KNOWLEDGECUDDLE PUBLICATION

International Journal of Computer Engineering and Science, August- 2014

Secure Digital Signature Schemes based on Hash Functions

PATEL PRACHI PRAVINKUMAR
M.E.(C.E.), student
B.V.M.Engineering College
V V Nagar
prachi.patel1105@gmail.com

ABSTRACT: ***One of the major challenges facing consultants today is maintaining a level of knowledge of leading and emerging technologies, beyond the superficial or buzzword level. We need to develop a level of understanding that allows us to communicate effectively with both suppliers and customers.Digital signature scheme is a fundamental cryptographic tool which allows one to sign an electronic message and later the produced signature can be verified by the owner of the message. This paper presents a digital signature scheme and discusses the security aspects of proposed digital signature scheme. This paper provides a literature review and analysis of the security systems and the emphasis is on digital signature, hashed message algorithm.***

Keywords:*Digital signature, Hashed message algorithm, MD5 Algorithm, Public key encryption, SHA2 Algorithm.*

---

1. Introduction

Digital signature is a sort of Cryptography. Cryptography means keeping communications private. It is a practical art of converting messages or data into a different form, such that no one read them without having access to the 'key'.
Along with the thriving improvement of the technologies communication and information, systems of paper-based workflow is quickly substituted by the electronic-based medium in which all information and forms are digitally procedure such as e-government and e-commerce. In these systems, it is very significant to protect the sensitivity and security of digital object from malicious.

2. Digital Signature And Public KeyEncrypion

2.1 Digital Signature

A digital signature is the electronic equivalent of a handwritten signature, verifying ty of electronic documents. In fact, digital signatures provide even more security than their handwritten counterparts.
More often than not a digital signature uses a system of public key encryption to verify that a document has not been altered.

2.2 Public Key Encryption

Public key encryption (PKE) uses a system of two keys:
a private key, which only you use (and of course protect with a well-chosen, carefully protected passphrase); and a public key, which other people use. Public keys are often stored on public key servers.A document that is encrypted with one of these keys can be decrypted only with the other key in the pair.

Digital signatures can be used anywhere that a system for authenticating data is necessary, i.e. anywhere a handwritten signature could be used.

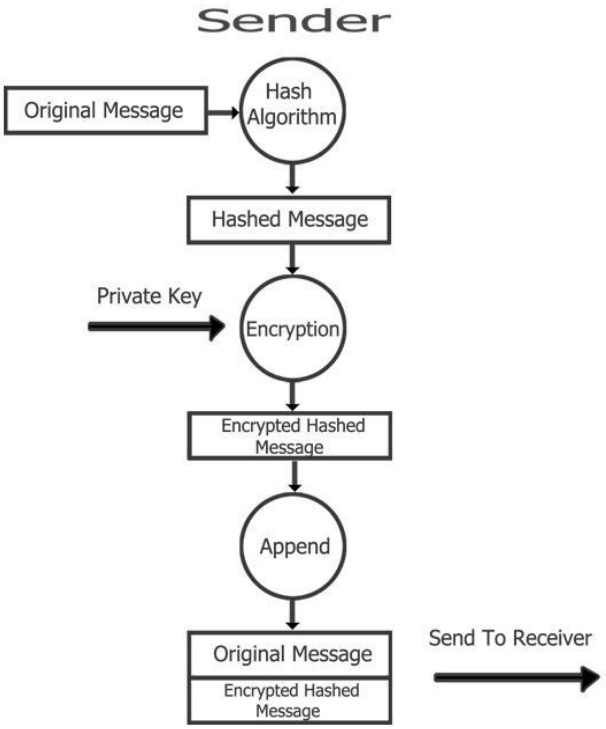

Fig. 1 Process of digital signature for authentication

The public-key cryptosystem gives rise to a new and remarkable idea, which is the concept of digital signature. The digital signature is the electronic analog of the handwritten signature. A signer can digitally sign a document with his/her secret key (Private Key), and generates a signature on that document as shown in Figure 1. Then, he/she sends the generated signature, a document and his\her public key to any verifier. Therefore, a verifier can check the validity of the signature with the corresponding public key(Figure 2).any involved party must register his public key with a central authority, which is known as the Certificate Authority.
Therefore, this cryptosystem is known as a certificate-based public key cryptosystem.

In a classic encryption system, when two parties (A is a sender and B is a recipient), they must agree on a particular private key so as to be used in encryption and decryption processes. 'A' can encrypt his message using the secret key and sends the corresponding cipher text to 'B'. The cipher text should be produced in such a way that any unintended receiver could not determine the original message. Then, 'B' can retrieve the original message by performing an inverse transformation of the cipher text using the same key. The triple algorithms (a key generation, encryption, and decryption) are called a private key encryption system, which should be efficient and secure.

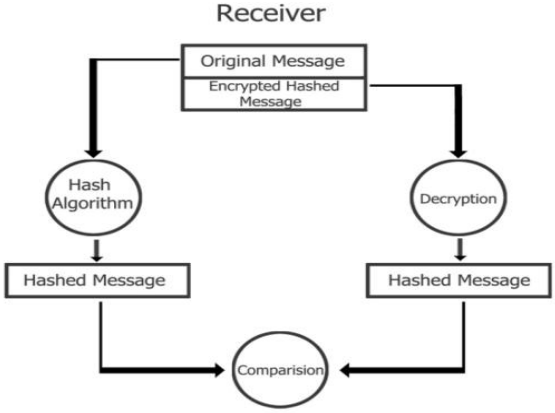

Fig.2 Verification of Digital Signature on the Receiver Side

3. COMPARISION OF HASH ALGORITHM IN DIGITAL SIGNATURE

Cryptographic hash functions is further used for digital signatures. In verification of the authentication of the data, the sender and the receiver compare the hash code and checks if it is genuine. The message is authentic when the message retrieved by the receiver is similar to the messages originally signed. Any changes to the data will affect the hash code which is sent with the data.

3.1 MD5 Algorithm

MD5 algorithm operates on a 128-bit state, divided into four 32-bit words, denoted A, B, C and D. These are initialized to certain fixed constants. The main algorithm then uses each 512-bit message block in turn to modify the state. The processing of a message block consists of four similar stages, termed rounds; each round is composed of 16 similar operations based on a non-linear function F, modular addition, and left rotation. Figure 3 illustrates one operation within a round. There are four possible functions F.

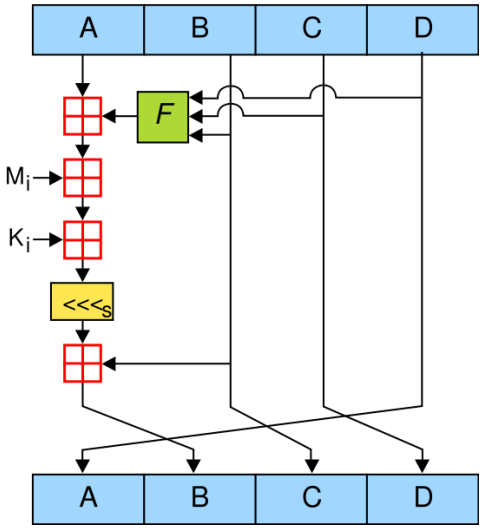

Fig. 3 One Operation of MD5 Algorithm

$$F(B,C,D) = (B \wedge C) \vee (\neg B \wedge D)$$
$$G(B,C,D) = (B \wedge D) \vee (C \wedge \neg D)$$
$$H(B,C,D) = B \oplus C \oplus D$$
$$I(B,C,D) = C \oplus (B \vee \neg D)$$

$\oplus, \wedge, \vee, \neg$ denote the XOR,AND,OR and NOT operations respectively.

3.2 SHA-2 Algorithm (Secure Hash Standard)

SHA stands for Secure Hash Algorithm. SHA-2 includes an outstanding number of changes from its predecessor, SHA-1. SHA-2 is a set of cryptographic hash functions (SHA-224, SHA-256, SHA-384, SHA-512) which was designed by the National Security Agency (NSA) and was published in 2001 by the NIST as a U.S. Federal Information Processing Standard .SHA-2 is similar to the SHA-1 algorithm, these attacks have not been successfully extended to SHA-2. A new hash function, SHA-3, was selected by The NIST hash function competition in 2012.

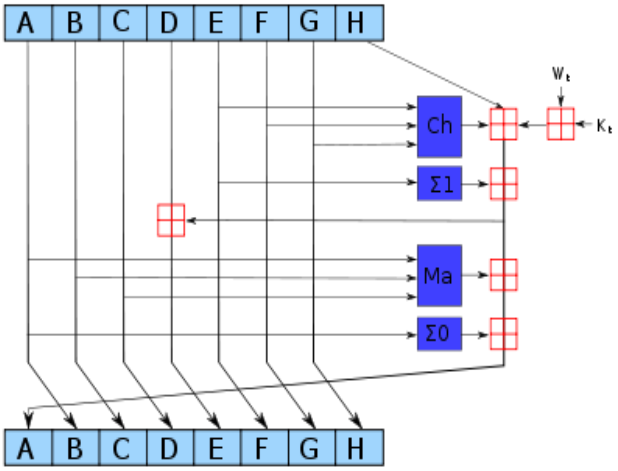

Fig.4 Iteration in a SHA-2 Family Function

$$Ch[E,F,G] = [E \wedge F] \oplus [\neg E \wedge G]$$

$$Ma[A,B,C] = [A \wedge B] \oplus [A \wedge C] \oplus [B \wedge C]$$

$$\sum_0 (A) = [A \ggg 2] \oplus [A \ggg 13] \oplus [A \ggg 22]$$

$$\sum_1 (E) = [E \ggg 6] \oplus [E \ggg 11] \oplus [A \ggg 25]$$

The bitwise rotation uses different constants for SHA-512. The given numbers are for SHA-256. The green symbol is an addition modulo 232 in Figure 5, SHA-1 and SHA-2 are the secure hash algorithms which are required by law to be used in certain U.S. Government applications , including the usage within other cryptographic algorithms and protocols in order to protect sensitive unclassified information. FIPS PUB 180-1 also favored adoption and use of SHA-1 by private and commercial organizations. SHA-1 is not used for most government applications.

3.3Comparison of Hashed Algorithms(MD5 and SHA2)

The size of the output MD5 algorithm is 32 bytes and SHA-2 is 64 bytes. In the first step of processing, useless elements should be added to its length will be a ratio of 512. This is done by adding both 1 bit and adequate 0 bits to the end of the message. Then, the actual length of the message in the format of 64 bits should be O Red in the last 62 bits in order that the length of the message is involved in the calculation of hashed message, Because of the output, these algorithms are constant and their time of complex thus equals O (n).

TABLE I
COMPARISON OF HASH ALGORITHM

Algorithm	**Methodology**	**Output**	**Time Complex**	**Performance**
MD5	Divide to 512b, 64 times loop	32B	O(n)	Collision After 2006
SHA2	Divide to 512b, 64 times loop	64B	O(n)	Without collision

Hashed message, the so-called man-in-the-middle attack is important in defying digital signature. A remarkable feature of digital signature is that it cannot be altered once it is signed. Digital signatures are not similar to handwritten signatures as their constancy depends on the signed document.

Then we compared the hashed algorithms in terms of its logical operators and the complexity of the hardware involved as shown in Table II.

TABLE II
COMPARISON OF LOGICAL OPERATIONS, CURRENT STATUS AND HARDWARE COMPLEXITY

Algorithm	**Logical operations**	**Current status**	**Hardware complexity**
MD5	AND,OR,NOT,Rotating shifts	Collision	Medium
SHA2	AND,OR,NOT,Rotatingshifts,XOR	Running	Large

From Table II, the logical operations required for proposed algorithm are OR and XOR compared to other algorithms which required more than four logical operations. The hardware complexity requirement is also lower compared to other algorithms. Hardware complexity contains devices such as Logic Devices, Programmable and Gate Arrays and Application Specific Integrated Circuits.

4. RESULT

Hashed file is called as a sign file and stored as hashed file. During operation, the "signature version" emerges on the screen then the message of entering file name will be printed, and asks the user to enter the path of the file and also opens a file with Rb "only read binary". Then, hashing function is fetched followed by the encoder function which is then converted to hexadecimal, producing a unique code for each file.

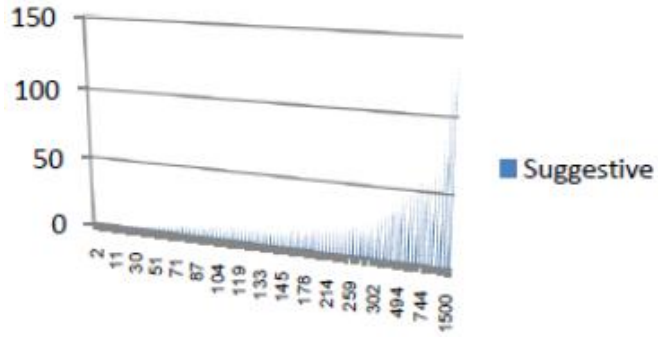

Fig. 5 A Sample of 100 Hashed Files in Digital Signature

Figure 5 shows the size of original file versus size of hashed files. It illustrates the average of hashed size is 8.51% of the size of the original file.

5. CONCLUSION

Digital signatures are supposed to achieve some of the properties for hand signatures, e.g. (Validity and Verifiability). The bandwidth of a subliminal channel is defined as how many bits of covert message can be

transmitted through such a channel in one session of protocol run. It measures the capacity of the subliminal channel in conveying hidden information. Testing new algorithms showed that its hashed file size is 4% reduction of the original file in messages with size lower than 1600 bytes.

REFERENCES

[1] Secure Digital Signature Schemes Based on Hash Functions.International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-2, Issue-4, March 2013

[2] A Method for Obtaining Digital Signatures and Public- Key Cryptosystems R.L. Rivest, A. Shamir, and L. Adleman

[3] http://cs.wellesley.edu/~cs310/lectures/digit_signatures_slides_handouts.pdf.cs.wellesley.edu

[4] Mohammad Amir, JarrarAhmed , Sham Bansal, Ashish Kumar Garg, Man Singh, Digital Signature Scheme Using Two Hash Functions, International Journal of Science and Research (IJSR).

[5] Yan-Chun Wang,Han-Xiong Fang and Ying Xia, Research and Application of Digital Signature Based on Elliptic Curve Cryptosystem, 2012 International Conference on Environmental Engineering and Technology Advances in Biomedical Engineering, Vol.8

[6] ThulasimaniLakshmanan and MadheswaranMuthusamyA Novel Secure Hash Algorithm for Public Key Digital Signature Schemes, The International Arab Journal of Information Technology, Vol. 9, No. 3, May 2012

[7] A Novel Secure Hash Algorithm for Public Key Digital Signature Schemes.

[8] http://www.cs.washington.edu/research/projects/poirot3/Oakland/sp/PAPERS/00044729.PDFwww.cs.washington.edu.S.R

[9] Digital signatures by S.R.Subramanya and Byung K.YI