Digitally Signed Transmission Schema Through MD5

Neelima Naralasetty
Assistant Professor
Department of IT
V.R.Siddhartha Engineering College

Jayalakshmi Gundabathina
Assistant Professor
Department of IT
V.R.Siddhartha Engineering College

Narasimham Challa
Professor&Dean-Computers
Amrita Sai Institute of Science & Technology
Vijayawada,AP,India

Abstract

Internet banking is one of the most modern trends in performing online financial dealings all over the globe. Conveyance of PIN to the customer is the main vital element for the bank. For this system to be done in a most secure, proficient and protected approach between a bank and the customer ONLINE. This paper proposes delivery of PIN through ONLINE by digitally signed transmission schema implemented through message digest algorithm MD5 using asymmetric encryption and decryption algorithm RSA to ensure or guarantee message integrity and confidentiality at sender's side and examine the same at the receiver's side for verification.

1. Introduction

Today we are living in the age of Information Technology. In this era of IT, every transaction goes online. We need to provide security to the message being sent to the receiver. Data being received by the receiver give assurance that data integrity and confidentiality is maintained. Cryptography provides such security for data transmission between sender and the receiver [1]. Message integrity and confidentiality are the processes of ensuring that the data reached the receiver without any variations and no tampering by any third party. To achieve these processes, there are many approaches. One such approach is using message digest algorithm with a digital signature encrypted on it by using an asymmetric algorithm

2. Message Digest Algorithms

Message digest functions or hash functions produce hash values of fixed length by taking plain text as input values of arbitrary length [2].The mainly used message digest algorithms namely are MD4, MD5, and SHA-1.

- MD4 message digest algorithm takes input value of arbitrary length and produces 128-bit output. The MD4 algorithm is ideal for digital signature applications where a large file can be securely "compressed" before being signed with any public-key cryptosystem [3].
- MD5 message digest algorithm is an extension of MD4, when compared it offers much more security assertion [4].
- Secure Hash Algorithm (SHA-1) is a one-way hash algorithm produces 160-bit output and used to create digital signatures [5].

3. Digital Signature

Digital signature scheme is a mathematical scheme for representing the authenticity of a digital message or document. A valid digital signature makes receiver to believe that the message was created by a known sender, and that it was not changed in transit. The mostly used digital signature algorithms are RSA digital signature process and Digital Signature Algorithm.

RSA digital signature process: The RSA algorithm uses modular arithmetic to transform a message into unreadable ciphertext between two parties using public key cryptography technique to send secure and verifiable messages to each other [6].

Digital Signature Algorithm: The DSA key generation has two phases where, the first phase involves sharing of parameters between two users and second phase involves computation of public and private keys for a single user [7].

For our implementation we have considered MD5, which produces the hash function or finger-print of the given plain text, as it is an improvement over MD4.MD5 algorithm takes an input of arbitrary length and produces desires output called the hash code, which is the function of the input message.MD5 algorithm is intended for digital signature applications where a large file must be compressed in a sequence manner before being encrypted with a private key [4].

Digital signature is of signing a message document electronically for verification by the receiver that the received document is from the person, from whom he is expecting and no other person can sign the document except by the sender [8]. For electronically signing the document the sender has to encrypt with his private key they obtained message digest, where the message digest encrypted with any of the public key algorithms is known as digital signature. Because only the sender knows the private key, sender himself produced a valid signature. A hacker cannot use the public key to come up with a correct encrypted value that would authenticate properly.

Inorder to encrypt the message digest, public key cryptography algorithm such as RSA which facilitates two keys one private and public key for encryption and decryption. As symmetric algorithm provides the single secret key both for encryption and decryption which minimizes the security intensities.

4. Framework Outline

In this paper, we were constructing the framework for netBanking system. NetBanking allows customers of particular bank to make financial transactions on a secure website operated by the bank [9]. To access online banking, the customer would go to the bank's website, and enter his customer id and password. Traditional method for sending password to customer is by postal envelope; here we propose a novel method of sending a password online in a secured way.

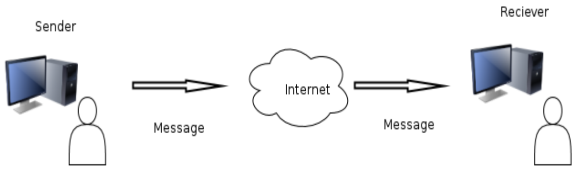


Fig 1: Internet Banking Process

5. Proposed System

The proposed system methodology involves, digital signature should be imposed on the sender side i.e., bank and the receiver i.e., customer should verify the message for authentication.

Procedure at sender's side

1) Generate the hash value of the message M to be sent to the customer.

$$H=MD5\ (M)$$

2) Encrypt the obtained message digest by private key (e) of the sender I.e., bank to produce digital signature (DS)

$$DS=MD\ e \bmod n$$

3) Send the original message M along with the generated digital signature (DS) to the receiver.

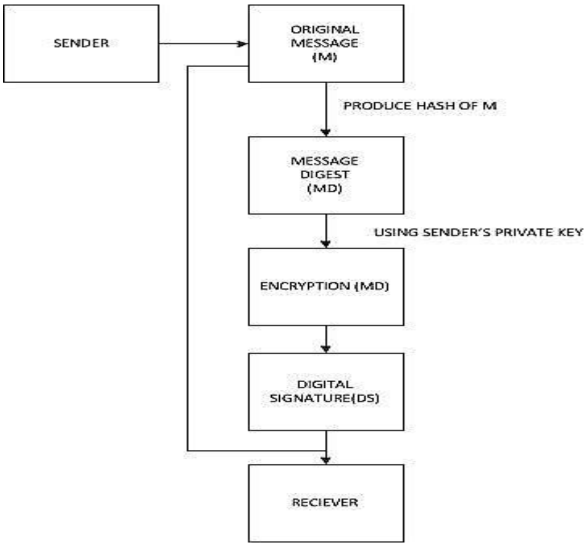


Fig 2: Sender Side Procedure

Procedure at receiver's side:

1) Customer uses the same MD5 algorithm to calculate the message digest of the receiver message.

H1=MD5 (M)

2) Receiver uses public key (d) to decrypt the digital signature.

H2=DS d mod n

3) Compare H1 and H2

4) If H1 equals H2, then it is proved that message integrity is achieved. Otherwise it means that the message received by the receiver is altered. And privacy is also achieved since the sender is encrypting the message digest with his private key and this private key is known only to the sender.

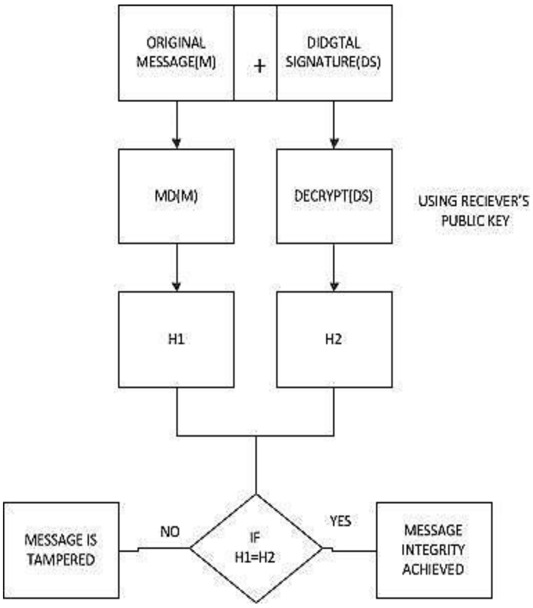
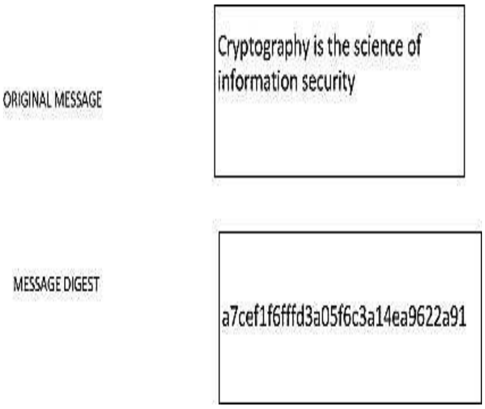


Fig 3: Receiver Side Procedure

6. Implementation Procedure

Senders' side:

For instance, a plain text message is tested for achievement of message integrity and privacy. First, a hash value is generated for the taken plain text message.



ORIGINAL MESSAGE

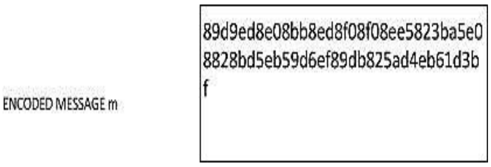
Cryptography is the science of information security

MESSAGE DIGEST

a7cef1f6fffd3a05f6c3a14ea9622a91

Fig 4: Message Digest

Before encryption, for RSA algorithm implementation the message digest is encoded using base 64 encoding scheme as

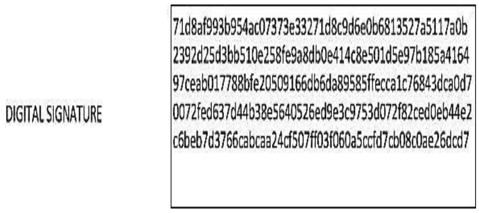


ENCODED MESSAGE m

89d9ed8e08bb8ed8f08f08ee5823ba5e0
8828bd5eb59d6ef89db825ad4eb61d3b
f

Fig 5: Encoded Message

Second, encrypt the generated ‘m’ with senders’ private key to obtain digital signature, using Ciphertext: c = m^e mod n



DIGITAL SIGNATURE

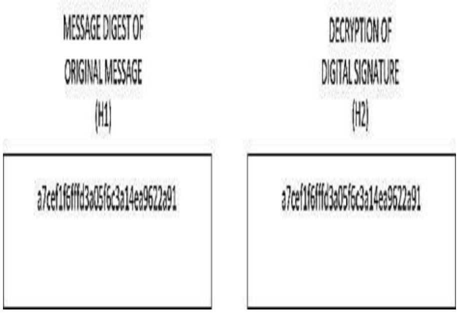
```
71d8af993b954ac07373e33271d8c9d6e0b6813527a5117a0b
2392d25d3bb510e258fe9a8db0e414c8e501d5e97b185a4164
97ceab017788bfe20509166db6da89585ffecca1c76843dca0d7
0072fed637d44b38e5640526ed9e3c9753d072f82ced0eb44e2
c6beb7d3766cabcaa24cf507ff03f060a5ccfd7cb08c0ae26dcd7
```

Fig 6: Digital Signature

Finally, the original message along with the digital signature is sent to the receiver.

Receivers’ side:

The digital signature along with the original message is received by the receiver. At this side, the receiver will generate the message digest (H1) for received original message and also decrypts the digital signature (H2).If H1 equals to H2 ,it is confirmed that the message received by the receiver is not hacked and message integrity as well as privacy is also attained.



MESSAGE DIGEST OF ORIGINAL MESSAGE (H1)

```
a7cef1f6fffd3a05f6c3a14ea9622a91
```

DECRYPTION OF DIGITAL SIGNATURE (H2)

```
a7cef1f6fffd3a05f6c3a14ea9622a91
```

Fig 7: Message Integrity verification

This procedure can be implemented for delivering PIN to the customer in netBanking system since message integrity and privacy are achieved using MD5 and RSA algorithms together.

7. Conclusion

Delivery of PIN to the customer online in internet banking by maintaining data integrity and confidentiality is most essential transaction that is to be performed between a bank and a customer. Both the financial institution and the customer should convince that the message conveyed is only known to sender and the receiver. In this paper we proposed and implemented asymmetric algorithm for encrypting the calculated hash function and digitally signing the document to generate digital signature to maintain data integrity and privacy of the message being sent. In future our proposed work can be extended.

8. References:

[1] Stallings, W., 1999, Cryptography and Network Security: Principles and Practices (Prentice Hall, Upper Saddle River, New Jersey).

[2] Priteshwar Nath Sallam, Jitendra Agrawal, Santosh Sahu," A New Approach 160-bit Message Digest Algorithm", International Journal of Computer Applications (0975 – 8887) Volume 38– No.5, January 2012

[3] R.Rivest," The MD4 Message Digest Algorithm",CRYPTO '90 Proceedings of the 10th Annual International Cryptology Conference on Advances in Cryptology Pages 303-311 Springer-Verlag London, UK ©1991

[4] R. Rivest, "The MD5 Message-Digest Algorithm," RFC 1321,MIT LCS & RSA Data Security, Inc., April 1992.

[5] Kimmo Jarvinen, “Design and Implementation of a SHA-1 Hash Module on FPGAs”,November 2004.

[6] Chong Fu ,Zhi-Liang Zhu , “An Efficient Implementation of RSA Digital Signature Algorithm”, Wireless Communications, Networking and Mobile Computing, 2008. WiCOM '08. 4th International Conference on October 2008.

[7] Kitsos P., Sklavos N., and Koufopavlou O., “An Efficient Implementation of the Digital Signature Algorithm,” in Proceedings of IEEE International Conference on Electronics Circuits and Systems (ICECS’02), Croatia, vol.3, pp. 1151-1154, September 15-18, 2002.

[8] R. Nagpal, “ An Introduction to Digital Signatures”, Asian School of Cyber Laws in 2008.

[9] Akinci S, Aksoy S, Atilgan E (2004). “Adoption of internet banking among sophisticated consumer segments in an advanced developing country”, Int J. Bank Mark. 22 (3):212-32.