International Journal of Advanced Technology & Engineering Research (IJATER)
National Conference on Recent Trends in Science, Technology & Management (NCRTSTM-2018)

RECENT TRENDS ON DIGITAL SIGNATURE FOR INTERNET SECURITY

T. K..Jena, Asst. Prof. in Mathematics, Dept. of BSH , GIET, Bhubaneswar.

Abstract

For secure communication over open networks, the digital signature technique is essential. Digital signatures are being used in secure e-mail and credit card transactions over the Internet. It has varieties of applications in order to ensure integrity, authenticity and confidentiality of the message. This paper gives a concrete idea how a message is encrypted with digital signature and get verified . In this paper we study digital signature and its different digital signature algorithm for internet security[5].

Keywords: Cryptography, Digital Signature, RSA

1. Introduction

In our everyday life internet became an integral part. Security is an important term in this regard. If serious attacks occurs communication, transaction and other important functions will be affected.

Following are some security requirements which must be taken into consideration during any type of communication through internet :

- **Integrity** : There should be no modification done during transmission from sender to reciver.
- **Confidentiality:** The protection of data from unauthorized user. Or providing security to the data send through network.
- **Authenticity:** Access permission.
- **Non-repudation:** Preventing from denial of service attack.
- **Access Control:** Preventing unauthorized access to resource.

If someone changes one’s document and pretending to be original person, it does not validate. A malicious person can copy one’s signature in their own document illegally, but in digital signature the intruder cannot do this.

A digital signature is the electronic equivalent of physical signature and is based on public key cryptosystem .It is proposed by Whitefield Diffie and Martin Helman in 1970 [1].

As in the case of physical signature, a digital signature is used to validate the authenticity of the message. The message authentication holds true if the person capable of generating a valid digital signature. Digital signature must be a function of sender’s private key and the message being sent. Digital signature verification process may be performed by any party. Therefore digital signature verification must be a function of sender’s public key [1].

For a given message ‘x’ , the protocol for transmitting a message between two parties Alice and Bob are:

- Alice and Bob agree on digital signature scheme
- Bob transmit his public key to Alice .
- Bob uses his private key and the digital signature signing function to sign the message ‘x’ gives the digital signature ‘y’.
- Bob transmit the message ‘x’ and the digital signature ‘y’ to Alice .
- Alice verifies the digital signature ‘y’ for the message ‘x’ via digital signature verification function.

The algorithm behind digital signature is difficult so that it is impossible to forge them. There are many digital signature algorithm .Here we will discussing MD5 algorithm , RSA digital signature algorithm and Elgamal digital signature algorithm.

2. Properties:

Properties of Digital Signature can be described as follows for which it has been chosen in Internet Security:-

- The signature must be an authentic one that means the recipient should understand that the signer signed the document.
- The signature to be used for a particular transaction and it cannot be used in another document.
- It must not be unalterable, i.e. the electronic document should not be changed once it is signed by someone.

- Signature should be non-reputable, which means after the signer signs a document then the signer can not claim that he has not signed.

3. Related work

The German digital signature act came into force in the August of 1997 even before the EU's Directive; in fact the directive was adjusted to conform to the German Digital signature Act .

In the December of 1997 the European Union invited a proposal for its electronic signature directive with the purpose of making electronic signatures at least as binding as paper-based signatures in abide to facilitate "free movement of goods and service in the internal market". On the off chance that this yields the right message, then it is obvious that the message was surely scrambled by the private key of an, and consequently just A could have sent it.

Herzberg in a private communication suggested signing the viewing program as well as the document, insuring that the data displayed is viewed as it was intended.

Austria fully implemented the directive in 1999; and concretized the malleability problem by specifying that only data formats may be used which have an "available specification" and which exclude "dynamic changes" or "invisibilities."

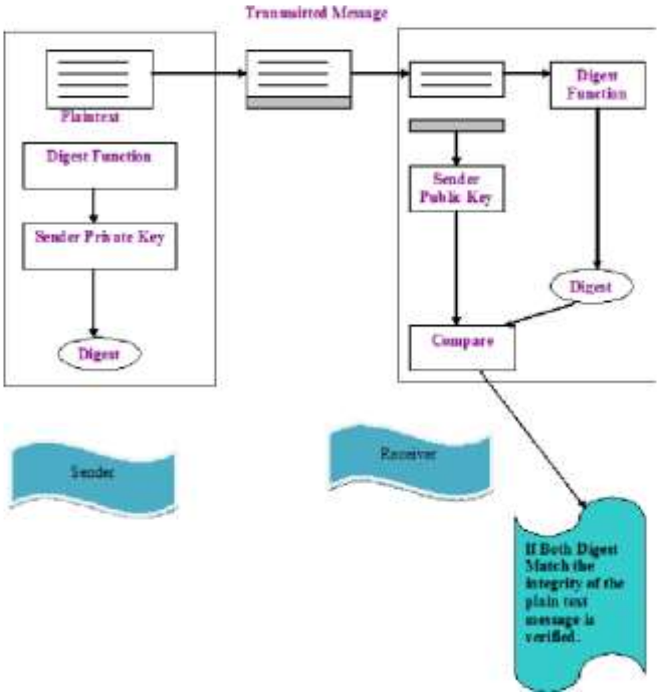
Ulrich Pordesch a German researcher viewed it a risk to have other agencies verify and sign a document, "imbedding and using the schemes in application systems involves considerable risks, in particular, if the signer or the verifier uses an application environment which is maintained, used, or controlled, by other persons or organizations." He used personal signature for authentication purpose.

4. Algorithm

Message Digest: A message digest algorithm takes input of any size and transforms it into a fixed string size. Since a million bytes or more of data is reduced to 128 or 160 bits, information is lost and the transformation is not reversible. A major property of a digest is that given a known input string, it is computationally infeasible to discover a different input string with the same digest. Since public key algorithms are so computationally expensive, the digest of a message is signed rather than the entire message. With a suitable digesting algorithm, the security properties of the message are not affected. The signature on the message still authenticates the message, and a valid signature still verifies that a message hasn't been altered [6].

4.1 MD5 Algorithm

MD5 algorithm was developed by Professor Ronald L. Rivest in 1991. In this algorithm, a message of arbitrary length is taken as an input and produces output as a 128-bit fingerprint or message digest of the input. The MD5 algorithm is intended for digital signature applications, where before being encrypted with a private (secret) key under a public-key cryptosystem such as RSA, a large file must be compressed in a secure manner [2,3].
When the received message from the decryption is matched with the original message and results to be same, we can say that the message has properly received from source to destination without losing it contents and provides all internet security requirements i.e. integrity, confidentiality, non repudiation, and authentication etc .



4.2 RSA Algorithm

RSA, named for Ronald Rivest, Adi Shamir, and Leonard Adleman, the developers of the algorithm, is the best known of all the public key algorithms [3,8].

The R.S.A digital signature scheme is composed of two steps :

- Key setup stage
- Signing and verification stage

- **Key setup stage:**
- Chose two large prime numbers p, q
- Compute $n = p * q$
- Compute $\emptyset(n) = \emptyset(pq) = (p-1)(q-1)$
- Select a random integer b such that $0 < b < \emptyset(n), \gcd(\emptyset(n), b) = 1$
- Compute$a = b^{-1}\ mod\ \emptyset(n)$, where $\emptyset(n)$ is the Euler's $\emptyset$ function .

On completion of key setup stage the public key is $K_{PUB} = (n, b)$ and private key is $K_{PR} = (p, q, a)$

Once the private and public key has been established signing of the message 'x' to form the signature 'y' is performed as :$y = Sign_{KPR}(x) = x^{a}\ mod\ n$ [9].

The verification of signature 'y' is done by computing : $Ver_{KPUB}(x) = y^{b}\ mod\ n$ and compare the result to the message 'x' if $y^{b}\ modn \equiv x$,then verification is successful .Otherwise verification fails .

5. Application

Digital signatures are being increasingly used in secure e-mail and credit card transactions over the Internet. The two most common secure e-mail systems using digital signatures are Good Privacy and Secure/Multipurpose Internet Mail Extension. Both of these systems support the RSA based signature. The money transaction by credit card is done through Secure Electronic Transaction . It consists of a set of security protocol and formats to enable prior existing credit card payment infrastructure to work on the Internet [2,3].

6. Conclusion

The digital signature has become a significant tool in international commerce. Additional businesses will likely use digital signatures in an increasing percentage of their commercial transactions As a digital signature provides the legal elements of a traditional handwritten signature and upgraded security, uprightness, and legitimacy, extra organizations will probably utilize advanced marks in an expanding percentage of their commercial transactions. A secure electronic commerce provides a "paperless" way of transacting business. Electronic communications must be sent in a fraction of a second so that the intruder will not be able to access any data during transmission of electronic data. A digitally signed contract may be e-mailed from a business in India to a recipient in New York in less than one minute[7], while the same document could take a day (or even longer) to arrive if sent through a commercial delivery service.

Appendix

- **Cryptography:** The art of protecting information by transforming it (encrypting it) into an unreadable format, called cipher text. If an user has private key then he can decipher the text. Cryptography systems can be broadly classified into **Symmetric key systems** and **public-key systems.**

- **Symmetric key Cryptography:** This is a system based on the sender and receiver of a message knowing and using the same secret key to encrypt and decrypt their messages. One weakness of this system is that the sender and receiver must trust some communications channel to transmit the secret key to prevent from disclosure. This form of cryptography ensures data integrity, data authentication and confidentiality

- **Public Key Cryptography:** This system is based on pairs of keys called public key and private key. The public key is published and known to everyone while the private key is kept secret with the owner. The need for a sender and a receiver to share a secret key and trust some communications channel is eliminated. This concept was introduced in 1976 by Whitfield Diffie and Martin Hellman.

- **Hash Function:** A cryptographic hash function is a deterministic procedure that takes an arbitrary block of data and returns a fixed size bit string, the (cryptographic) hash value, such that an accidental or intentional change to the data will change the hash value. The data to be encoded is often called the "message", and the hash value is sometimes called the message digest or digest or hash [10].

References

[1] Kain K. Electronic documents and digital signature.

.

[2] Rivest R. The MD5 message digest algorithm 1992 .

[3] Kain K, Smith SW, Asokan R. Digital signatures and electronic documents: a cautionary tale. In advanced communications and multimedia security 2002(pp. 293-307). Springer US.

[4] Kumar MH, Singh DA, An efficient implementation of digital signature algorithm with SRNN public key cryptography. International *Journal of Research Review in Engineering Science and Technology* .,2012

[5] IEEE Security & privacy trends in cryptography

[6] C. Brenn. *Summary of the Austrian Law on Electronic Signatures.* http://rechten.kub.nl/ Simone/brenn.html

[7] W.Diffie and M.E Hellman. New Directions in Cryptography. IEEE Transactions on Information theory, IT-22(6) 644-654 ,November 1976

[8] R.Rivest , A.Shamir, and L.Adleman .A method for obtaining Digital Signatures and Public Key Cryptosystem. *Communication s of the ACM,* 21(2): 120-126, February 1978.

[9] C.P.Schnorr. Efficient Signature Generation by Smart cards. *Journal of Cryptology*, 4(3): 161-174, 1991.

[10] NIST .Secure Hash Standard (SHS) .Federal Information Processing Standards Publication 180-1 , April 1995.

Biographies

T.K.JENA received Msc degree in Mathematics from Utkal University and M.Tech degree in Computer Science from Utkal University .He worked as Research Associate in NISER and presently works as Asst. Prof. in GIET,Baniatangi, Bhubaneswar. His teaching and research areas include Cryptography and Network security, Discrete Structure and Optimization engineering. The author may be reached at
tkjena@gietbbsr.com