Research Article

A Study about Prevent Tampering with Encrypted Messages over the Network Using Digital Signature

Majed Al-khairow and Mohamad Firas Al-halabi

Department of Mathematics, Faculty of Science, Damascus University, Damascus, Syria

Correspondence should be addressed to Mohamad Firas Al-halabi; dr-mfalh@scs-net.org

Received 4 April 2022; Accepted 2 June 2022; Published 9 July 2022

Academic Editor: G. Muhiuddin

Copyright © 2022 Majed Al-khairow and Mohamad Firas Al-halabi. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

In this paper, we present a proposed model to increase the authenticity of messages sent over the network; our model went through two stages: First, it is the modification of the MD5 algorithm, which is the basic and comprehensive algorithm from which the Digital signature was launched, where we have modified the logical operations by changing the direction of the shift from left to right and by changing the order of the temporary storage spaces (a, b, c, d). We came up with a lower execution time, and we also compared the execution time of our modified algorithm with the original algorithm and some other Digital signature algorithms. Second, the integration of our modified algorithm with cipher algorithms to increase the authenticity of the sent messages. We applied an example to our proposed model where we used two encryption standards (AES, DES). Finally, we implemented the model using the C# programming language.

1. Introduction

The world is witnessing a vast and rapid development in the field of technology in the world of communication, so modern means of communication, especially the Internet, have become indispensable means. After the communications depended on the phone and then fax, the Internet appeared and became the ideal means of communicating, transmitting, and presenting information. There has been an urgent need to protect, document, and prove this information’s authenticity. From here, the so-called Digital signature appeared. In 1989, the first Digital signature was recognized in France in the field of credit cards with the aim of achieving this, the French Court of Cassation recognized the validity of the Digital signature as it considered that it consisted of two components, namely, showing the credit card and entering the card holder’s secret number and confirmed that this method provides the existing guarantees in hand-signing, and it is even superior to it [1]. Ron Rivest developed the MD5 algorithm at MIT in 1992, one of the members who developed the RSA public key encryption algorithm [2]. In 2009, President Bashar al-Assad issued the Digital signature law in Syria [3]. In 2011, a study was conducted at the University of Aleppo to enhance the security of data exchange on the Internet by means of Digital signature algorithms [4], and most of the Digital signature algorithms focused on one goal, which is authentication. In this research, we are interested in studying both authentication and confidentiality; we first presented the desired objective of the research, then we introduced some basic concepts. We also presented some of the Digital signature and encryption algorithms used in this research, after that we made a modification to the MD5 algorithm in order to reduce its execution time. To achieve confidentiality and authentication, we proposed a model based on some encryption algorithms in addition to the modified algorithm. Finally, we programmed our proposed model in C#, proven with an example.

2. Research Objective

Due to the urgent need to develop new tools to enable or prevent the tampering of encrypted messages across the network and protect these messages, this paper proposes a
developed model for integrating encryption algorithms with a digital signature. The main objective is to increase the authentication of encrypted messages. In order to achieve this within an acceptable time, we did some modifications to the MD5 algorithm to get a lower executive time.

3. Research Materials and Methods

In this research, we rely on Digital signature and cryptography, and we will study the MD5 algorithm which is the starting point from which the Digital signature began, in addition to modifying and comparing it with some other Digital signature algorithms and then merging it with some encryption algorithms.

3.1. Basic Definitions and Concepts. We will present a set of basic concepts that we will use in this research [4–10].

3.1.1. Plain Text. It is the intelligible original message or data, that is, the input to the encryption algorithm.

3.1.2. Encryption Algorithm. It is the process of converting text or data into an ambiguous form for the purpose of hiding this data or is the process of converting Plain text to cipher text.

3.1.3. Key. It is the password used in the encryption or decryption algorithm. It is one of the most important things to hide as it is considered one of the secret things that only those authorized to decode the code know.

3.1.4. Cipher Text. It is the fuzzy message generated as an output from the encryption algorithm and depends on both the plaintext and the key.

3.1.5. Authentication. It is a process by which specific information is proven and confirmed, and this information can be the source of the document, the identity of the sender, the time of signing the document, and the date it was sent.

3.1.6. Digital Signature. A Digital signature is the digital equivalent of a manual signature. It is an authentication technique that includes measures to prevent denial either by the source (sender) or by the destination (receiver). A digital signature can also include measures to check the integrity of the message.

3.2. Some Digital Signature Algorithms. Digital signature algorithms are similar to encryption algorithms. But what distinguishes them from encryption algorithms is that they are one-way algorithms, and they take messages of different lengths. Each of them produces a fixed-length fingerprint (The message digest resulting from the application of the algorithm). We mention some of them: MD5, where this algorithm is considered the first appearance of the Digital signature and was classified by a first-generation algorithm, and as for the second generation, it was developed in 1995 and was called the SHA-1 algorithm. The third generation of this algorithm was recently discovered and called the SHA-2 algorithm, as shown in Table 1. The SHA-2 algorithm is divided into some other algorithms (SHA-224, SHA-256, SHA-384, and SHA-512). We will study the MD5 algorithm which is the cornerstone of all Digital signature algorithms developed afterward.

3.2.1. Message Digest 5 Algorithm (MD5). The MD5 algorithm takes messages of unlimited length and gives a 128 bit fixed-length fingerprint on the output. In terms of input, the message length is 512 bits. If it exceeds that, it will divide the message into more than one block, but if it is less than that, it will be subject to processing by the operations of Padding (It is a set of bits placed at the end of the message if the message length is shorter than the Block Size Message that this type of cipher can handle, and it must be at least 1 bit and at most 512 bits). It is worth noting that the output will be only 128 bits, so the MD5 algorithm is an encryption algorithm with a key length of 128 bits, as shown in Figure 1.

After the message is divided into blocks, the first block will be sent to the buffer which will be processed inside, as shown in Figure 2.

From Figure 2, we find that there are four rectangles placed on top of each other called a ROUND. In each round, the data are entered in a 16-step process. All steps have the same algorithm. While we will now explain the concept of a round with some detail, then we will go deep inside to see the step.

3.2.2. Round. There are four rounds in each Buffer, and they all have the same algorithm. Still, they differ from each other in that they use different Boolean functions, such as F, G, H, and I, so the values of these functions are different, their internal structure is 16 steps, and each round takes 512-bit input of Yq (Figure 2). The Yq value is the split message, the message is divided into 512-bit blocks (Figure 1), and the 512-bit value of Yq is entered on the round with entry values (A, B, C, and D). Whose total values are 128 bits, the value of Yq is constant in all four rounds of one HMD5 buffer and of course differs from each HMD5 buffer, and the next due to the difference in the value of the message part, in the round: T function A real set of values in radians is given as follows:

\[ T[i] = 2^{32} \times \text{abs}(\sin(\pi(i))) ; i = 1 \ldots 64 \]  

Each round has a sequential order of steps found in the buffer. These steps are governed by the following equation:

\[ b = b + ((a + g(b, c, d) + X[i] + T[i]) \times s) \]  

The algorithm of this step calculation equation is shown in Figure 3.

Amounts: a, b, c, and d: the temporary storage spaces that are used in a specific order in each step.

G: it is one of the Boolean functions (I, F, G, and H) changing according to each round, and it is calculated from Table 2
3.3. Cryptography. Cryptography is a science of information security [9]. Cryptography is the art of data protection and the science of message confidentiality, as hiding the meaning of the message is one of the main goals of cryptography which includes storing and sending information securely through unprotected media, such as the Internet or wireless networks by encrypting text information to become in an incomprehensible or readable form. With the help of various encryption algorithms, only the intended user can convert the incomprehensible form of the text into the original text information. In the next paragraph, we mention some encryption standards.

3.3.1. Advanced Standard Encryption (AES). The AES standard is a symmetric block encoder. This standard was published by the National Institute of Standards and Technology (NIST) in 2001. This standard can handle 128 bit blocks. The standard uses AES10, 12, or 14 rounds depending on the length of the key used which can be (256, 192, or 128) bits, respectively.

The AES standard deals with several rounds. Each round consists of several stages. Data are transferred from one stage to another. We call the data at the beginning and end of each stage, we call it the state; the states are like 16 byte blocks but are represented by 4 × 4 S-order arrays we call a data array where each element is expressed as $s_{rc}$. The condition can sometimes be expressed as a $1 \times 4$
matrix of words (this makes sense if we consider each
column of the original matrix as a word). The AES
standard deals with five units of data: Bit, Byte, Word,
Block, and State.

At the beginning of the encryption process, the data
constituting the data blocks are added to the status matrix
column by column and within each column from top to
bottom. At the end of the encryption, data are extracted from
the state in the same way [10].

3.3.2. Data Encryption Standard (DES). The DES standard is
based on the symmetric key theory. The use of the same key
when encrypting and decrypting, since the size of the en-
tered text, is fixed at 64 bits. The size of the encryption key
used is 56 bits. This algorithm operates in three following
stages:

(1) Encryption Key Processing. Here, tables and se-
quential operations are used in which rotation and
permutation are used to finally result in (16) keys to
be used in later stages.

(2) Algorithm Application. Tables and sequential oper-
ations are used in this stage in which rotation and
permutation are also performed as in the previous
stage with the difference that it is done on the text to
be encrypted and not on the encryption key, and
substitution tables are used.

(3) At this stage, a reverse process is performed for part
of what was done in the first stage, where the text is
replaced using permutation tables. Note that, the
decryption process takes place in an opposite way to
the encryption process with very small differences
[9].

4. Model Characterization

4.1. Modified MD5 Algorithm. In this paper, we have made a
modification to the equation of step computation in the
MD5 algorithm, where we changed the direction of the
displacement from left to right, in addition to that, we made
a modification to the logical operations where we replaced
the XOR with AND and we know that the XOR takes two
results and is processed inside the computer while the AND, it takes only one result and it is processed inside the computer, so the execution time of the XOR is greater than the time of the AND execution. Table 3 shows the modifications made to the logical operations.

We changed the order of the temporary storage spaces (a, b, c, d), in order to reduce the time, as shown in the following equation:

\[ d = c + ((a + g(b, c, d) + X[i] + T[i]) \gg s). \] (3)

The modified step calculation equation algorithm is shown in Figure 5.

### 4.2. Suggested Model

Our proposed model introduces a new mechanism for protecting and tampering with messages sent over the network. Our proposed model is based on integrating our modified algorithm with two encryption algorithms, as shown in Figure 6.

Our proposed model consists of two parts: a section for the sender and another for the receiver, where the sender encrypts the message to be sent with one of the encryption algorithms, and then a fingerprint is taken from the cipher text using the modified MD5 algorithm, and then the sender combines the cipher text with the resulting fingerprint. Finally, the sender encrypts the merge output with one of the encryption algorithms and sends the final cipher text to the

freelancer. On the other hand, the receiver will receive the message sent to him, decrypt it then decipher the merging process and isolate the cipher text from the fingerprint then take a fingerprint of the cipher text, and finally perform a comparison process between the two fingerprints. In addition, the two fingerprints are compared to verify the authenticity and confidentiality of the sent message.

A set of steps can explain the working mechanism of our proposed model; where it was divided into steps for the
sender and others for the receiver, and the following is a
detail of that.

Sender steps: The sender performs the following steps:

1. Encrypting the Message Using an Encryption Algorithm
2. Applying the modified MD5 algorithm to the encrypted message and outputting the message’s fingerprint
3. Combining the resulting fingerprint with the cipher text into a single message and rearranging
4. Applying an encryption algorithm to the resulting message (the merge message)

Receiver steps: The receiver performs the following steps:

1. Decoding the Received Message.
2. Decomposing the encrypted message from the resulting fingerprint.
3. Applying the same modified MD5 algorithm that the sender applied to the encrypted message and outputting a second fingerprint.
4. Comparing the two fingerprints (the fingerprint obtained from the sender and the fingerprint obtained from applying the modified MD5 algorithm); if the two fingerprints match, then the message is not tampered with and the code will be decoded securely.

If the two fingerprints are different, the message has been tampered with.

4.3. Experimental Results. To evaluate the efficiency of the modified algorithm that we have proposed we will use C# in order to simulate the experimental results that we have reached during our research according to the following two stages.

The first stage: reducing the execution time of the MD5 algorithm by making a change in the direction of the offset and some modifications to the logical operations where we replaced the XOR with AND operator because, as we know that the XOR takes two results and is processed inside the computer, while the AND takes only one result and is processed inside the computer. And, thus the execution time of XOR is greater than the execution time of AND, and by changing the order of the temporary storage spaces (a, b, c, d), we found the fingerprint for different sizes of texts using our modified algorithm, the original algorithm, and SHA-1 algorithm and calculated the execution time using some functions in a library System Diagnostics for each of the three algorithms as shown in Table 4.

Figure 7 shows our results as it is obvious that our modified algorithm reduced the execution time of the original algorithm.

The second stage is increasing the authenticity of the encrypted messages; this was done through our proposed...
model which relies on the merging mechanism between our modified algorithm and cipher algorithms.

4.3.1. Illustrative Example. In this example, we show the working mechanism of our proposed model using the encryption standards (AES, DES) with the modified digital signature algorithm MD5 where we wrote and implemented the code of our proposed model in Visual Studio 2019 in C# language as shown in Figure 8.

Figure 8 shows that our proposed model is divided into two parts: a section for the receiver and a quote for the sender is as follows.

(1) Sender Section. The sender writes the message to be sent in the input text field as well as two encryption keys in the (keyDES, keyAES) fields of the encryption standards (AES, DES) as in Figure 9.

The sender presses the encryption button and the entered text is encrypted by the AES encryption standard, and the cipher text is shown in the Cipher1 field. In the Merge field, then the merge output is encrypted using the DES encryption standard and the second cipher text is shown in the Cipher2 field as in Figure 10. The sender sends the cipher text with the two encryption keys to the receiver where the two encryption keys are sent over a secure communication channel.

(2) Receiver Section. The receiver receives the encrypted text with the two encryption keys and puts them in the place designated for them as in Figure 11.

The receiver presses the decryption button, and the program decrypts the cipher-text received from the sender with the DES encryption standard and shows it in the DeCipher2 field. Then, the fingerprint is isolated from the cipher text and placed in the Cipher1 and MD5S fields, then the fingerprint is taken.
from the cipher text in the Cipher1 field and shown in the MD5R field. Finally, a comparison is made between the two fingerprints in the fields MD5S and MD5R, and the result is shown in the output field as shown in Figure 12.

5. Results and Their Discussion

First, we formulate a model describing how messages are tampered with and protected. We also suggested
modifications to the MD5 algorithm’s working mechanism to reduce its execution time. We compared the execution time of the modified algorithm with the execution time of the original MD5 algorithm, and then we applied our proposed model which depends on integrating our modified algorithm with cipher algorithms. In addition, we provide an example that illustrates this.

6. Conclusions and Recommendations

Through this research we have done, we reached the following conclusions:

(1) Modifying the MD5 algorithm in order to reduce the time of its implementation
(2) Applying our modified algorithm to a sample of texts and showing that the execution time is less than the time of the original algorithm
(3) Building a proposed model based on our modified algorithm and merging it with encryption algorithms in order to increase the authenticity and protection of sent messages
(4) Applying our proposed model with an illustrative example; As we used our modified algorithm and encryption standards (AES, DES)

To complement the research results and conclusions we recommend the following:

(1) The possibility of modifying the Boolean flags in our algorithm in order to obtain less execution time
(2) Applying encryption and digital signature algorithms to enhance the authentication, integrity, and confidentiality of sent messages
(3) The possibility of modifying our proposed model by merging our modified algorithm with more than two encryption algorithms

7. Research Limitations

Although knowing the encryption algorithm’s execution time is important, this paper was not concerned with calculating the overall execution time of the suggested model. Rather, our direction to achieve the security requirements of authentication and confidentiality is by integrating our modified algorithm with two encryption algorithms.

Data Availability

The data used to support the study are included in the paper.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References