Indian Journal of Science and Technology, *Vol 7(S6), 1–5, October 2014*

ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Generating A Digital Signature Based On New Cryptographic Scheme For User Authentication And Security

K. Ganeshkumar* and D. Arivazhagan

AMET University, Chennai, India; ganesheclipse@gmail.com, arivazhagand@hotmail.com

Abstract

This paper analyzes the computer security of systems and importance of the digital signature and hashing message algorithm. The proposed digital signature algorithm gives a new technology for producing effective output of digital signature as a result the signing [1] and verifying of signatures are very fast compared to earlier ones. To improve the security and authentication of sending data, this method uses "Message Digest", "IDEA" and "GOST"[2] algorithms. The new message digest algorithm is to provide high security, to transfer data by combination of digital signature algorithm and symmetric key cryptography algorithm. The new hashing algorithm proposed creates a unique digital fingerprint along with symmetric key encryption generated IDEA and GOST algorithms [3,4]. The receiver used the symmetric key and hashing algorithm to form a signature. If this message digest match with the sender digests the message the content will be decrypted and read by sender.

Keywords: Digital Signature, Hash Function, Encryption, Message Digest, Finger Print, Security

1. Introduction

The process of creation of digital signature has two major things one is signing and another one is sealing with key. Signing is otherwise called mathematical summery or hash code, it is uniquely identified fingerprint of the original message. If the single bit of the original message changes, the message digest will dramatically change. The next step is sign the hash code with private key, the signed hash code is appended with encrypted original message [5]. The receiver check the original image with public key at the same time the new message digest will be generated and it will be compared with the sender's message digest if it is matched the message will be accepted. Public key cryptography [6] is suitable for small amount of messages and it is faster also. Here we describe a new hash algorithm and symmetric public key encryption to provide a high secure data.

Let us consider an attacker wants to crack the original image of sender; it is enough to change the hashing function between the original image and the message digest. It means attacker can identify the original image after encryption although somewhat difficult to crack. Hence we propose a new hash algorithm to generate a digital fingerprint [7] and one public key encryption technology to make the digital signature secured.

2. Digital Signature Signing

2.1 Existing Digital Signature

The MD5 algorithm is commonly used for creating a digital finger print. The MD5 algorithm converts the original message in to 32 bit chunks. The algorithm divided the whole message in to four 32 bit messages because it considers the message as 128 fixed length[8]. The message

*Author for correspondence

blocks are subjected to five round of modification; each modification contains 16 operations based on non linear function. Let we consider the F,G,H,I are the different modification[9].

F(B,C,D)=(B^C)V(¬B^D)

G(B,C,D)=(B^D)V(C^¬ D)

H(B,C,D)=BØCØD

I(B,C,D)=CØ(BV¬D)

⊕, ∧, ∨, ¬ denote the XOR, AND, OR and NOT operations respectively

After getting this message digest [10] will be encrypted by private key of the sender. The encrypted message digest is called digital signature. Finally the digital signature added with original message and send to the receiver [11].

2.1.1 Steps to Working of Digital Signature

1. 'A' wants to email a message to 'B'
2. 'A' has to upload the file
3. Using special software, system gets a message hash (mathematical summary) of the document.
4. Now 'A' uses the private key to encrypt.
5. The encrypted message is called digital signature (it will vary in different messages)
6. First the sender has to ensure that the system sends it to the correct receiver, and make a hash of received messages, these steps are shown in figure 1.

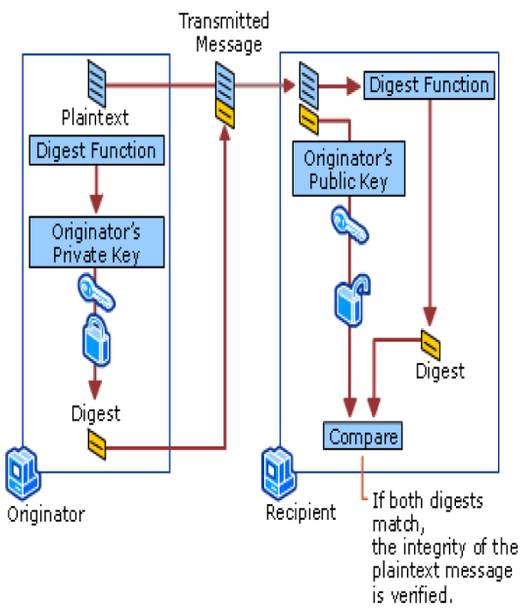

Figure 1. Existing digital signature algorithm.

If the hash matches with received document, then it is original [12].

2.1.2 Issues in Existing Digital Signature Algorithm

In current digital signature the steps of algorithm used for authenticate and integrity. Although we have one private key to encryption the message it produce only message digest, it is not producing the fully encrypted data. At the end of the process the sender sends the original data along with this digital signature. There is no security for the original message [13]. The hacker may hack the message and separate the message from the signature. The private key is also known to the sender so it is not secured, because the sender uses the common encryption algorithm for encryption.

2.2 Proposed Digital Signature Scheme

In the proposed scheme the hash function will be modified to very high secured level, the user private key also modified. In the existing scheme the plain text (original Message) will be added to the digital signature finally [13]. The proposed system encrypts the original message twice using two different algorithms. This is not only authenticity and integrity but the scheme is highly secured.

2.3 Proposed Hash Function

The proposed hash algorithm considers the plain text as 128 bit fixed length, but it separates the blocks by 16 bit. The proposed hash function has three processing steps: pre-processing, processing and output.

i) Pre-process is used to prepare the message into process as follows:

   a) Padding: This process ensure the message in the form of 16 bit chunks.
   b) Parsing: 16 bits is processed into 8 or 4 bit message.

Before the beginning of hash function, the initial hash value is set by H0. The hash can represent the eight 16 bit data. A,B,C,D,E,F,G,H

ii) Processing: Depends up on the length of the message, the system will increase the security of the message digest. The number of block may be increased. Next the changes have been introduced in round function then to increase the XOR operation to make the

structure more complex. The proposed hash algorithm uses functions and constants that are created by XOR operation. After preprocess completed each 16 bit block is processed by the following steps:

Step 1: for I=1 to 8
Message =128 bit dividing by 16

Step 2: initialize the 8 working variable A,B,C,D,E,F,G . and initialize the hash value h(i)

Step 3: A=A+F(B,C,D)+E+G
B=A+F(B,C,D)+E+G
C=F2(DBE)-1
D=F3(EAG)
E=F4(AHF)*B^2
F=F5(CGE)+(DCB)
G=F6(DEF)
H=F7(ABC)XOR(BDC)

Step 4: Assign to the hash value H(i)
H(0)=A
H(1)=B
H(2)=C
H(3)=D
H(4)=E
H(5)=F
H(6)=G
H(7)=H

Step 5: for i=1 to 7
Function(i)
{fact(A+ascii(i)*i)}

2.3.1 *Proposed encryption algorithm*

In excising scheme the original message is directly added to the signature. In our proposed scheme, a message is encrypted using two different kind of encryption algorithms. One is GOST algorithm, the process of GOST[4,5] algorithm is divided the whole message in to 256 bit chunks and it shuffle the chunks using hash function. The another one is IDEA (International Data Encryption Algorithm) algorithm it operates 64 bit blocks and it perform XOR operation in each bits finally add the two encrypted message and form a new encrypted data[6].

2.4 Frame Work For Proposed Scheme

In our proposed system the sender sends encrypted message instead of plain text. The plain text is made into two messages: plain text1 and plain text2. Both two messages are then encrypted by two different algorithms viz. GOST and IDEA. The message digest is also created by new proposed hash algorithm function to prove a high security data. The proposed scheme is given in Figure 2.

2.5 Experimental Results and Analysis

The proposed hashing algorithm produce a message digest for the text and images that is tested based on the time and security[13]. The algorithm has been tested using a computer system with a i3 processor and 2 GB ram. Based on the results the proposed algorithm has less time to generate a message digest when compared with MD5

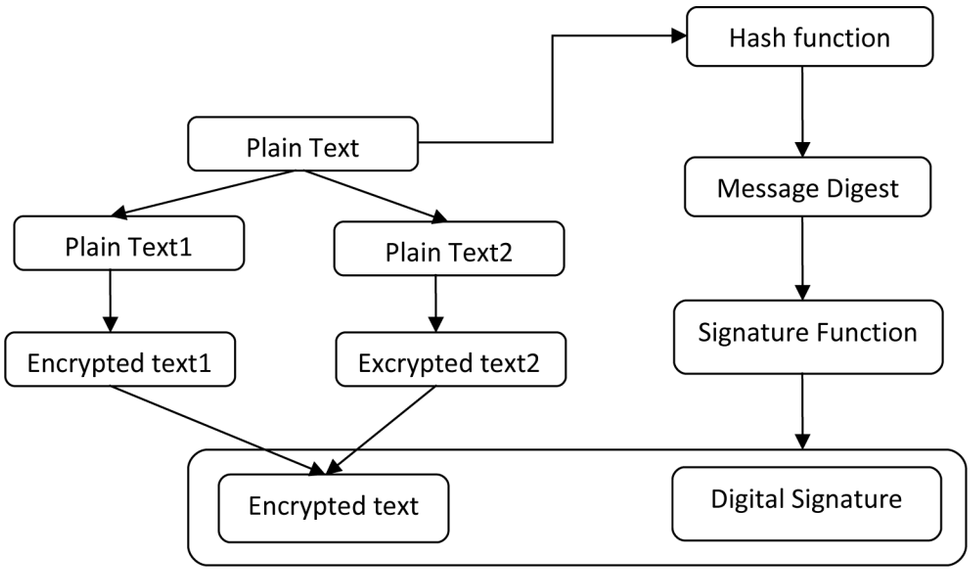

Figure 2. The proposed Digital Signature algorithm.

because the proposed algorithm meet the message with 16 bit blocks.

For a simple message "pop" in the 8 bit ASCII message has length of 24 bits which is "01110000 01101111 01110000" first separate the 24 bits in to two 16 bits values, the second 16 bits having only 8 bits then the algorithm adding another 8 bits as 0's the length of the 16 bits message is shown in Table 1.

The "pop " message has a single 128 bit block. Parse the 128 bit into 16 bit words M1,m2,m3:

01110000011011110111000000000000 . regarding our proposed algorithm the 128 bit message will be divided into 8 words w1,w2…….w8, after separating the words the shuffling will occur based on our algorithm. The MATLAB simulated test vectors for the proposed algorithm. Table 2 shows the hash value of test vector for the simple message in both existing and proposed algorithm.

The data sample is "The five boxing wizards jump quickly" it is given as the first input and in the second time the same data with small modification, for example, changing "jump" into "pump" will be given. The second one is generate a new message digest to compare with the first one[12]. It shows that the message digest value will vary for the input value (Table 3).

The proposed algorithm tested by the sample image Figure 3a,b. We take some sample images like flower and bridge photos to generate the hash value. The images also generated a different message digest like text messages. This shows that the proposed algorithm provides high security and authentication.

Table 1. Preprocessing

P	O	P	8 zeros	16 bits
01110000	01101111	01110000	00000000	01……..00

Table 2. Generating of hash value for test vector

Hash	String	Hash Values
Existing	Pop	01110000011011110111000000000000
Proposed	Pop	10101011000101011101001110001100

Table 3. Generating of hash values

Hash	String	Hash Values
Existing	The five boxing wizards jump quickly	1010101001……..00001
Proposed	The five boxing wizards pump quickly	10100001000……1

Figure 3a. Uuhashed image1.

Figure 3b. Uuhashed image2.

3. Security Analysis of Proposed Algorithm

The effective hash algorithm has a strong ability to persist all kinds of crypto analysis and attackers try to break the algorithm like brute force analysis and collision attacks. The proposed algorithm provides more complexity compared to older algorithms because of it will deal with 16 bit messages [4] This algorithm will encrypt the plain text also; it is not only used for authentication but also for security.

The results from table 1,2,3,4,5,6 define that the proposed algorithm works efficiently in generating digital signature for all kinds of messages.

4. Conclusion

This paper proposed the new hash algorithm for creating message digest and new scheme for encrypting the plain text also. This new scheme uses the known secured algorithms like GOST and IDEA [4,5] algorithms to encrypt the plain text. In this scheme, it provides better security with authentication using different type of files. This scheme provides higher resistance from brute force attacks and other cyber attack. The overall schema of the digital signature is also very effective compared to all other digital signatures. In this proposed algorithm the plain text also encrypted with two major cryptography algorithms[13] offering high protection to the plain text.

Table 4. Hash computation existing and proposed algorithm for flower image

Hash algorithm	Hashing time in seconds	Message digest
Existing	26.78	21d12dff5ad5fdf2df….5
Proposed	21.07	14df2df5de5w3w3ww ….7

Table 5. Hash computation existing and proposed algorithm for bridge image

Hash algorithm	Hashing time in seconds	Message digest
Existing	30.302	7e4t4g4445s989w6……e
Proposed	28.257	7er8er5er7er5wer5er555…..r

Table 6. Security Analysis

Hash Algorithm	Brute Force	Complexity	Original Message
MD4	YES	2^40	YES
MD5	YES	2^50	YES
PROPOSED	NO	2^80	NO

5. References

1. Ministry of Science, Technology and Innovation, Malaysia, "National Cyber Security Policy: The Way Forward," Federal Government Administrative Centre. 2006.
2. UK Office of Cyber Security, "Cyber Security Strategy of the United Kingdom : safety, security and resilience in cyber space" Office of Public Sector Information, Information Policy Team, 2009.
3. United State, Executive Office of the President "Cyber Space Policy Review: Assuring a Trusted and Resilient Information and Communication Infrastructure," United State, Executive Office of the President, 2009.
4. Ganeshkumar, K., Arivazhagan, D. and Sundaram, S. Strategies of cybercrime: Viruses and security sphere. J. Acad. Indus. Res. 2013; 2(7), 397-401.
5. K. Ganeshkumar* et al., "Advance Cryptography Algorithm for Symmetric Image Encryption and Decryption Scheme for Improving Data Security" J.Acad.Indus 10(2), 563:566
6. O. Mikle, "Practical attacks on digital signatures using MD5 message digest.", Cryprology ePrint Archive, report 2004; p.356.
7. Q. Sun and S. F. Chang, "A secure and robust digital signature scheme for JPEG2000 image authentication." Multimedia, IEEE Transactions on 2005; 7(3),480-494, 2005.
8. R. Cramer and V. Shoup, "Signature schemes based on the strong RSA assumption." ACM Transactions on Information and System Security (TISSEC) 2000; 3(3), 161-185.
9. A. Noore, "A secure conditional access system using digital signature and encryption". Consumer Electronics, ICCE. 2003 IEEE International Conference on, IEEE, 2003.
10. J.Stern, D. Pointcheval, "Flaws in applying proof methodologies to signature schemes." Advances in CRYPTO, 2002; 215-224.
11. M. Aydos, T. Yantk, "A high-speed ECC-based wireless authentication on an ARM microprocessor". Computer Security Applications, ACSAC'00. 16th Annual Conference, IEEE. 2000.
12. M. Shah, A. R. Swaminathan, "Privacy-preserving audit and extraction of digital contents." Cryptology ePrint-Archive, Report 186, 2008.
13. J. Ding, B. Y. Yang, "New differential-algebraic attacks and reparametrization of rainbow". Applied Cryptography and Network Security, Springer, 2008.