توليد مفتاح سري مع سهولة حفظه وتذكره

Generating a suitable secret key with faciliting its saving and remembering

أ.م. د. صالح نعمان عبدالله العسلي[1]

Dr. Saleh Noman Abdulla Alassali [2]

https://doi.org/10.54582/TSJ.2.2.23

(1) أستاذ مشارك في قسم علوم الحاسوب : جامعة إقليم سبأ: مأرب

عنوان المراسلة : :sano201023@gmail.com

(2) Dept. Computer Science, University of Saba Region, Marib, Yemen

الملخص :

تعتمد حماية المعلومات على الحماية المنطقية، والحماية المنطقية بدورها تعتمد على كلمة سر أو مفتاح سري مناسب، أي غير قابل للتخمين، وهذا يتطلب طول مناسب، وأيضا مكونات مناسبة. ولكن تواجه مشكلة وهي في كيفية تكوين وأيضا نسيان المفتاح السري المناسب.

هذا البحث يقترح فكرة لتوليد مفتاح سري مناسب مع سهولة حفظه وتذكره، وتقوم الفكرة على توليد رموز مختلفة عددها اكثر من ضعف العدد المطلوب ثم يتم اختيار العدد المناسب من تلك الرموز، ثم يتم تقسيم تلك الرموز الى مجموعات، كل مجموعة تتكون من ٤ رموز، ويتم اسناد اسم معين لكل مجموعة، ثم يتم اسناد كل مجموعة الى اصبع من أصابع اليدين، ويتم تحديد نقطة بداية من احدى الأصابع، ثم يتم تحديد اتجاه معين للوصول من نقطة البداية الى نقطة النهاية، فيكون المفتاح السري هو مجموعة الرموز الموجودة بين نقطة البداية وبين نقطة النهاية عند اتخاذ نفس المسار المحدد مسبقا، وبالتالي يسهل تذكره.

الكلمات المفتاحية:

الكتابة المشفرة – التشفير – فك التشفير – متماثل – غير متماثل – المفتاح السري – الخصوصية – التوثيق.

https://doi.org/10.54582/TSJ.2.2.23

Abstract

Nowadays, most people use cryptography to deal with sensitive information either during storing or during communication. Dealing with cryptography requires secret or privet keys. But some of users use unsuitable secret keys. They use either short, or weak keys. The short and weak keys are easy to be remembered. The risk of using weak or short keys is that the weak key can be guessed and the short key can be broken easily. In cryptography, it is known that the security produced are directly proportional to the quality and the length of the used secret keys. On security rules, secret key should not be saved or written in any file or written, because it weakens the associated security. This paper suggests a method to remember a long secret key easily by assigning a suitable name to each finger of the two hands, selecting start and end points, selecting predefined path, and finger sequence. The collection of symbols to the finger-names between the start and end points at the predefined path is the secret key.

Keywords: cryptography , encryption/decryption, Symmetric, Asymmetric, private-key Confidentiality, authentication

https://doi.org/10.54582/TSJ.2.2.23

I. Introduction

In computer environment, cryptography is an effective tool to hide the sensitive information and identity-authentication. Encryption/decryption techniques can be used to convert readable information to unreadable information and vice versa. The security produced by any encryption/decryption technique is directly proportional to the quality and the length of the used secret key. If a user uses Advance Encryption Standard(AES) algorithm of 256-bits for encrypting/decrypting his/her sensitive data/information, that means the secret key consisted of 32 symbols, should be used, the user may forget this long secret key. [1],[2]

Problem statement

Indeed, one problem may arise of using long secret key. How does user memorize a suitable secret key for long time? The user may be obliged to write the secret key. Short or weak keys are easy to be remembered, but long or strong keys are not easy to be remembered. Writing a secret key in any place, or saving it in any file, weakens the security produced by that key. [1],[2],[3],[4]

Objectives

To generate specific secret key.

To remember this secret key easily.

Approach

This paper suggests a method to generate and to remember a long secret key by assigning a suitable name to each finger of his/her two hands, selecting start and end points, and selecting predefined finger's sequence that covers all fingers. The secret key will be the collection of symbols to the finger-names at the same predefined sequence.

This paper is organized as follows: the related works is discussed in Section II. The suggested method is explained in Section III, Implementation is in Section IV, and Conclusion is in Section V.

II. Related Work

This section gives a brief description to the information confidentiality using cryptography and the concept of identity authentication.

II.1 Logical security

All information and systems inside computer are secured by the logical security. Logical security consists of several tools like access control, privileges and encryption/decryption. Any computer is built in access control system. Access control system may use compound of user-name and password to prevent unauthorized user from login to the computer or to unauthorized account. So, access control system requires opening account to every user to be able to login the computer. Any account needs requirements, like user-name, password, suitable privileges, and so on. All account's requirements should be saved in the database system during the opening of the account. Also every account is granted privileges according to the associated role or the tasks related to that account. Indeed, access control system is important part of logical security. [3],[4],[5]

The password is a set of characters and numbers in which the user identifies himself. The secret key is a set of characters and numbers on which the cipher operates.

In general, any type of logical security depends on the following:

1. Symbols randomization and
2. Symbols number

Actually, most computer systems and information are secured by the password or secret keys. The security produced is directly proportional to the quantity of the symbols, and the accuracy of the randomization of that symbols' used as a password or a secret key' along with the associated algorithm. But these type of securities are not sufficient, especially for sensitive data/information. May users left their screens opened, for some moments, beside his/her partners, in their organization while he/she is doing other works, making sensitive data/information at risk. [2], [3]

II.1.1 Encryption/ decryption

Encryption is the process of transforming plaintext into ciphertext. Decryption is the process of transforming ciphertext into plaintext. In practice, there are two types of cryptosystem: a symmetric and an asymmetric cryptosystem. A symmetric cryptosystem is one that uses only one key for encryption and decryption. An asymmetric cryptosystem is one that uses one key called public-key for encryption and another key called private-key for decryption. In a symmetric-key cipher, the same key is used by both the sender and the receiver. The used key is called the secret key. In an asymmetric-key cipher, a pair of keys are used. The sender uses the public-key, the receiver uses the private-key or vice versa. [1],[3],[4]

II.1.2 Data/information confidentiality

Data/information confidentiality refers to protection against unauthorized data access. Confidentiality is the protection of transmitted or stored data/information from passive attack. Confidentiality ensures that the data/information in a computer system or transmitted are read only by authorized parties. So cryptography can be used efficiently to fulfill information confidentiality.

Data/information confidentiality depends on cryptograph which in turn depends on the algorithm used and the secret key. In general, the algorithms of cryptograph are usually known, but the keys should be kept secret. So the security gained based on the randomization of the content of the secret construction, the length of the secret keys. [3],[4],[5],[6]

II.2 **Authentication**

Authentication is the process of proving that a subject is what the subject claims to be. Authentication is a measure used to verify the eligibility of a subject an assurance of the identity of the person or machine, the ability of that subject to access certain data/information. Authentication stops masquerading impostors. The process of authentication actually depends on the application: Sometimes it is needed to insure that the delivered message/document is as it was in the source i.e. without any modification. In this case the authentication process only should be applied on the message/document itself. In other words, no need for verification on the source. Such as these situations, it is better to use either CRC or Message Digest methods, depending on the situation, because they are faster and more economic than using Public-key algorithm. But when verification on the source and the document are required alike we are resorted to use public-key algorithm. [2],[3],[4]

The access control system uses user-name and password as an authentication tools to allow/prevent user from login to the user's account.

II.3 Weakness may be associated with secret keys

Cryptography is effective tool to hide sensitive information, using suitable algorithm and suitable secret key. Most algorithms that are being used in cryptography, were studied and analysed by many specialists, so the probability of the found defects in the algorithm are very small. But using short or weak secret key, vulnerable to brute force or guessing attacks. Suitable secret key means difficult to be guessed, and long enough, i.e. contains very large space-key which has immunity against brute force attack. [1],[5]

II.3.1 Brute force attack

Brute force in its simple definition is a way in which the cryptanalyst tries to cover all the key-space to extract the plaintext from the associated cipher-text. Short-key means that little key-space. So the brute force is a suitable way with the short-keys. [3],[4],[5],[6]

II.3.2 The security gained by the secret key length

The security gained by the length of the keys based on the key spaces. The produced security is directly proportional to the key spaces, if the key spaces are not sufficient, there is a weakness in security gained. But there is a limitation to the length of the secret key that the user can be able to memorize the selected key symbols.

In many situations, someone can impersonate an account of another user, in the same organization and may access right of the that user, by exploiting inadvertency of that user and steals some files which contain sensitive information and exploiting available algorithms and the high computations powers to break the secret key. That may be done by covering all the probabilities of existing secret key symbols. Indeed, any secret key consists of set of symbols which exist in the ordinary keyboard, that is around 100 symbols. [6],[7]

If the user selects 15 symbols, from ordinary keyboard to be used as a secret key, because of long secret key cannot be remembered easily. Then the corresponding secret key-space is around 100^{15} . Nowadays, the high computations powers can exhaust 100^{15} and cover all the probabilities of existing secret key symbols, especially in decryption. In decryption process, the row material of encrypted information will be available to the opponents, and the opponents may use the brought force methods to retrieve the encrypted information. Also the opponents can exploit the available algorithms found in the net and the high computations powers found in the net also, to cover all the probabilities of existing secret keys within short period. So short secret key is not sufficient, and not applicable to the recent algorithms like AES, or SHA-256 bits, that require 32 symbols= 256-bits. [6],[7],[8],[9]

II.3.3 Guessing attack

Weak-key vulnerable to guessing attack, weak-key, like 101010...... sequence of ones and zeros, or ababab.... or something like that, or any strings have meaning vulnerable to guessing attacks. For example this key "qwertyuiop[asdfghjkl" is very weak, it consisted of 20 characters, but this symbols corresponding to the 2nd and 3th rows of the keyboard. But in many cases, the cryptanalyst tries to guess the secret key using dictionary words or some other technics. [8],[9],[10]

Indeed, cryptanalyst uses several types of attacks through which reduce the total cost of breaking the cipher-text. Cryptanalyst will try to use the behaviour conduct and the curriculum vitae of the user to guess the secret key and retrieve secret information. [2],[7],[9],[10]

III. Description of the suggested method

This section gives a description to the suggested method which reduces the number of symbols used to construct suitable keys at the user. One way hash function is used to generate the required symmetric keys. The following subsections describe generating suitable key in the suggested method.

One way hash function accepts tow inputs 1: an arbitrary length file text, and 2: a secret key. The output from the one way hash function is of a fixed-length hash value, called Message Digest code corresponds to the inputs. If one character, or one bit is changed in the inputs, the output Message Digest Code will be changed correspond to that inputs changes.

III.1 Generating suitable secret key

To overcome the problem associated with remembering long strong secret key, the suggested method is as follow:

1. Generating randomly suitable number of symbols, greater than the required actual key.
2. Dividing the generated symbols into n groups, n> 10, each group consists of only 4 symbols.
3. Assigning one group to one finger, the name of the finger is the name of the first symbol in the group. Repeat this step 10 times to cover all the hands fingers.
4. Selecting start and end points on two fingers.
5. Selecting a suitable path to go from the start point to the end point. The secret key will be the concatenation of the symbols from the start to the end points.

Steps description

The following steps describe the processes of generating suitable user secret key:

Step1. The user generates randomly suitable number of symbols, greater than the required actual key, say 88 symbols. For example, let us generate 88 symbols like

sB1-Q<*9h=5y7t>.W2!8g3elk,0+#p4fD:?rS&b6$)wc
Tj%’~3o?iN^{zu@q/“;RmH1lav9+f80s.}cy2Pg(\Fi3%

Step2. Dividing the generated symbols to n groups, n> 10, each group consists of only 4 symbols. Like:

sB1- Q<*9 h=5y 7t>. W!8{ g3El k,0+ #p4f D|?r &Sb6 $wc)
Tj%’ ~3O? Ni^{ zU@q /“Rm; H1]a v9+f 8[s. }cY2 Pg(\ Fi3%

Step3. Assigning names, each group is named by the first symbol in that group, and assigning one group to one finger, the name of the finger is the name of the group. Repeat this step 10 times to cover all the hands fingers.

sB1- Q<*9 h=5y 7t>. W!8{ g3El k,0+ #p4f D|?r &Sb6 $wc)
Tj%’ ~3O? Ni^{ zU@q /“Rm; H1]a v9+f 8[s. }cY2 Pg(\ Fi3%

Step4. Selecting start and end points. For example, let the start point is the Middle finger in the right hand, tappet Selecting a suitable path to go from the start point to the end point.

https://doi.org/10.54582/TSJ.2.2.23

III.2 Implementation

The suggested key generation model is implemented using C++ compiler under Windows environment.

```
ÂÑÓBu@îæg~~£CUý,XwÍfb·:„1Ñv‰¸Fs\€ŠÅ

Øf[r¥õOr×»^ò‰N|"‹Gé

$ Ö t W 1 z * _ ë ~ µ ½ ² DEL ü % » Ã E I ⍰ š é Ë Ð ß ‹ Ú Ï ³ s è v ]
é‰ƒäú:¥SŠj#gøØv³6õ¾˜ºÃü³cyÎÆßXV\‰Y:3š>N}mo
?ªßPŽ4lé¤ÊÝ”`ƒ°-‹p¶ÙÑÕ’°í<Œ¼¶B¶dùú8HÝRÇöÕ¢@
P P 3 É e { › ü Û ä ‹ ¬ — Ú Å – e % Ú + ¶ e 2 y Ï M 3 o I U “ @
Á™D | 8/;2!84><!!7?4,*#)”<--1>.57=-(::
```

Security gained and Verification

The suggested method has security gained as follow:

1. Security gained corresponding to the first passphrase file, because the first passphrase file may contain any data, related to any directory.
2. Security gained corresponding to the second passphrase file, because the second passphrase file may contain any data, related to any directory.
3. Security gained corresponding to the salt, because the salt is kept secretly.

Conclusion

Identity impersonation may occur due to the weakness in the secret keys. This paper focus on the problem of memorizing/remembering long secret key, and suggests to generate randomly suitable number of symbols, greater than the required key, dividing the generated symbols into n groups, n, each group consists of only 4 symbols. Assigning names for each group by the first symbol in that group, and assigning one group to one finger of the human hand, the name of the finger is the name of the group. Doing his 10 times will cover all the hands fingers.

References

[1] William Stallings, —"Cryptography and Network Security: Principles and Practice", (7th Edition), Prentice Hall, 2017.

[2] Y.A. Alahmadi and S.N. Alassali," An Improved Key Distribution Protocol Using Symmetric Key Cryptography", International Journal of Computer Sciences and Engineering (IJCSE),Vol.8, Issue.11, pp.21-26, 2020.

[3] Runhai Jiao 1,*, Hong Ouyang 2, Yukun Lin 1, Yaoming Luo 3, Gang Li 4, Zaiyu Jiang 2 and Qian Zheng, "A Computation-Efficient Group Key Distribution Protocol Based on a New Secret Sharing Scheme", Information 2019, 10, 175; doi:10.3390/info10050175, PP. 1–18, 2019.

[4] David M. Burton (2003) "Elementary Number Theory" 2nd Edition Universal Book Stall New Delhi India.

[5] Douglasr. Stinson (2002) "Cryptography: Theory and Practice" Department of Combinatory and Optimization University of Waterloo, Waterloo, Ontario Canada. 2nd Edition, Chapman & Hall/CRC.

[6] Deborah Russell and G. T. Gangemi Sr (2014) " Computer Security Basics" O'Reilly & Associates, Inc., New York.

[7] H.X.Mel. Doris Baker(2011) "Cryptography Decrypted" 2nd Edition. Addison-Wesley.

[8] K. Liu, J. Ye and Y. Wang, "The Security Analysis on Otway-Rees Protocol Based on BAN Logic", IEEE 4th International Conference on Computational and Information Sciences (ICCIS), Chongqing, China, pp.341-344, 2012.

[9] Deborah Russell and G. T. Gangemi Sr (2001) " Computer Security Basics" O'Reilly & Associates, Inc., New York.

[10] Bruce Schneier (2001) "Applied Cryptography" 2nd Edition John Wiley & Sons. (ASIA) Pvt. Ltd., 2 Clementi Loop # 02-01, Singapore 129809.