College of Adminstration and Economics Tanmyat AL-Rafidain 92(30) 2008
P.P [9-18]

Applying Message Authentication Code (MAC) in text chatting system

Abdulla A. Abdulla
Assistant Lecturer
Computer Science Department
University of Mosul
aaamoa@gmail.com

Yaseen H. Ismaeel
Assistant Lecturer
Computer Science Department
University of Mosul
Yaseen_info_2005@yahoo.com

Abstract

The use of Cryptography of text Authentication has become a standard approach in many applications, particularly in Internet Security Protocols. This research describes a new approach of authentication text and can be applied to text chatting system. This work presents simple and practical constructions Message Authentication Code (MAC) based on a cryptographic hash function. The proposed MAC Code provides security and authenticity for any length of messages, furthermore it is fast and easy to implement.

تطبيق رمز وثوقية الرسالة في نظام المحادثة النصية

المستخلص

إستخدام التشفير لتحقيق وثوقية النصوص أصبح من الذي الطرق القياسية في العديد من التطبيقات وخاصة أمنية الانترنت. هذا البحث يوضح طريقة جديدة لوثوقية النصوص وتطبيقها في نظام المحادثة النصية. هذا العمل قدم طريقة بسيطة وسهلة التطبيق من الناحية العملية لإنتاج رمز وثوقية الرسالة (MAC**) بالأعتماد على دوال التموية المشفرة. رمز وثوقية الرسالة المقترح وفر السرية والوثوقية للرسائل وبأطوال غير محددة بالأضافة الى أن الطريقة المقترحة تعد سريعة وسهلة التطبيق.**

1. Introduction:

Message authentication is used when two parties sharing a key **a** wish to communicate and have some assurance that each received message comes from the purported sender and has not been altered along the way (Krovetz T., 2005). This is one of the most widely used cryptographic primitives and it may become even more so as security concerns grows. It is reasonable to anticipate that virtually every transmitted message (or packet) will use cryptographic means to ensure authenticity [Krovetz T., 2005][Bellare M.,

تأريخ استلام البحث ٢٠٠٧/٢/٢١ تأريخ قبول النشر ٢٠٠٧/٩/٩

1995]. Most commonly such a mechanism is based on a secret key **a** shared by the parties and takes the form of a message authentication code (MAC) [Bellare M., 1995]. A message authentication code (MAC) provides a way to detect whether a message has been tampered with during transmission. The usual model for authentication includes three participants: A transmitter, a receiver and an opponent. The transmitter sends a message over an insecure channel, where the opponent can introduce new messages as well as alter existing ones. The goal of opponent is to deceive the receiver into a believe that the new message is authentic [Boesgaard M., 2005] . If the sender and receiver would use a MAC utilizing a (secret) key there would be no way for the opponent to intercept and send out a new message as he doesn't know the key [Krovetz T., 2005][Boesgaard M.,2005]. There are two primary methods of constructing MACs: with block cipher or with hash functions [Bellare M., 1998][Gouda M., 2003]. The most prevalent MAC is the cipher block chaining message authentication code(CBC MAC) specified in the international standard ISO and the U.S. standard ANSI, which depends on DES block cipher [Bellare M., 1995][Gouda M. , 2003].

Wegman - carter [Krovetz T. , 2005] message authentication paradigm is for the sender first to hash the message with a hash function known only to himself and the receiver. The sender then applies some cryptographic function (usually encryption) to the resulting hash value which produces a message tag that's sent along with the message to the receiver. The receiver can then repeat the process verifying that the received tag is valid for the received message in a correctly designed MAC only those knowing the secret hash function and cryptographic key have a reasonable chance of creating a valid tag for any new message. Gilbert, Mac Williams and Sloane [Edgar N., 1974] introduced the idea of provably secure authentication. This method is fast, but it requires keys longer than L bytes to handle L - bytes messages, and it requires a completely new key for each message, Wegman and Carter [Wegman M., 1979] pointed out that the key length could be merely 64 long L for the first message plus 16 bytes for each additional message . Karp and Rabin [Karp R., 1987] achieved a key length of 32 bytes for the first message.

This research presented a proposed MAC depending on calculating hash function and applying it in text chatting system. The proposed MAC used a secret key encryption and accepted any length of messages. The new MAC is to detect any opponent activities i.e. disclosure, insertion, deletion, and rearranging of message characters while sending through computer's network; so it provides both message authentication and security.

2. Hash Function:

Cryptographic hash functions play an important role in achieving authentication and data integrity. The basic idea of cryptographic hash

functions is that a hash value serves as a compact representative image (sometimes called an imprint, digital fingerprint, or message digest) of an input string, and can be used as if it were uniquely identifiable with that string. Hash functions take a message m and produce a hash value. Messages can be of arbitrary length, while the hash value is a fixed length value. Following at the highest level, Cryptographic hash functions may be classified into two classes: hash functions, whose specification dictates a single input parameter - a message unkeyed hash functions; and keyed hash function, whose specification dictates two distinct inputs a message and a secret key [Stallings W., 1999] [Audubon J. , 2003].

This paper concerned with keyed hash functions which are also called one - way hash functions (or Message Authentication Code (MAC)). Atypical usage of one-way hash functions for data integrity is as follows: The hash - value corresponding to a particular message M is computed at time t_1. At a subsequent time t_2, the following test is carried out to determine whether the message has been altered, i.e., whether a message M' is the same as the original message. The hash - value of M' is computed and compared to the protected hash - value; if they are identical, one accepts that the inputs are also equal, and thus that the message has not been altered [Stallings W., 1999] [Jan C., 1998].

A hash-value should be uniquely identifiable with a single input in practice, and collisions should be computationally infeasible to find (essentially never occurring in practice). In this paper, a novel and fast one-way hash function is proposed, The proposed one-way hash function (MAC) is based on calculating 5 bytes hash value to provide more security and authenticity to the hash value itself [Stallings W., 1999] [JiXian Y., 2005].

3. Message Authentication Code (MAC):

An alternative authentication technique involves the use of a secret key to generate a small fixed-size block of data known as a cryptographic checksum or MAC that is appended to the message. This technique assumes that two communicating parties, say A and B, share a common secret key K. When A has a message to send to B, it calculates the MAC as a function of the message and the key: MAC = C_k(M). The message plus MAC are transmitted to the intended recipient. The recipient performs the same calculation on the received message using the same secret key, to generate a new MAC . The received MAC is compared to the calculated MAC. If we assume that only the receiver and the sender know the identity of the secret key, and if the received MAC matches the calculated MAC then the receiver is assured that the message has not been altered and the message is form the alleged sender. MAC mechanism can be illustrated in Figure 1 [Stallings W., 1999] [Jan C., 1998] .

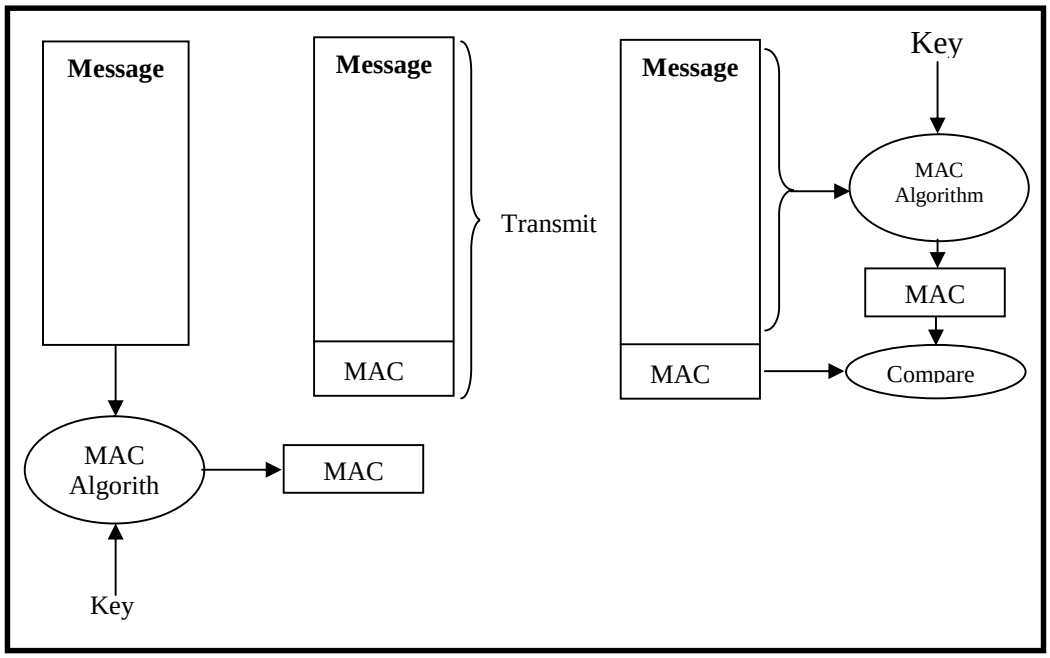


Figure 1 MAC Mechanism

4. The Proposed MAC Description:

To provide message authentication and security in the proposed system, the following ideas has been depended :

A. The MAC depended on secret encryption methods. The secret key shared between communication parties (i.e. sender and receiver) . [Schneier B.,1996] [Pfleeger C., 1989]

B. To provide the security to the resulted cipher text; the idea of transposition methods was used depending on the secret key .

[Schneier B. ,1996] [Pfleeger C. , 1989]

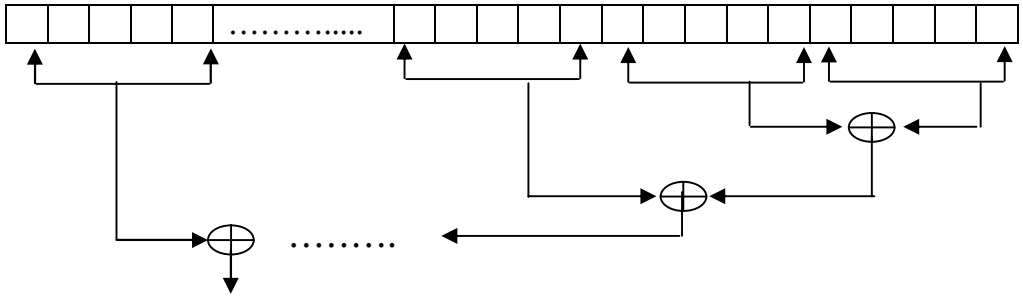
C. The proposed MAC use hash function in different way. First the key inserted in the begin and end of the message, Second calculate 5 bytes hash values of the new message .

D. To provide high level of message authentication and security in the proposed MAC. The MAC value not transmitted with the message separately but it embedded in the message and the all (message and MAC value) are encrypted according to the new proposed method .

5 . The proposed algorithm :

First : the sender do the following steps :

1. Input the message (plain text) and do message padding operation if message length MOD 5 not equal zero .
2. Input the 5 characters secret key and inserted it in the begin and end of the message to produce a new character sequence .
3. Make XOR operation start from the last 5 characters (5 bytes) to the begin of the characters sequence resulted from step 2 .
   i.e.



4. Arrange the 5 bytes resulted from step 3 depending on the key , and make XOR operation between these bytes to produce one byte represented the MD1 value .
5. Perform XOR operation to the characters sequence resulted from step 2 to produce MD2 value .
6. Calculate the MD3 , MD4 , and MD5 values for the characters sequence resulted from step 2 as follows :

   MD3 = (A no. $\oplus$ E no.) $\cap$ (I no. $\oplus$ 5)

   MD4 = (O no. $\cup$ 5) $\oplus$ (MD2 $\oplus$ MD1)

   MD5 = (Characters sequence length - 10) $\oplus$ (MD3 $\cup$ MD4)

   Where A no. , E no. , I no. , and O no. represent the number of these characters in the sequence. $\oplus$, $\cap$, $\cup$ represent logical XOR , AND , OR operations . MD1,MD2,MD3,MD4 and MD5 represent (5 bytes) hash value .
7. Replace the 5 bytes key which are inserted in the step 2 by the 5 bytes values of MD1 , MD2 , MD3 , MD4 , and MD5 to produce new characters sequence .
8. Rearrange the characters sequence resulted from step 7 five times in the form of even characters followed by odd characters .

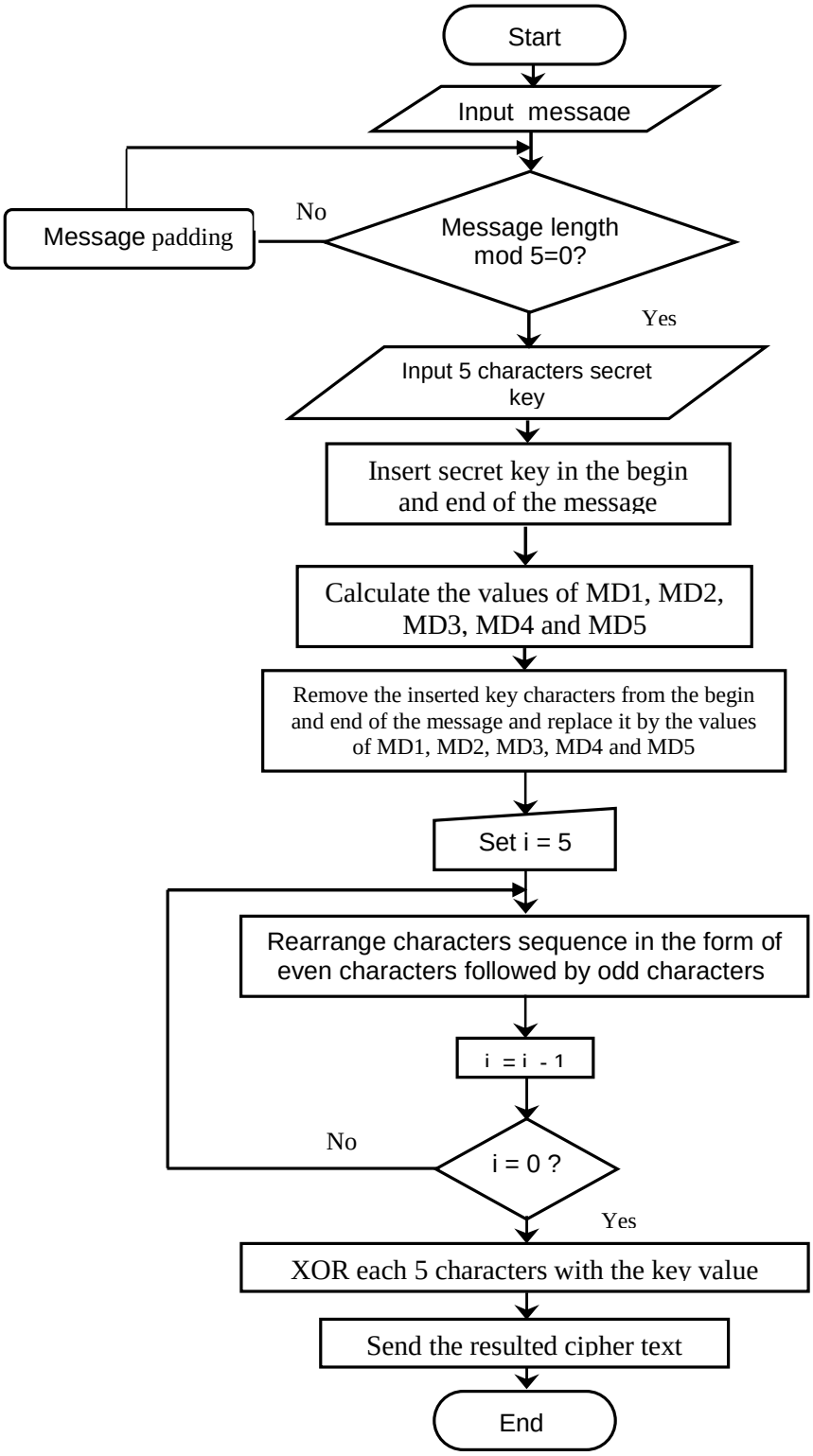


Figure 2 sender algorithm for the proposed system

9. Make XOR operation between each 5 characters (block) of the characters sequence resulted from step 8 with 5 bytes key to produce the cipher text, which will be send to the receiver. the sender algorithm flowchart of the proposed system is clarified in figure 2 .

Second: The Receiver Do the Following Steps:

1. Input cipher text, and it's length MOD 5 must be zero .
2. Input 5 character (bytes) secret key.
3. Make XOR operation between each 5 bytes of the cipher text sequence with the 5 bytes secret key.
4. Rearrange the characters sequence resulted from step 3 five times in the form of even characters followed by odd characters.
5. Remove the 5 bytes represent MD1, MD2, MD3, MD4, and MD5 values (MAC value) from the begin and the end of the sequence resulted from step 4, and replace these value by 5 bytes secret key value.
6. Calculate the value of MD1, MD2, MD3, MD4, and MD5 values (MAC value) depending on the same way used by the sender, and use the characters sequence resulted from step 5 .
7. If the calculated values of MD1, MD2, MD3, MD4, and MD5 values in sep [6 match the values in step 5 then the receiver be assured that the message is authentic and it's came from authorized sender, otherwise the message not authentic. the receiver algorithm flowchart for the proposed system is explained in the figure 3 .

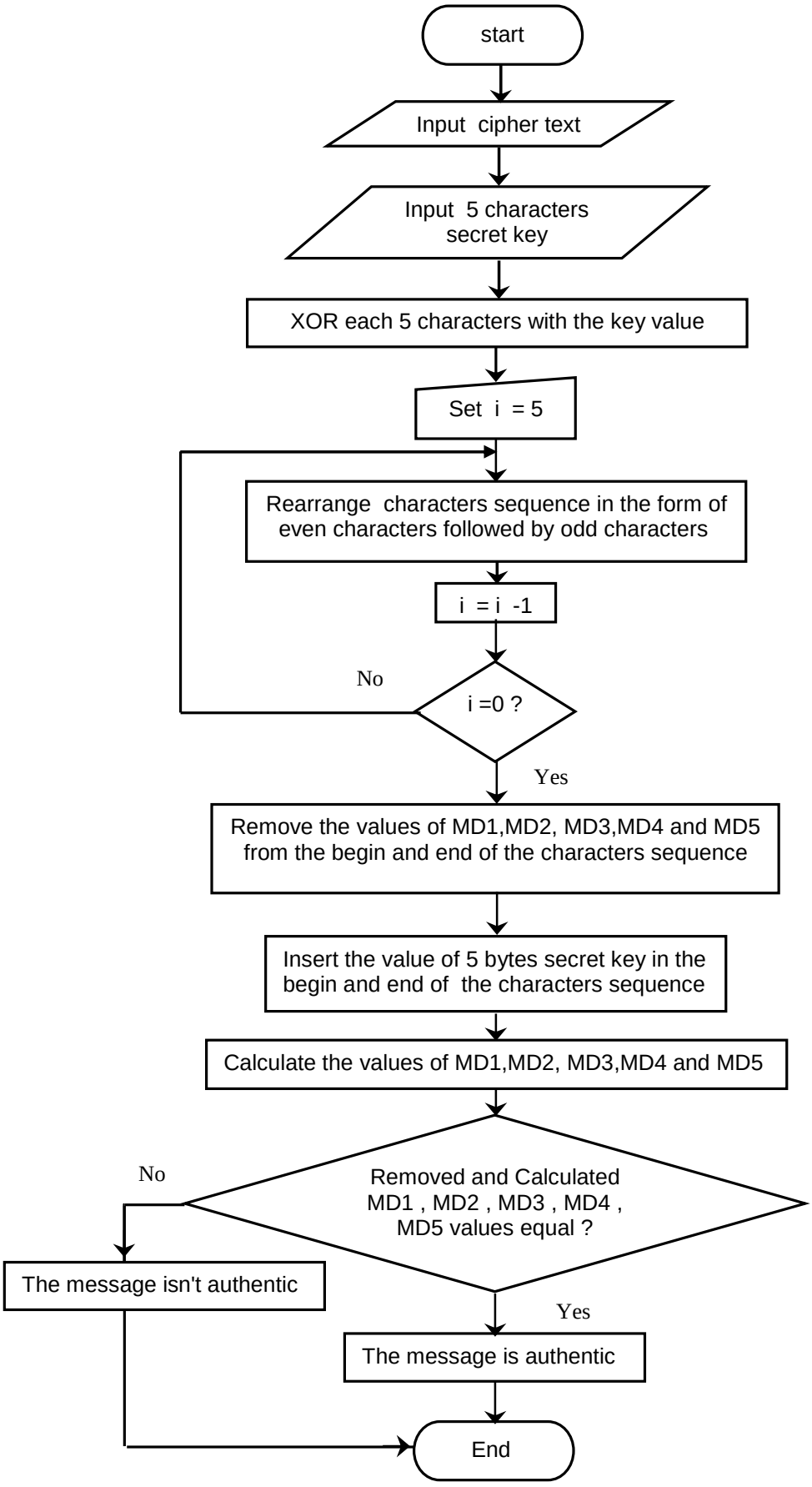


Figure 3 receiver algorithm for the proposed system

6. Practical Experiment:

The proposed MAC system is programmed using Visual Java++ language, so the figure 4 explains the main window of the system. The proposed MAC system tested using different types of messages with any length as show in the following examples:

1. plain text is "send help soon" , the key is "٨٩٧٨٦ " , so the cipher text will be " H DWYV $66",[H KVXV +77"# "
2. plain text is "I will meet you this night" , the key is "89997" , so the cipher text will be :
   " MQPD WP^_L }79wg MQPD WP^_L }79 wg"
3. plain text is "call me now" , the key is "٩٥٤٣٢ " , so the cipher text will be "WZC q22x{]]N |44r"

Figure 4 MAC system

7. Conclusions:

In this paper, a novel message authentication code (MAC) is presented and applied in text chatting system. The proposed MAC system has many good features include: High speed of operation, Easy to implement and accepted any length of messages .

The proposed MAC system uses high complexity hash value (tag) which consists of 5 bytes and each byte results from different calculations. The hash function is used to present hash value (MAC) is collision free so it's computational infeasible to find two messages have same hash value.

To provide high level of security and authenticity in the proposed MAC system, the hash value (MAC, tag) not transmitted with the message separately but it embedded in the message and the all (message and MAC value) are encrypted using the idea of transposition methods .

References :

1. Audubon J. James, (2003) , "Sha-1 encryption algorithm", vocal technologies, ltd., parkway buffalo, in New York,
2. Bellare M., Canetti r., Krawczyk H., (1998), "Keying hash functions for message authentication", springer _ veriag .
3. Bellare M., Guerin R., Rogaway P., (1995) "XOR MAC: new methods for message authentication using finite pseudorandom functions "advances in cryptology –crypto 95 proceedings, lecture notes in computer science vol.963.
4. Boesgaard M., Scavenius O., and etal., (2005), "Badger a fast and provably secure MAC", Applied Cryptography and Network Security (ACNS) conference .
5. Edgar N. Gilbert, F. Jessie Mac Williams, Neil J. A. Sloane, (1974), "Codes which detect deception", bell system technical journal 53, 405-424. Issn 0005-8580 .
6. Gouda M., (2003), "Survey of message authentication code (MAC) constructions and future development", computer science, university of Texas at austin.
7. Jan C. A., (1998), "Basic methods of cryptography", published by Cambridge university press.
8. JiXian Y., (2005), "A Mathematical Theory of Hash Function", YiChun 336000, JiangXi, China
9. Karp R., Rabin M ., (1987), "Efficient randomized pattern – matching algorithms", IBM journal of research and development .
10. Krovetz T., (2005), "Message authentication on 64-bit architectures", department of computer science, California state university, Sacramento ca95819 usa .
11. Pfleeger C. P., (1989), "Security In Computing", the university of tennessee, published by prentice-hall international, inc, printed in the united state of america
12. Schneier B., (1996), "Applied Cryptography", published by katherine schowalter,, printed in united state of america .
13. Stallings w., (1999), "Cryptography and Network security principles and practice", second edition, published by prentic _ hall, inc, the united state of america.
14. Wegman M., Carter J., (1979), "new classes and applications of hash function".