APPROACHES TO ENHANCE INFORMATION SECURITY BY USING DIGITAL SIGNATURE

Miss. Garima Singh
Master of Computer Application, NCRD's Sterling Institute of Management Studies
Email: garima1620@gmail.com

Prof. Jayalekshmi K.R
Professor, Department of MCA, SIMS
Email: jlekshmi76@gmail.com

This paper presents overview information about basic concept of Digital Signature using encryption & decryption and its application in today's e- commerce. Digital signature algorithms, technologies, Digital signatures viz. ink on paper signatures are discussed. There are few drawbacks of technology. Applications of digital signature technology are on the rise because of legal and technological developments, along with strong market demand for secured transactions on the Internet. In order to predict the future demand for digital signature products and online security, it is important to understand the application development trends in digital signature technology. Digital signatures play an important role in recent technology for providing essential properties such as integrity, authentication and undesirability.

Keywords:*Digital signature, Cryptography, Group digital signature,authentication, public-private key*

INTRODUCTION

The advent of Information Technology revolutionized the whole world and fortunately India led a leading role and captured global attention. India passed Information Technology Act 2000 (The Act) which came into force on 17-10-2000. The Act applies to the whole of India and even to persons who commit offence outside India. The Act validates 'digital signature' and provides for enabling a person to use it just like the traditional signature. The basic purpose of digital signature is not different from our conventional signature. The purpose therefore is to authenticate the document, to identify the person and to make the contents of the document binding on person putting digital signature.

The arrival of digital signatures, and their legalization by Governments all over the world, has marked a new revolution in the world of electronic transactions. Digital Signatures will make business transactions over the Internet easier, and more reliable for businesses and consumers. Digital signatures are used to present any type of digital data, message or file in the form of numbers or mathematical format. It is a technique which is used for verifying the authenticity of the message and the user. It tells the receiver of the message that it has been sent by the known source and it also confirms that file is secure to be explored. They are most often used for the financial dealings and transactions and also in some scenarios where the delivery of information is required to be confidential.

The purpose of digital signature is the same as the handwritten signature. Instead of using pen and paper, a digital signature uses digital keys (public-key cryptology). Like the pen and paper method, a digital signature attaches the identity of the signer to the document and records a binding commitment to the document. The real value is in avoiding the paper and keeping your data electronic.

In addition to improved security, digital signatures provide the following advantages:

1. No need to print out documents for signing;
2. Reduced storage of paper copies;
3. Improved management and access (anytime/anywhere) of electronic versus paper documents;
4. Elimination of need for faxing or overnight mailing—reduction of cycle time;
5. Improved security of document transmission; and
6. Enhanced management processes outside the ‘‘final signature’’ step.

LITERATURE REVIEW

This section discusses in the research works conducted so far by various researchers to enforce E-Governance security using several types of digital signature schemes.

"A Digital Signature Schemes Without Using One-way Hash and Message Redundancy and Its Application on Key t Agreement13" was published by Hua Zhang, Zheng Yuan, Qiao-yan Wen and in this paper he worked on Digital signature schemes based on public-key cryptosystem are vulnerable to existential forgery attack which can prevented by use of one-way hash function and message redundancy. In paper the authors have proposed a forgery attack over the digital signature scheme proposed by Chang and Chang in

2004. The authors have also shown improved scheme using new key agreement protocol over the Chang and Chang model which actually lacks the use of one-way hash function and redundancy padding

"An Abuse-Free Fair Contract-Signing Protocol Based on the based on RSA Signature15,16" was published by auhor Guilin Wang in this paper the author have proposed a new digital contract signing protocol Digital signature scheme.RSA In this proposed model the trusted third party is only involved when one party is cheating the other or the communication channel is interrupted. Furthermore, this protocol emphasises on the new property i.e. abuse freeness which denotes that in case of unsuccessful execution of the protocol, neither the party can show the validity of the intermediate result to the other.

"The Application of a Scheme of Digital Signature in Electronic Government35" was published by author Na Zhu, GuoXi Xiao in this paper the authors have proposed a scheme of digital signature in electronic government to settle some specific problems such as spilling out secret, forging or denial and so on. Apart from this, a brief analysis regarding security issues of digital signature is also mentioned in this paper.

"A Secured Banking Transaction System using Digital Signature Algorithm48" was published by author Sunil Karforma, Prof. Sripati Mukhopadhyay in this paper the authors have implemented the object oriented concept of digital signature algorithm over banking transactions performed via the public medium *i.e.* internet. Using this object oriented approach, the authenticity and security of the information is achieved, which is exchanged among the electronic participants.

OBJECTIVE

A digital signature is a mathematical technique used to validate the authenticity and integrity of a message, software, or digital document. Digital signatures can be used for many types of documents where traditional pen-and-ink signatures were used in the past. However, the mere existence of a digital signature is not adequate assurance that a document is what it appears to be. Moreover, government and enterprise settings often need to impose additional constraints on their signature workflows, such as restricting user choices and document behavior during and after signing.

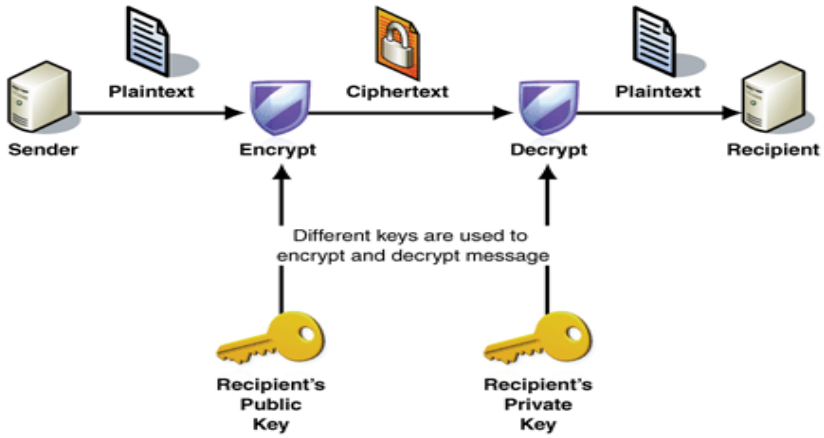
ROLE OF DIGITAL SIGNATURE IN ENHANCING INFORMATION SECURITY

Cryptography: cryptography is the science of information security. Cryptography includes techniques such as microdots, merging word with the images and other way to hide information in storage or transit. However in today's computer centric world, cryptography is most often associated with scrambling plaintext into cipher text called encryption, then back again to plaintext known as description. The two main types of cryptography are secret key cryptography and public key cryptography.

In cryptography the term key refers to a numeric value used by an algorithm to alter information, making that information secure and visible only to individuals who have the corresponding key to recover the information.

Messages are encrypted by the sender using the key and decrypted by the receiver by using the same key.

Fig1: cryptography



This method works well if you are communicating with a limited number of people, but it comes impractical to exchange the secret key with the large number of people. The public key can be freely distributed without compromising the private key, which must be kept secrets by its owner. Because these key works only as a pair, encryption initiated with the public key can be decrypted only with the corresponding private key. The major benefits from cryptography.

Confidentiality: Data confidentiality refers to a situation in which a message is inaccessible to others except the intended recipient. Encryption and decryption ensure confidentiality.

Authenticity: Authentication means verifying the identity of entities that the person with whom you are corresponding are actually the same who they say they are. This is achieved by public and private key generation.

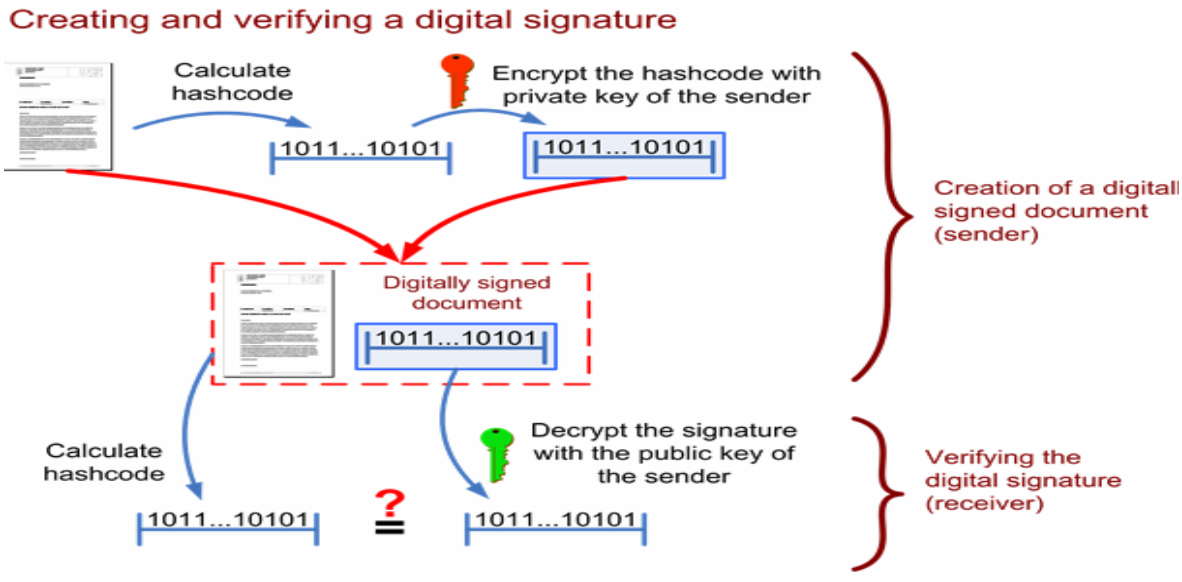
Integrity: Integrity means ensuring that data cannot be corrupted or modified or transaction is unaltered. This can be verified using message digest to message which is transmitted from sender to receiver.

Non-repudiation: It provides security against denial by third unauthorised party which involved in communication. This is provided through public key cryptography by digital signing the document.

Working of Digital Signature -

Assume you were going to send the draft of a certain contract to your business partner in another town. You want to give your lawyer the assurance that it was unchanged from what you sent and that it is really from you. Here then would be the process:

1. You copy-and-paste the contract (it's a short one!) into an e-mail note.
2. Using special software, you obtain a message hash (mathematical summary) of the contract.
3. You then use a private key that you have previously obtained from a public-private key authority to encrypt the hash.
4. The encrypted hash becomes your digital signature of the message. (Note that it will be different each time you send a message.) The process of creating and verifying a digital signal is shown in fig2.



Digital Signatures Vs. Ink On Paper Signatures

• An ink signature could be replicated from one document to another by copying the image manually or digitally, but to have credible signature copies that can resist some scrutiny is a significant manual or technical skill, and to produce ink signature copies that resist professional scrutiny is very difficult.

• A Digital Signature is a combination of 0 & 1s created using crypto algorithms.

Figure 3. Handwritten Versus Digital Signatures

	Handwritten Signature	Digital Signature
Concept		Digital signature using asymmetric encryption / decryption method 13598293948977765830 19293933923939239239 49294959935939993953 99943049384550490594 49395234898434857558
Problem	Reusable	Impossible to reuse

A GROUP DIGITAL SIGNATURE:

Group digital signatures allow members of a group to sign messages on behalf of the group ,such that -the verifier of the signature can check, that the signature is a valid group

signature but cannot discover which group member made it. In case of dispute at rusted authority, called group centre or the group member together can identify the signer.

Chaum and van Heyst introduced the concept of group signatures which are a special type of digital signatures .One of the most important properties of digital signature is its ability to sign people's documents in a secure and efficient manner. In digital signature, it is very difficult to forge the signatures in spite of the ease of verifying the validity of the digital signature. Rivest was the first who constructed a digital signature based on number-theoretic assumption. From the viewpoints of verifiers, only a single group public key is needed to verify group signatures. On the other hand, from the viewpoint of the signing group, its internal structure is hidden from verifiers while the signer's identities can be revealed, if necessary. In virtue of these advantages, group signatures have many potentially practical applications, such as e-voting, e-bidding and e-cash etc.

Group signatures have many potentially practical applications, such as e-voting, e-bidding and e-cash etc. technique using a digital signature algorithm and a challenge-response identification protocol is proposed to provide effective authentication. The proposed digital signature algorithm is based on solving quadratic congruence, factorization, and discrete logarithm problems. Based on the public key infrastructure, group members generate their public-private keys first. The designed authority generates the group member's identity code (ID), the group identity mark, and the group secret key. Every group member keeps his/her private key and the ID for signing. These parameters can ensure only members who can make signatures and provide data authenticity and no repudiation for any signer. The challenge-response identification protocol with overlapping-shifting-EXOR logical operations is proposed to ensure the signer to obtain group secret key securely and prevent any signer from making false claims. According to the security analysis, the processing time of the proposed approach is faster than the existing RSA and ElGamal group digital signature systems.

Moreover, the proposed method would be suited to microprocessor-based devices such as smart cards, computer systems, networks and control systems because of its simplicity, confidentiality, and fast processing speed. The digital signature algorithm based on solving quadratic congruence, factorization and discrete logarithm problems is used to correctly identify the signer in the group. The group members first apply this digital signature algorithm to generate their public-private key pairs respectively and register their identities in

the AI. According to enrolled group members' identities, the AI then generates a group secret key in the database for further transmission. Five processes are included. They are:

(1) Public-private key generation by group members

(2) Group identity mark and member identity code generation for group members

(3) The challenge-response identification

(4) Signing Process

(5) Verification Process

LIMITATION AND FUTURE SCOPE

Although the digital signature technique is a very effective method of maintaining integrity and authentication of data, there are some drawbacks associated with this method. They are discussed in this section.

1. The private key must be kept in a secured manner. The loss of private key can cause severe damage since, anyone who gets the private key can use it to send signed messages to the public key holders and the public key will recognize these messages as valid and so the receivers will feel that the message was sent by the authentic private key holder.
2. The process of generation and verification of digital signature requires considerable amount of time. So, for frequent exchange of messages the speed of communication will reduce.
3. When the digital signature is not verified by the public key, then the receiver simply marks the message as invalid but he does not know whether the message was corrupted or the false private key was used.
4. For using the digital signature the user has to obtain private and public key, the receiver has to obtain the digital signature certificate also. This requires them to pay additional amount of money.
5. If a user changes his private key after every fixed interval of time, then the record of all these changes must be kept. If a dispute arises over a previously sent message then the old key pair needs to be referred. Thus storage of all the previous keys is another overhead.
6. Although digital signature provides authenticity, it does not ensure secrecy of the data. To provide the secrecy, some other technique such as encryption and decryption needs to be used.

CONCULSION

In this paper we have been able to verify why the paper documents are getting replaced with the E-document. Digital signature provides public and private keys and so files encrypted with the public key can only be decrypted by the holder of the private key. Apart from the security advantages, this system has been proved to maintain the integrity of the information secured. The system has therefore eliminated the fear of losing vital information. Cryptography is important for more than just privacy, however. Cryptography protects the world's banking system as well. Without the ability to protect bank transactions and communications, criminals could interfere with the transactions and steal the money without trace. Many traditional and newer businesses and applications have recently been carrying out enormous amounts of electronic transactions, which have led to a critical need for protecting the information from being maliciously altered, for ensuring the authenticity, and for supporting non-repudiation. The digital signature is here to stay and it should. The next challenge, however, is making it easier to get one.

REFRENCES

[1] Alok Gupta, Y. Alex Tung, James R. Marsden, "Digital signature: use and modification to achieve success in next generational e-business processes", science direct.

[2]. http://www.digital-signature.com/digital-signaturesoftware-guide

[3]. en.wikipedia.org/wiki/Digital_signature.

[4]. http://www.cse.unr.edu/~bebis/CS477/Papers/Digital Signatures.pdf

[5]. http://www.windowsitpro.com/content1/topic/digitalsignature- technology]

[6]. Roy A., Karforma S., A Survey on EGovernance Security, International Journal of Computer Engineering and Computer Applications (IJCECA). Fall Edition 2011, Vol 08 Issue No. 01, Pp: 50-62, ISSN 0974-4983.

[7]. http://infoscience.epfl.ch/record/177328/files/EFforgeryResilient.pdf