J. Bangladesh Electron. 12 (1-2); 01-06, 2012

Strong Message Authentication and Confidentiality Checking Approach through Authentication Code Tied to Ciphertext

Sydul Islam Khan[1], Md. Alamgir Kabir[2], Anisur Rahman[1]
Md. Ismail Jabiullah[3] and M. Lutfar Rahman[4]

[1] Department of Computer Science and Engineering, Daffodil International University, Bangladesh
[2]Department of Software Engineering, Daffodil International University, Bangladesh
[3]Department of Computer Science and Engineering, Hamdard University Bangladesh, and
[4]Daffodil International University, Bangladesh.
[1]ksonju_cs@yahoo.com, [3]mijjabi@yahoo.com

Abstract

Message Authentication and confidentiality checking of the message are very much demanding issues in various aspects for current secured electronic transactions. A strong message authentication and confidentiality checking technique has been designed, developed and implemented using Java programming language. To do this, message is encrypted with a secret key K_1 that produces message authentication code (MAC), concatenate it with the message and again encrypted them with another secret key K_2 and again encrypted the output with key K_1 that builds the ciphertext that is to be sent to the destination. In the receiving end, first perform decryption with the secret key K_1 and then again decrypts the output with the secret key K_2 that produces the message and the MAC of the message, and then decrypts the message only to produce message authentication code MAC'; and compare the new MAC' with received message authentication code MAC that ensures the authentication of the message. Here, key values ensure the strong authentication and also confidentiality of the communicating message. It can be applied where higher-level security services of the communicating messages are needed.

Keywords: Message Authentication, Ciphertext, Secret Key, Confidentiality, Integrity and Message Authentication Code.

1. INTRODUCTION

Message authentication is a procedure that allows communicating parties to verify that received message is authentic and a message is said to be authentic when it is genuine and comes from its alleged source. An electronic transaction is best thought of as a type of electronic message that change the relationship between the sender and receiver in some important way. Electronic transactions offer speed of execution regardless of distance. They also offer accuracy and precision [1]. The key benefit of the system is a considerable potential for saving time and cost. Secure Electronic Transactions (SET) relies on the science of cryptography – the art of encoding and decoding messages. One of the reasons that encryption mechanism does not provide a good solution for message authentication is that it is difficult for the receiver to identify the legitimate plaintext. To address this problem, we can apply a process to generate a message authentication code (MAC) to the message so that only legitimate plaintext can pass the MAC detection. Such MACs are used in the network communication to provide data integrity verification against bit errors introduced by communication channel noise. But it cannot provide data integrity protection against malicious attackers. The reason is that the attackers can manipulate the message in a way which cannot be detected by MAC. Although encrypting the message and its MAC as a whole seems to be a valid approach, yet existing work shows that it still suffers from some attacks. Also it cannot solve the efficiency issue of the encryption mechanism. In light of MAC, we can design a code that uses a secret key. Without the key, modifying the message in a way that it matches the code is impossible. This idea leads to the design of MAC. Essentially, the message authentication code (MAC) is a small fixed-size block of data that is generated based on a message M of variable length using secret key K as follows. It is also called cryptographic checksum.

$$MAC = E_K(M)$$

If a party A wishes to send party B a message M, and protects it via a MAC, they first need to share a secret key K. Then A calculates code MAC as a function of M and K. Then the message M plus the code MAC are transmitted to B. B performs the same calculation on M, using K to generate a new code MAC′. The received code MAC is compared to the calculated code MAC′ to verify the data integrity. As only A is able to generate MAC, source authentication is also achieved. MAC provides an efficient way to message authentication. It also separates the authentication function from confidentiality. This is an attractive feature for many applications where confidentiality is not necessary. Message Authentication is one of the demanding areas of network security. Message authentication is a process to verify that the received message come from the alleged source and have not been altered.

A message authentication technique involves the use of a secret key or shared key to generate a small fixed-size block of data that is known as cryptographic checksum or message authentication code (MAC) or message digest (MD). The message plus the MAC are transmitted to the destination. The intended recipient performs the same calculation on the received message, using the same secret key or shared key, to generate a new message digest or message authentication code. 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:

(a) The receiver is assured that the message has not been altered. If an attacker alters the message but does not alter the MAC, then the receiver’s calculation of the MAC will differ from the received MAC. Because the attacker is assumed not to know the secret key, the attacker cannot alter the MAC to correspond to the alterations in the message.

(b) The receiver is assured that the message is from the alleged sender. Because no one else knows the secret key, no one else could prepare a message with a proper MAC.

(c) If the message includes a sequence number, then the receiver can be assured of the proper sequence because an attacker cannot successfully alter the sequence number.

To realize the processes of the message authentication code generating and verifying two conventional approaches are studied. In this paper, an improved approach for message authentication and confidentiality checking approach has been designed, developed and implemented in Java for achieving the better security services of the message transaction system. A comparative study on the proposed system and the conventional systems has also been performed and presented.

2. CONVENTIONAL METHODS

To realize the message authentication, two approaches are studied and realized. First approach establishes a message authentication between the communicants. The diagram of the message authentication using message encryption with a shared secret key is depicted in Fig. 1.

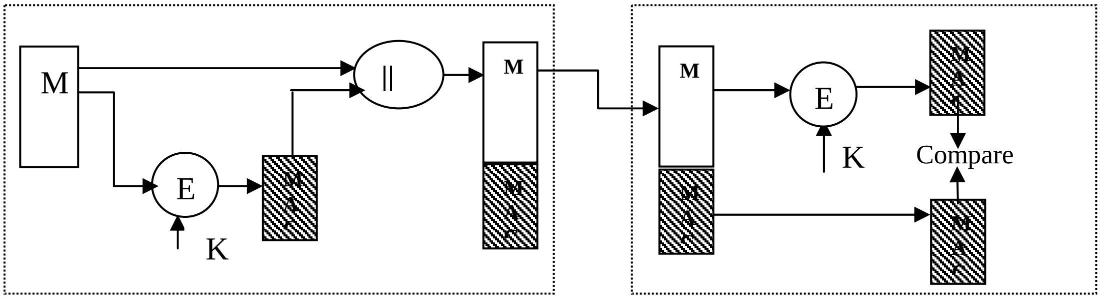


Fig. 1: Secured Message Transactions with Message

In this approach, message is encrypted with a shared secret key K that produces a message authentication code (MAC) and concatenates it with the message. Then the message plus the message digest is sent to the destination. In the receiving end, the message is again encrypted with the same shared secret key K and produces another message authentication code MAC' and compared it with the received MAC. If the MACs are the same, then the receiver assured that the received message is come from the alleged source and the message is not altered. It establishes secured message transactions with message authentication. The communicating message has not been altered in the transition. This process does not provide confidentiality, integrity and non-repudiation security services. To provide these security services, another layer of security mechanisms are needed.

The second approach establishes a stronger message authentication and confidentiality checking between the communicants.

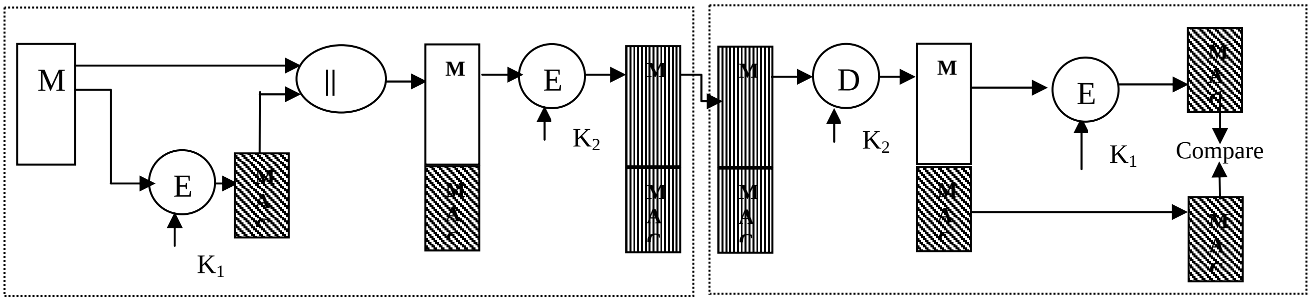


Fig. 2: Secured Message Transactions with Message Authentication and Confidentiality; Authentication Tied to

In this approach, message is encrypted with a shared secret key K_1 that produces a message authentication code MAC and concatenates it with the message. Then the message plus the MAC is again encrypted with another shared secret key K_2. The output is sent to the destination. In the receiving end, the received information is decrypted with the secret key K_2 that produces the message and the MAC of the message. Then the message is encrypted with the same shared secret key and produces another message authentication code MAC and compared it with the received MAC. If the MACs are the same, then the receiver assured that the received message is come from the alleged source and the message is not altered. In this case, encryption-decryption with the shared secret key K_2 assures the confidentiality of the message and the message authentication code MAC. This is a layer two security of the communicating message in the transaction. And the other part of the process establishes secured message transactions with message authentication. The diagram of the message authentication with more confidentiality in the message using message encryption with two shared secret keys is depicted in Fig. 2. In our paper, a stronger approach stronger approach has been established for message authentication and confidentiality checking of the communicating message by using two secret shared keys.

3. PROPOSED SYSTEM

Consider the straight forward secret-key encryption-decryption process on the transmitted messages. A message M transmitted from source A to the destination B is encrypted by a conventional cryptographic mechanism using a secret key shared by the sender A and as well as receiver B. If no other party knows the secret key K and no other party can decrypt the transmitted message, then the confidentiality is provided.

Methodology

Here, message is encrypted with a key K_1 that produces message authentication code (MAC), concatenate it with the message and again encrypted them with key K_2 and again encrypted the output with key K_1 which builds the ciphertext that is to be sent to the destination. In the receiving end, first perform decryption with the key K_1 and then again decrypts the output with key K_2 that produces the message and the message authentication code MAC of the message, and then decrypts the message only to produce message authentication code MAC'; and compare the new message authentication code MAC' with received message authentication code MAC that ensures the authentication of the message. Here, key values ensure the strong authentication and also confidentiality of the communicating message. The diagram of the message authentication with more confidentiality in the message using message encryption with two shared secret keys is depicted in Fig. 3.

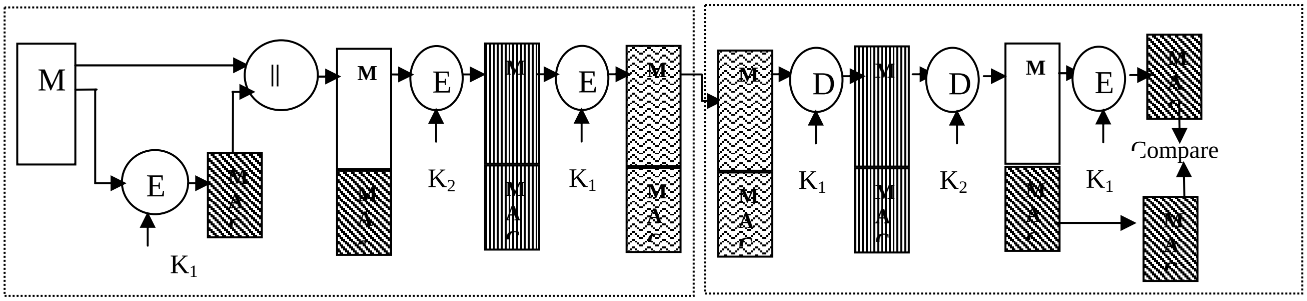


Fig. 3: Stronger Secured Message Transactions with Message Authentication and Confidentiality; Authentication Tied to Plaintext

Algorithm:

The encryption algorithm of the proposed system is composed of the following steps.

Step 1: Sender select the message and divide it into block of messages of key length. Padding is used if necessary.

Step 2: Perform encryption process on the block of messages using the secret key K_1 that produces the message authentication code MAC or check sum. Concatenate it with the message and again encrypted them with another secret key K_2 and the output is again encrypted with the secret key K_1 which builds the ciphertext that is to be sent to the destination.

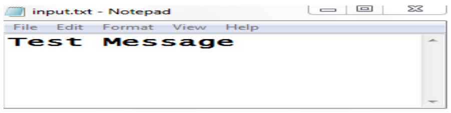
Step 3: In the receiving end, first receiver performs decryption with the secret key K_1 and then the output is again decrypted with the secret key K_2 that produces the message and the message authentication code MAC of the message.

Step 4: Then the receiver encrypts the message only to produce a new message authentication code MAC'; and compare the new generated MAC' with the received MAC. This ensures the authentication of the message. Here, using the two secret key values ensures the strong authentication and two times encryption-decryption establishes the confidentiality of the communicating messages.

The whole process is depicted in Fig. 3.

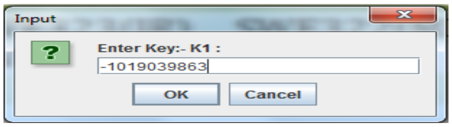
4. IMPLEMENTATION ON JAVA

The proposed method has been implemented using the Java programming language because of its simplicity, better security and its better interactive property with the users. For this Java software JbK-6u21-windows-i586 is installed in C drive of the system. For example, if take "Test Message" is taken as the plaintext (Fig. 1), -1019039863 as the secret key K_1 (Fig. 2), the process produces the ciphertext given in Fig. 3. The produced ciphertext is used here as the MAC.



Test Message

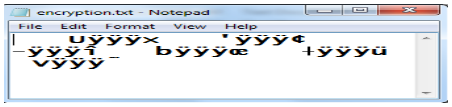
Fig.1: Input Message



Enter Key:- K1 :
-1019039863

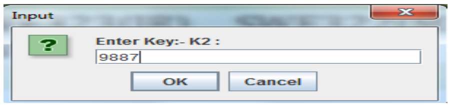
Fig.2: Secret Key K_1

Then the number 9887 is used here as the secret key K_2 depicted in the Fig. 4 to produce the second ciphertext that is pictured in Fig. 5. This output is again encrypted with the secret key K_1 to produce the final ciphertext and that is to be sent to the destination.



```
    Uÿÿÿ×      'ÿÿÿ¢
—ÿÿÿî ˍ    bÿÿÿœ     +ÿÿÿü
 vÿÿÿ˜
```

Fig.3: MAC by K_1

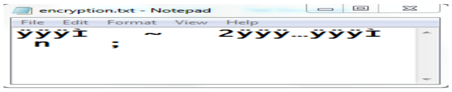


Enter Key:- K2 :

9887

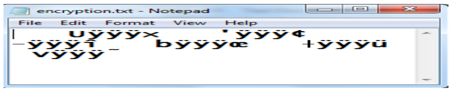
Fig.4: Secret Key K_2

In the receiving end, the received ciphertext is first decrypt by using the secret key K_1 that produces the intermediary ciphertext pictured in Fig. 6. After that the intermediary ciphertext is again decrypted by the secret key K_2 to retrieve the plaintext that is given in Fig. 8. And the message is again encrypted with the secret key K_1 that produces the MAC (Fig. 3) and is compared with the received MAC.



```
ÿÿÿì     ~      2ÿÿÿ…ÿÿÿì
 n      ;
```

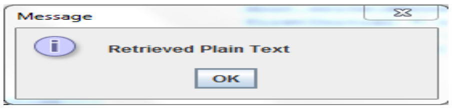
Fig.5: Ciphertext is sent to the Destination



```
    Uÿÿÿ×      'ÿÿÿ¢
—ÿÿÿî ˍ    bÿÿÿœ     +ÿÿÿü
 vÿÿÿ˜
```

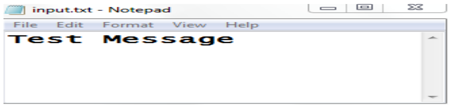
Fig.6: Retirevd Ciphertext

If the produced MAC is matched to the received MAC, that assures that the message is not altered in the transition, i.e. the message is found in the receiving end with full authentication.



Retrieved Plain Text

Fig.7: Secret Key K_1



```
Test  Message
```

Fig.8: Secret Key K_1

The process is implemented in Java programming language for several times for different messages and is found its satisfactory results.

5. Security Analysis

Any security system performs the fundamental security services which are confidentiality, authentication, integrity checking and non-repudiation. The proposed system performs all the security services and is shown in Table 1.

Approaches	Confidentiality	Authentication	Integrity	Non-repudiation
Fig.1	No	Yes	No	No
Fig.2	Yes	Yes	No	Yes
Fig.3	Yes	Yes	Yes	Yes

Finally, the desired plain text is found again that is given as input (Fig. 16). Here, the retrieved output is also found as plain text file in project folder.

For the proposed system it is tried try to implement the project in Java language because of stronger security. The proposed system is run very well in this program. Several different inputs are analyzed for this program and every one of them is produced correct output. It can be observed that the program can be used for variable length file transfer. Some difficulties are faced to implement the program in Java language, because Java language has some limitations. To overcome these difficulties it is needed for further research in future.

6. CONCLUSIONS

A message authentication and confidentiality checking technique has been designed, developed and implemented using Java programming language and is found stronger security services. For doing this, first message is encrypted with a secret key K_1 that produces message authentication code (MAC), concatenate it with the message and again encrypted them with another secret key K_2 and again encrypted the output with key K_1 that builds the ciphertext that is to be sent to the destination. In the receiving end, first perform decryption with the secret key K_1 and then again decrypts the output with the secret key K_2 that produces the message and the MAC of the message, and then decrypts the message only to produce message authentication code MAC'; and compare the new MAC' with received message authentication code MAC that ensures the authentication of the message. In this method, key values ensure the strong authentication and also confidentiality of the communicating message. It can be applied where higher-level security services of the communicating messages are needed.

REFERENCES

[1] Charlie Kaufman, Radia Perlman and Mike Speciner, "Network Security Private Communication in a Public World", 2nd Edition, 2003, ISBN: 81-7808-790-1.

[2] Behrouz A. Forouzan, "Cryptography & Network Security", 1st Edition, 2007, ISBN-13: 978-0-07-066046-5. Accessed on January 05, 2011.

[3] William Stallings, "Cryptography and Network Security – Principles and Practice", 4th Edition, 2006, ISBN: 978-81-203-3018-4.

[4] Bruce Schneier, "Applied Cryptography", 2nd Edition, 2003, ISBN: 9971-51-348-X.

[5] Wikipedia, http://en.wikipedia.org/wiki/Initialization_vector, Accessed on December 02, 2010.

[6] Wikipedia, http://en.wikipedia.org/wiki/Block_cipher_modes_of_operation, Accessed on December 03, 2010.

[7] Citrix Product, http://support.citrix.com/proddocs/index.jsp?topic=/access-gateway-46/ag-appendix-types-cryptography-con.html, Accessed on December 12, 2010.

[8] Crypt::C,http://search.cpan.org/~lds/Crypt-CBC-2.12/CBC.pm#LIMITATIONS, Accessed on December 22, 2010.