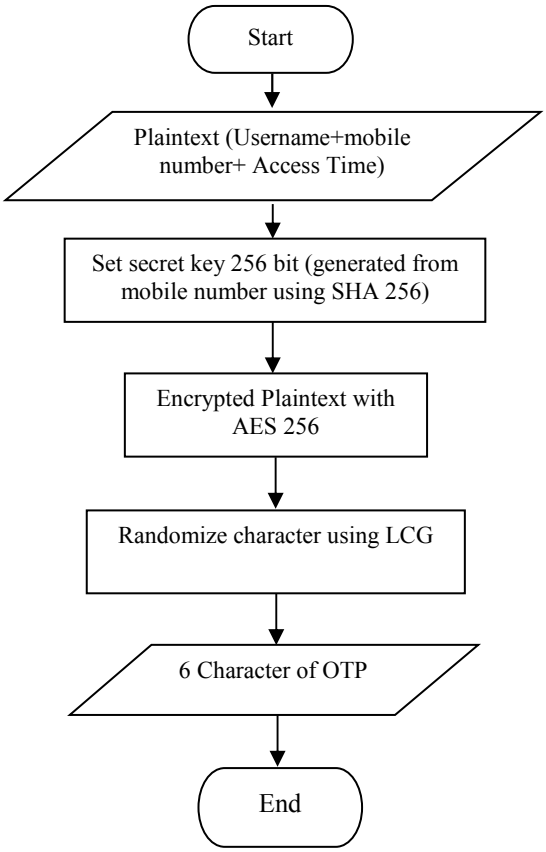

Fig. 1. Flowchart of Proposed Method.

The process of generating OTP is shown in fig 1 and design as follows:

a. Plaintext is a combine of usernames, mobile's number and access time.
b. Plaintext will be encrypted using the AES algorithm.
c. The secret key for AES 256 should be 32 characters or 256 bits. It is generated from mobile's number using SHA256.
d. The encryption result, then randomized by using LCG, which is 6 characters used as OTP.

The OTP will be sent automatically to the user's mobile phone when the user clicks the login button. The user will input the OTP code on the provided page. If the code is valid, the user will be direct to a homepage, but if the code is invalid, the user will be back to the login page, and OTP will be re-generated and sent back to user's mobile phone.

IV. RESULT AND DISCUSSION

Based on the algorithm in fig 1, this research is performed to prove that OTP generated randomly and not predictable. This evaluated will be the answer, as this research compatible in security aspects as Dongdong Zhao[5] proposed or not. The differences in access time made the

plaintext is different so that it produces a different value of OTP. Table 1 shows the generated of OTP from one user who has different in access time.

TABLE I. OTP RESULTS USING AES + LCG

No	Plaintext	OTP (AES+LCG)
1	i2munix@gmail.com081937106931 2018-07-28 05:59:12	Veu0Le
2	i2munix@gmail.com081937106931 2018-07-28 06:02:03	cWPHOe
3	i2munix@gmail.com081937106931 2018-07-28 06:02:29	h2N7/7
4	i2munix@gmail.com081937106931 2018-07-28 06:03:02	va7gOh
5	i2munix@gmail.com081937106931 2018-07-28 06:03:22	YuxOrc
6	i2munix@gmail.com081937106931 2018-07-28 06:03:41	WPKhC5
7	i2munix@gmail.com081937106931 2018-07-28 06:04:03	5Pe59W
8	i2munix@gmail.com081937106931 2018-07-28 06:04:32	ROPhti
9	i2munix@gmail.com081937106931 2018-07-28 06:05:04	3HcePf
10	i2munix@gmail.com081937106931 2018-07-28 06:05:34	nBke5n

LCG has a possibility to generate repeating random values. To overcome this problem, access time has been added to the plaintext. Table 1 shows that adding access time will produce dynamic plaintext, which means that OTP results will also be dynamic and difficult to guess.

A. *Sniffing Attack*

Sniffing attack are performed to ensure that OTP is safe to apply. This Testing uses user data which performs as follows, Username *i2munix@gmail.com*, mobile's number is *081937106931*, and access time is *2018-07-28 05:59:12*.
The result of OTP which is generated from account above is **Veu0Le**. In this test, we set the OTP validation time is 30 seconds.
This test uses an infrastructure network with one computer web server, one laptop as a user computer, one computer as a sniffer, one handphone as a user mobile. The three computers are connected in the localhost.
The user opens a web-based system and trying to authenticate on the computer users. While at the same time sniffer monitor by using Wireshark and got the result as in Fig 2. While the OTP code of the user obtained by sniffer can be seen in Fig 3.

Fig. 2. Username and Password of the user that obtained by using Wireshark.

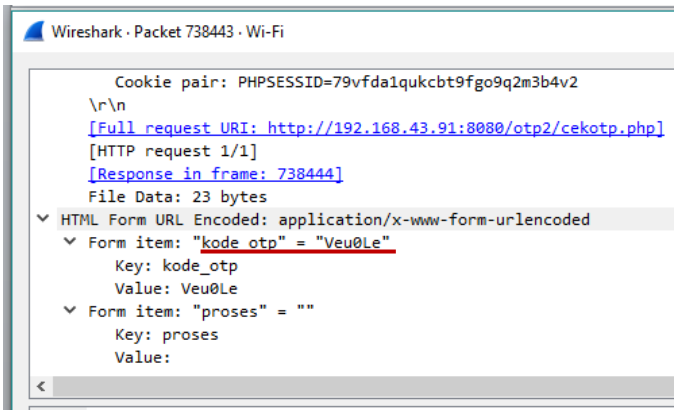

Fig. 3. The user's OTP code that obtained by using Wireshark.

When the sniffer gets the username, password and OTP code, then the sniffer accesses the login page. Notice Fig 4.

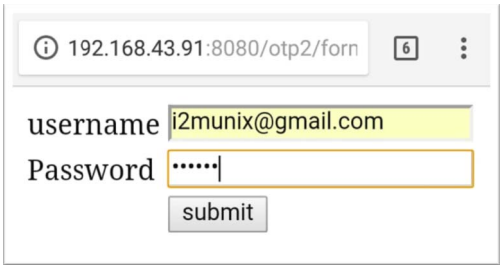

Fig. 4. Login Page

The sniffer enters the username and password, the system checks whether the username has actually been registered or not. If it is registered, then the user should enter the OTP code, notice fig 5.

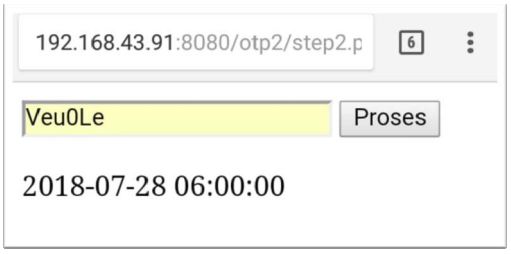

Fig. 5. Web page of OTP's code.

Fig 5 shows the code and time on the system that the sniffer tries to login. The OTP code entered on the same day is 2018-07-29 06:00:00 which is means 48 seconds later after user access time. The access time made by the actual user is 2018-07-29 05:59:12. we show in fig 6 that login is failed because in this test the valid time for OTP is only 30 seconds.

Fig. 6. Login is failed because OTP is expired.

V. CONCLUSION

LCG has advantages in its speed because it requires little bit operations but the random numbers easily predictable so as not cryptographically secure. In addition, LCG is also possible to generate repeated randomness within a certain period. However, with the proposed method, the weakness of LCG in generating random numbers can be overcome by creating dynamically plaintext that generated based on user access time.

OTP generated in this research has successfully passed the sniffing attack. Sniffing is the technique for monitoring and catching all packets passing through the network. The proposed OTP is able to cope with sniffing due to OTP term restrictions. In this test, the OTP validity period is set to 30 seconds, if the OTP is obtained by sniffer after 30 seconds since it was sent to the user's mobile, the sniffer will fail to access user's account and failed to login.

The proposed scheme is compatible in security aspects, it's proved by this research can perform OTP that randomly and not predictable and also passed the sniffing attack.

References

[1] I. Imamah, A. Djunaidy and a. et, "Comparasion of Password Generator between Coupled Linear," in *IOP Conf. Series: Journal of Physics: Conf. Series 953* , Bali, 2017.

[2] D. Zhao and W. Luo, "One-time password authentication scheme based on the negative database," *Engineering Applications of Artificial Intelligence,* vol. 62, pp. 396-404, 2017.

[3] L. Lamport, "Password Authentication With Insecure Communication," *Commun ACM ,* vol. 24, no. 11, pp. 770-772, 1981.

[4] Shally and S. G. Aujla, "A Review of One Time Password Mobile Verification," *International Journal of Computer Science Engineering,* vol. 4, no. 3, pp. 113-118, 2014.

[5] D. &. L. W. Zhao, "One-Time Password Authentication Scheme Based on The Negative Database," *Engineering Applications of Artificial Intellegence,* pp. 396-404, 2017.

[6] C.-S. Park, "One-Time Password based on Hash Chain without Shared Secret and Re-Registration," *Computers & Security,* vol. 75, pp. 138-146, 2018.

[7] H. Zodpe and A. Sapkal, "An Efficient AES Implementation using FPGA with Enhanced Security Features," *Journal of King Saud University - Engineering Sciences,* 2018.

[8] A. E. T. Tchendjeu, . R. Tchitnga and H. B. Fotsin, "FPGA Implementation of Linear Congruential Generator Based on Block Reduction Technique," *Journal of Circuits, Systems and Computers,* vol. 27, no. 10, 2018.

[9] Y. Huang, Z. Huang, H. Zhao and X. Lai, "A new One-time Password Method," in *IERI Procedia*, 2013.

[10] I. Imamah, A. Djunaidy and M. Husni, "Penerapan AES untuk Otentikasi Akses Cloud Computing," *Jurnal Ilmiah Simantec,* vol. 4, pp. 27-34, 2014.