MODIFICATION AFFINE CIPHERS ALGORITHM FOR CRYPTOGRAPHY PASSWORD

Article · April 2017

CITATIONS
3

READS
5,897

1 author:

Ajay Babu Sriramoju
RANDSTAD Technologies, USA
14 PUBLICATIONS **46** CITATIONS

SEE PROFILE

International Journal of Research In Science & Engineering e-ISSN: 2394-8299
Volume: 3 Issue: 2 March-April 2017 p-ISSN: 2394-8280

MODIFICATION AFFINE CIPHERS ALGORITHM FOR CRYPTOGRAPHY PASSWORD

Sriramoju Ajay Babu
[1]*Programmer Analyst , Randstad Technologies, EQT Plaza 625 Liberty Avenue, Suite 1020 Pittsburgh, Pennsylvania -15222, USA.*

ABSTRACT

Computers as a means of storing and transmitting data, information, and confidential documents are important and can often be easily accessed by people who are not responsible. Security and confidentiality of data on computer networks today become a very important issue and continues to grow. Some of the cases relating to computer network security today become a job that requires handling fee and security has been tremendous. Vital systems such as defense systems, banking systems and systems of many users (multi-user) requires such a high level of security. This study aims to build a prototype of data security (cryptography) for passwords using a modified method of affine ciphers. Model analysis of cryptographic needs this password using State Transition Diagram (STD).

Keyword: Cryptography, Passwords, Affine Ciphers, State Transition Diagrams

---

1. INTRODUCTION

Computers as a means of storing and transmitting data, information, and confidential documents are important and can often be easily accessed by people who are not responsible. Kris (2003) states that the security and confidentiality of data on computer networks today become a very important issue and continues to grow. Some of the cases relating to computer network security today become a job that requires handling fee and security has been tremendous. Vital systems such as defense systems, banking systems and systems of many users (multi-user) requires such a high level of security. Advances in computer networking with the concept of open system will provide the opportunity and the opportunity to access these vital areas. Therefore, data, information, and documents for delivery or data storage security needs to be done.

Wirdasari (2008) states that cryptography is a means to secure data, information, and documents by means of encoding it into a form that can not be understood more meaning. This data security can be applied into two forms, namely: (1) sending data through communication channels (data encryption) and (2) of data storage in disk storage (data encryption at rest).

One interesting phenomenon to be studied is the number of events that occur on a computer system many users (multi-user) which data, information, and documents can be easily accessed by unauthenticated users. Ibisa (2011) states that in order to avoid that the user is not interested or do not have the authority to access the system, this access must be controlled trials with using a password. The phenomenon described above will be overcome by creating a password that is difficult to be opened by using the principles of cryptography.

Cryptographic system for passwords can be built using a modified method of affine ciphers efficient and effective way to secure data, information, and documents. The application of the modification method of affine ciphers cryptosystems cryptography to applications in a password is needed to make the computer cannot be opened by pirates primarily by other users who do not have access rights (Septiarini and Hamdani, 2011). This study aims to build data security (cryptography) for passwords using a modified method of affine ciphers.

2. THEORIES

The word cryptography (Cryptography) come from the Greek word meaning hidden Kryptos and graphein which means writing. Cryptography can be interpreted as the writing of confidential or can be interpreted also as a science or art to learn how a data, information, and documents are converted to forms particularly hard to understand (Luciano and Prichett, 1987; Menezes, 1996 in Munir, 2006; Schneier, 1996 in Munir, 2006; Munir, 2006; Wirdasari 2008; Septiarini and Hamdani, 2011; Abraham and Shefiu, 2012). Cryptography aims to maintain the confidentiality of data, information, and documents that can not be known by a person not entitled to it (unauthorized person). Herryawan (2010) states there are various systems that the intended use of passwords and different levels of confidentiality in accordance with user requests, but in practice the user wants conveniences such as: confidentiality Data, speed, accuracy, and cost. An encoded data called plaintext or cleartext while the data was encrypted called ciphertext. The process is performed to convert plaintext into ciphertext is called encryption (encryption) or Encipherment while the process of turning ciphertext back into plaintext is called decryption (decryption) or decipherment (ISO 7498-2). Cryptographic parameters required for the conversion process that is controlled by a key or multiple keys.

Cryptography has now become one of the important conditions in the security of information technology, especially in the delivery of secret messages. Secret message delivery is very vulnerable to attacks carried out by a third party, such as wiretapping, disconnection of communication, changing the message sent, and others. Cryptography can improve security in sending messages or communications data by encrypting messages are based on certain algorithms and key known only to the parties entitled to the data, information, and documents.

A. The purpose Cryptography

Cryptography is a method that can be used to secure the message. Therefore, the purpose of cryptography in securing messages can be divided into three parts, namely:

a. The validity of the sender (user authentication) with regard to the authenticity of the sender can be expressed in a question "Is the received message actually came from the sender's real?"
b. The authenticity of the message (message authentication) relating to the integrity of the message (data integrity) that can be expressed in a question "Is the message received is not experiencing the changes (modifications)?"
c. Nonrepudiation, where the sender cannot deny (lie) that it was he who sent the message

B. Cipher and Key

Kris (2003) and Munir (2006) states that the cryptographic algorithm called a cipher which can be interpreted as a rule for encryption and decryption. Understanding cipher can

also be expressed as a mathematical function that is used to perform encryption and decryption. The concept of a cryptographic algorithm is a mathematical relationship between two sets consisting of elements of plaintext and ciphertext elements. Encryption and decryption is a function that will map the elements of the two sets. If P is the plaintext and C is the ciphertext, then the encryption function E which maps P to cipher C are as follows:

$$E(P) = C$$

While the decryption function D mapping cipher C into the plaintext P can be written as follows:

$$D(C) = P$$

The encryption process becomes decryption where will be performed in order returns the message to the original message then the above equation would be the following equation:

$$D(E(P)) = P$$

Modern Cryptography can be overcome algorithm security by using his key to unclassified, but the key must be kept confidential. Munir (2006) stated that the key (key) is a parameter that is used to transform the encryption and decryption, and mathematically can be written as follows:

$$EK(P) = C \text{ and } DK(C) = P$$

Equation can meet if the equation can be formulated as follows:

$$DK(EK(P)) = P$$

C. Affine Cipher

According to Munir (2006), Affine cipher is an extension of the Caesar cipher, which multiplies the plaintext with a value and add a shift. Mathematically encryption of plaintext P to produce ciphertext C can be expressed by congruent functions as follows:

$$E(P) = (ax + b) \bmod m$$

Where:
n = size of alphabet
a = integer that must be relatively prime to m (If not relatively prime, then the decryption is not biased do)
b = the number of shifts (Caesar cipher is the specialty of affine cipher with m = 1)
x = plaintext is converted to an integer from 0 to m-1 in the order of the alphabet
E (P) = ciphertext is converted to an integer from 0 to m-1 in accordance with the order of the alphabet.

While the decryption function can be written using the following equation:

$D(x) = a^{-1}(x - b) \bmod m$ where a-1 is the multiplicative inverse a modulus m to meet the following equation:

$1 = aa^{-1} \bmod m$ a multiplicative inverse exists only if a and m are coprime. If not then the process the algorithm stops. Decryption function is the inverse of the encryption function that can be written as follows:

$D(E(P)) = a^{-1}(E(P) - b) \bmod m$

$= a^{-1}(((ax + b) \bmod m) - b) \bmod m$

$= a^{-1}(ax + b - b) \bmod m$

$= a^{-1}ax \bmod m$

$D(E(x)) = x \bmod m$

D. Modification Affine Cipher

Modifications affine cipher is a cryptographic models such as affine cipher same provisions as described in the previous section. However, the model that will be developed is the inverse of the affine cipher in which letters and numbers as the final plaintext into ciphertext password will be the beginning. Normally password can consist of alphabets and numbers then the description of the alphabet A to Z and the numbers 0 through 9 with the corresponding values as shown in Table 4. A limited value because coprime with a possible 36 so that the value of one of 1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31 and 35.

3. RESULT AND DISCUSSION

The example of the testing process modification affine cipher algorithm looks as the follows:
Encryption for passwords: AFC25W using a modified method of affine cipher produce "UL0YJK", as shown in Table 1.

TABLE 1
Encryption "AFC25W" with modification Affine Cipher

Plaintext	A	F	C	2	5	W
Mod. Plaintext	W	5	2	C	F	A
X	22	31	28	2	5	0
7x + 10	164	227	206	24	45	10
(7x + 10) mod 36	20	11	26	24	9	10
Ciphertext	U	L	0	Y	J	K

Decryption functions written as follows: D (y) = 31 (y - 10) mod 36 where a-1 is the result of the calculation is 31, b is 10, and m is 36. Decryption of ciphertext "UL0YJK" generate password origin "AFC25W" as shown in Table 2.

TABLE 2
Decryption "UL0YJK" with modification Affine Cipher

Ciphertext	U	L	0	Y	J	K
Mod Ciphertext	K	J	Y	0	L	U
y	10	9	24	26	11	20
31(y- 10)	0	-31	434	496	31	310
31(y- 10) mod 36	0	5	2	28	31	22
Plaintext	A	F	C	2	5	W

4. CONCLUSION

Based on the research development of cryptographic software can be summarized that prototype cryptographic password has been constructed using analysis method State Transition Diagram (STD), cryptography password is encrypted and decrypted using a modified method of affine cipher. Character password that can be encrypted and decrypted ie original alphabet and numbers and also cryptography is a software password to encrypt and decrypt a password that can not be read by unauthorized people though to look at the source code program, for testing cryptographic password using a test case with a black box

technique that shows that a functional prototype of the software is correct. This test does not include alpha and beta testing.

REFERENCES

1. Abraham, O. dan Shefiu, G.O. 2012. An Improved Caesar Cipher (ICC) Algorithm, International Journal of Engineering Science & Advanced Technology, Volume 2, Issue-5.: 1199-1202
2. Ariwibowo, E. 2008. Aplikasi Pengamanan Dokumen Office dengan Algoritma Kriptografi Kunci Asimetri Elgamal, Jurnal Informatika, Vol 2 No. 2.
3. Dey, S. 2012. SD-AREE : A New Modified Caesar Cipher Cryptographic Method Along with Bit-Manipulation to Exclude Repetition from a Message to be Encrypted, Department of Computer Science St. Xavier's College [Autonomous] Kolkata, West Bengal, India.
4. Goyal, D dan Srivastava, V. 2012. RDA Algoritm: Symmeric Key Algoritm, International Journal of Information and Communication Technology Research, Volume 2 No. 4.
5. Hadi, A. 2011. Rancang Bangun Sistem Pengamanan Dokumen pada Sistem Informasi Akademik Menggunakan Digital Signature dengan Algoritma Kurva Eliptik, ISO 7498-2 : Security Architecture of OSI Reference Model.
6. Pressman, R.S. 1997. Software Engineering a Practitioner's Approach, 4th edition, McGraw-Hill International Editions, New York
7. Rahayu, T. P, Yakub, dan Limiady, I. 2012. Aplikasi Enkripsi Pesan Teks (SMS) pada Perangkat Handphone dengan Algoritma Caesar Cipher, Seminar Nasional Teknologi Informasi dan Komunikasi (SENTIKA) Yogyakarta.
8. Saroha, V, Mor, S dan Dagar, A. 2012. Enhancing Security of Caeser Cipher by Double Columnar Transposition Method, International Journal of Advanced Research Computer Science and Software Engineering, Volume 2, Issue 10.
9. Septiarini, A dan Hamdani. 2011. Sistem Kriptografi untuk Text Message Menggunakan Metode Affine, Jurnal Informatika Mulawarman, Vol 6 No. 1.
10. Singh, A, Nandal, A dan Malik, S. 2012. Impementation of Caeser Cipher with Rail Fence for Enhancing Data Security, International Journal of Advanced Research Computer Science andSoftware Engineering, Volume 2, Issue 12.
11. Srikantaswamy, S. G dan Phaneendra, H. D. 2012. Improved Caesar Cipher with Random Number Generation Technique and Multistage Encryption, International Journal on Cryptography and Information Security (IJCIS), Vol 2 No. 4.
12. Bhoyar, Mayur Ramkrushna. "Home automation system via internet using Android phone." InternationalJournal of Research in Science and Engineering. CSE Department, JDIET, Yavatmal: 6.
13. Maulana, Bagoes, and Robbi Rahim. "GO-BACK-N ARQ APPROACH FOR IDENTIFICATION AND REPAIRING FRAME IN TRANSMISSION DATA."
14. Nofriansyah, Dicky, and Robbi Rahim. "COMBINATION OF PIXEL VALUE DIFFERENCING ALGORITHM WITH CAESAR ALGORITHM FOR STEGANOGRAPHY."
15. Sriramoju Ajay, B. (2017). INTELLIGENT MOBILE APP FOR FINDING PATH AND TRACKING POST PACKETS USING ANDROID PLATFORM. International Journal Of Research In Science & Engineering, 3(2), 9. Retrieved from http://ijrise.org/home
16. Sriramoju Ajay, B. (2017). Investigation of Feasible Tourist Destinations using Android Mobile App. International Journal Of Research In Science & Engineering, 3(2), 9. Retrieved from http://ijrise.org/home

17. Babu, Sriramoju Ajay, and Namavaram Vijay. "Image Tag Ranking for Efficient Matching and Retrieval." (2016).
18. Babu, Sriramoju Ajay, and Namavaram Vijay. "Design and Implementation of a Framework for Image Search Reranking." (2016).
19. Babu, Sriramoju Ajay, and S. Shoban Babu. "International Journal of Research and Applications Jan-Mar© 2016 Transactions 3 (9): 422-426 eISSN: 2349–0020."