A Comprehensive Study of Cryptography and Digital Signature

Sonia[#1], Dibjot Kaur[#2]
[#1]*IT Department,* [#2]*Computer Science and Application,* [#1]*DAV College Sector-10 Chandigarh,* [#2]*Khalsa College Amritsar*
[#1]*House no. 886, Sector-41A, Chandigarh, India* [#2]*B-264, Ranjit Avenue, Amritsar, India,*
[#1]soniathind04@yahoo.com [#2]dkalra83@gmail.com

***Abstract*— Signature is a mark or sign on a document, commonly used to denote acceptance and approval which is considered adequate to validate for future reference .Thus legal, financial and other documents is determined to be authentic by presence and absence of signatures which makes it most critical in itself. Thus with the advancement in the computerised system where physical paper and ink is replaced with highly advanced electronic data transfer media digital signatures ensures privacy. Digital Signatures is a sort of cryptography which deals with encryption, decryption and authentication of data so as to provide a high level of assurance to the involved parties that the e-signature is genuinely the signer's, and that the electronic document (or the e-contract) is authentic. The environment in which a transaction is made is now changing because of the attractive solution Digital Signatures in which new rules and practises are employed to accompany the latest technology so as to maintain a complete trust between sender and receiver. Basically it provides higher degree of authenticity and integrity as compared to old tedious and labour intensive paper methods. Therefore to make a valid and tamper-proof document, Digital signatures are used widely in both e-commerce and m-commerce transactions.**

***Keywords*— Message security, Cryptography, Digital signature.**

I. INTRODUCTION

The widespread use of computer technology for information handling resulted in the need for higher data protection. The progress in the field of computer networks and Internet is increasing with tremendous volume in recent years. This raises important issue with regards to security. Several solutions emerged in the past which provide security at host or network level. These traditional solutions like antivirus, firewall, spy-ware, and authentication mechanisms provide security to some extends, but they still face the challenge of inherent system flaws, OS bugs and social engineering attacks. Message security provides four principle services: **privacy, authenticity, integrity, no repudiation**. Privacy means that the sender and the receiver expect confidentiality which can be achieved by Cryptography.

II. CRYPTOGRAPHY

Cryptography is the science of information security. The word is derived from the Greek kryptos, meaning hidden. Cryptography can be defined as the conversion of data into a scrambled code that can be deciphered and sent across a public or private network. The science of securely transferring information is known as cryptology and is usually separated into two distinct yet related sciences: cryptography and cryptanalysis.

There are two types of Cryptography

A. Secret key or Symmetric Cryptography

In Symmetric Cryptography the sender and receiver of a message know and use the same secret key to encrypt the message, and the receiver uses same key to decrypt the message. Other names for this type of encryption are secret-key, shared-key, and private-key.

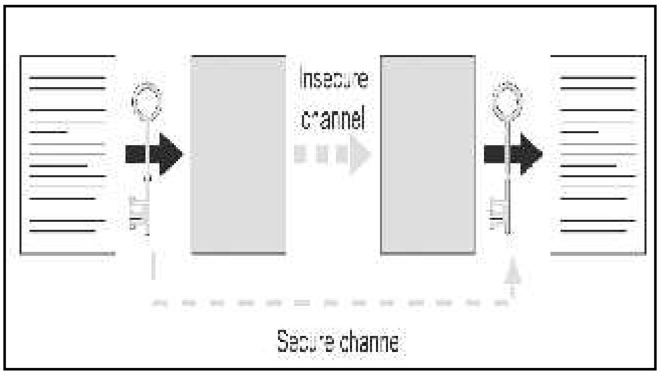

Fig. 1 Example of Conventional Encryption uses a shared key

B. Public key or Asymmetric Cryptography

Asymmetric (or public key) Cryptography involves two related keys, one of which only the owner knows (the 'private key') and the other which anyone can know (the 'public key').

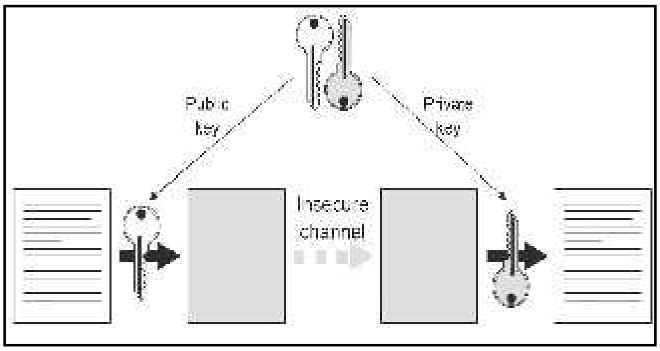

Fig. 1 Example of Public-Key Encryption uses matched public/private pairs

The other services issues Authenticity, integrity and no repudiation can be achieved with the help of fast cryptographic method commonly known as Digital signature

III. DIGITAL SIGNATURE

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’. The message may be converted using a ‘code’ (in which case each character or group of characters is substituted by an alternative one), or ‘cipher’ (in which case the message as a whole is converted, rather than individual characters). It deals with encryption, decryption and authentication.

The authenticity of many legal, financial, and other documents is determined by the presence or absence of an authorized handwritten signature. The signature is an un-forgeable piece of data that asserts that a named person wrote or otherwise agreed to the document to which the signature is attached. A digital signature functions for electronic documents like a handwritten signature does for printed documents. A digital signature actually provides a greater degree of security than a handwritten signature. The recipient of a digitally signed message can verify both that the message originated from the person whose signature is attached and that the message has not been altered either intentionally or accidentally since it was signed. Furthermore, secure digital signatures cannot be repudiated; the signer of a document cannot later disown it by claiming the signature was forged.

In other words, digital signatures enable "authentication" of digital messages, assuring the recipient of a digital message of both the identity of the sender and the integrity of the message.

The digital signature is intended for use in electronic mail, electronic funds transfer, electronic data interchange, software distribution, data storage, and other applications which require data integrity assurance and data origin authentication. The DSA is considered as the standard procedure to generate and verify digital signatures. A DSA digital signature is a pair of large numbers, represented in a computer as strings of binary digits.

Digital certificates - To implement public key encryption on a large scale, such as a secure Web server might need, requires a different approach. This is where digital certificates come in. A digital certificate (also known as electronic credentials or digital IDs) is essentially a bit of information that says the Web server is trusted by an independent source known as a Certificate Authority (CA). CA is a trusted third party organization or company that issues digital certificates. The CA is responsible for guaranteeing that the individuals or organizations granted these unique certificates are in fact, whom they claim to be.

Digital Signatures and hand – written signatures both rely on the fact that it is very hard to find two people with the same signature. Digital signatures are based on mathematical algorithms. These require the signature holder to have two keys (one private and the public) for signing and verification. A verifiable trustworthy entity called certification authority (CA) creates and distributes signatures. The digital signature of a document is a piece of information based on both the document and the signer’s private key. It is typically created through the use of a hash function and a private signing function (encrypting with the signer’s private key). People use public –key cryptography to compute digital signatures by associating something unique with each person. When public-key cryptography is used to encrypt a message, the sender encrypts the message with the public key of the intended recipient. When public -key cryptography is used to calculate a digital signature, the sender encrypts the “digital fingerprint” of the document with his or her own private key. Anyone with access to the public key of the signer may verify the signature.

In practice, public-key algorithms are often too inefficient for signing long documents. To save time, digital signature protocols use a cryptographic digest, which is a one-way hash of the document. The hash is signed instead of the document itself. Both the hashing and digital signature algorithms are agreed upon beforehand. Here is a summary of the process:

1. A one-way hash of the document is produced.
2. The hash is encrypted with the private key, thereby signing the document.
3. The document and the signed hash are transmitted.
4. The recipient produces a one-way hash of the document.
5. Using the digital signature algorithm, the recipient decrypts the signed hash with the sender's public key.

If the signed hash matches the recipient's hash, the signature is valid and the document is intact.

When two messages hash to the same message digest it is called a collision; the collision-free properties of hash functions are a necessary security requirement for most digital signature schemes. A hash function is secure if it is very time consuming, if at all possible, to figure out the original message given its digest. However, there is an attack called the birthday attack that relies on the fact that it is easier to find two messages that hash to the same value than to find a message that hashes to a particular value.

When software (code) is associated with publisher’s unique signature, distributing software on the Internet is no longer an anonymous activity. Digital signatures ensure accountability, just as a manufacturer’s brand name does on packaged software. If an organization or individual wants to use the Internet to distribute software, they should be willing to take responsibility for that software. This is based on the premise that accountability is a deterrent to the distribution of harmful code.

A. Approaches

A variety of approaches have been proposed for digital signature function. These approaches fall into two categories:

1) Direct Approach

A direct digital signature involves only the communication parties (source and destination). It is assumed that the destination knows the public key of the source. A digital signature may be formed by encrypting the entire message with the sender's private key or by encrypting the hash code of the message with the sender's private key.

Confidentiality can be provided by further encrypting the entire message plus signature with either the receiver's public key or a shared secret key. It is important to perform the signature function first and then an outer confidentiality function. In case of dispute some third party must view the message and signature. If the signature is calculated on an encrypted message, the third party also needs access to the decryption key to read the original message. All direct schemes described so far have a common flaw:

The validity of the scheme depends on the security of the sender's private key. If a sender later wishes to deny sending a particular message, he can claim that the private key was lost or stolen and that someone else forged his signature.

Administrative controls relating to the security of private keys can be employed to thwart or at least weaken this ploy. One example is to require every signed message to include a timestamp (date and time) and to require prompt reporting to compromise keys by a central authority. Another threat is that the private key might be stolen from sender X at time T. The opponent can then send a message signed with X's signature and stamped with a time before or equal to T.

2) Arbitrated digital signature:

The problems associated with direct digital signatures can be addressed by using an arbiter. As with direct signature schemes, there are a variety of arbitrated signature schemes. In general terms, these all operate as follows: every signed message from sender X to the receiver Y goes first to the arbiter A, who subjects the message and its signature to the number of tests to check its origin and content. The message is then dated and sends to Y with an indication that it has been verified to the satisfaction of the arbiter. With the presence of arbiter A, there are no chances of a sender X to disowning the message, as is the case with the direct digital signatures.

The arbiter plays a crucial role in arbitrated digital signatures and all parties must have a great deal of trust that the arbitration mechanism working properly. The use of a trusted system might satisfy this requirement.

B. Technology

Digital signatures require the use of public-key cryptography .If you are going to sign something, digitally, you need to obtain both a public key and a private key. The private key is something you keep entirely to yourself. You sign the document using your private key- which is really just a kind of code-then you give the person (the merchant of the website where you bought something or the bank lending your money to buy a house) who needs to verify your signature your corresponding public key. He uses your public key to make sure you are who you say you are. The public key and private key are related, but only mathematically, so knowing your private key. In fact, it's nearly impossible to figure out your private key from your public key.

The sender accomplishes the process of creating a digital signature. The receiver of the digital signature performs the verification of the digital signature.

C. Digital Signature Standard

The National Institute of Standards and Technology has published Federal Information processing standards Publications (FIPS PUBS), known as digital signature standard. The DSS makes use of the Secure Hash Algorithm (SHA) and present a new digital signature technique called the Digital Signature Algorithm (DSA) appropriate for applications requiring a digital rather than written signature. The DSA digital signature is a pair of large numbers represented in a computer as strings of binary digits. The digital signature is computed using a set of rules (i.e., the DSA) and a set of parameters such that the identity of the signatory and integrity of the data can be verified. The DSA provides the capability to generate and verify signatures. Signature generation makes use of a private key to generate a digital signature. Signature Verification makes use of a public key, which corresponds to, but is not the same as, the private key. Each user possesses a private and public key pair. Public keys are assumed signatures for stored as well as transmitted data. Anyone can verify the signature of a user by employing that user's public key. Signature generation can be performed only by the possessor of the user's private key.

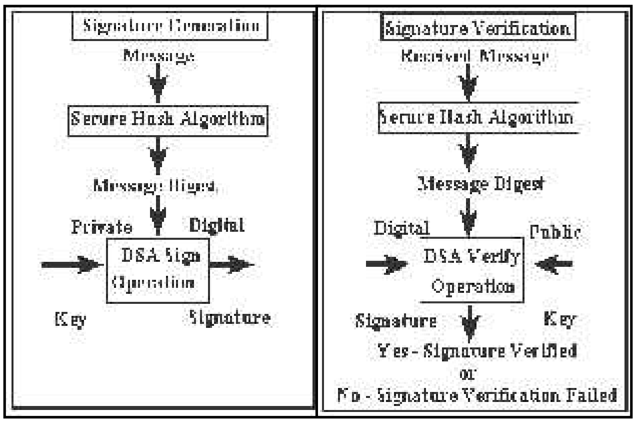

Fig. 3 Example of Using the SHA with the DSA

A hash function is used in the signature generation process to obtain a condensed version of data, called a message digest (Fig3). The message digest is then input to the DSA to generate the digital signature. The digital signature is sent to the intended verifier along with the signed data (often called the message). The verifier of the message and signature verifies the signature by using the sender's public key. The same hash function must also be used in the verification process. The hash function is specified in a separate standard, the Secure Hash Standard (SHS), FIPS 180. Similar procedures may be used to generate and verify signatures for stored as well as transmitted data.

The DSA authenticates the integrity of the signed data and the identity of the signatory. The DSA may also be used in proving to a third party that data was actually signed by the generator of the signature. The DSA is intended for use in electronic mail, electronic funds transfer, electronic data exchange, software distribution, data storage, and other applications which require data integrity assurance and data origin authentication.

The DSA may be implemented in software, firmware, hardware, or any combination thereof. NIST is developing a validation program to test implementations for conformance to this standard.

D. Digital Signature Certificates

It’s not just individuals who need to be authenticated. Servers need to prove their credentials too. That’s where a digital certificate comes into the picture, ensuring that the information sent to and received from a Web server is authentic, and that the Web server in question can be trusted. It can be trusted since it is verified by an independent source known as a certificate authority. The role of the certificate authority is to ensure that the system on either side can be trusted. Digital signature certificates are classified into three main classes.

Class 1: These certificates do not hold any legal validity as the validation process is based only on a valid e-mail ID and involves no direct verification.

Class 2: Here, the identity of a person is verified against a trusted, pre-verified database.

Class 3: This is the highest level where the person needs to present himself or herself in front of a Registration Authority (RA) and prove his/ her identity.

The digital certificate usually contains data such as the owner’s name, company and address, as well as the owner’s public key, along with the certificate’s serial number and validity period. The certificate also includes the certifying company’s ID and its digital signature. Irrespective of the class, pricing is on a per-user basis Costs vary for the three classes of digital certificates

E. Digital Signature Generation

In order to create a digital signature with the message, a process known as hash function which is a mathematical algorithm that creates a digital representation or fingerprint in the form of a hash result or message digest. The hash function generally has a standard length that is usually much smaller than the message but nevertheless substantially unique to it. Hash functions ensure that there have been no modifications to the check since it was digitally signed.

The next step is to encrypt the check and signature. The sender’ signature software transforms the result into a digital signature using the sender private key. The resulting signature is thus unique to both the message and the private key used to create it. Typically, a digital-signature is appended to its message and stored or transmitted with the message. However, it may also be sent or stored as a separate data element, so long as it maintains a reliable association with its message. Since a digital signature is unique to its message, it is useless when wholly disassociated from the message.

F. Validity of Digital Signature

Normally, a key expires after some period of time, such as one year, and a document signed with an expired key should not be accepted. However, there are many cases where it is necessary for signed documents to be regarded as legally valid for much longer than two years; long-term leases and contracts are examples. By registering the contract with a digital time-stamping service at the time it is signed, the signature can be validated even after the key expires.

If all parties to the contract keep a copy of the time-stamp, each can prove that the contract was signed with valid keys. In fact, the time-stamp can prove the validity of a contract even if one signer's key gets compromised at some point after the contract was signed. Any digitally signed document can be time-stamped, assuring that the validity of the signature can be verified after the key expires.

G. Purpose of Digital Signature

1) Signer Authentication

If public and private keys are associated with an identified signer, the digital signature attributes the message to the signer. The digital signature cannot be forged, unless the signer loses control of the private key.

2) Message authentication

Digital signature identifies the signed message with far greater certainty and precision than paper signatures. Verification reveals any tempering since the comparison of hash result shows whether the message is the same as when signed.

3) Non-repudiation

Creating a digital signature requires the signer to use his private key. This alters the signer that he is consummating a transaction with legal consequences, decreasing the chances of litigation later on.

4) Integrity

Digital signature creation and verification processes provide a high level of assurance that the digital signature is that of the signer. Compared to tedious and labor intensive paper methods, such as checking signature cards, digital signatures yield a high degree of assurance without adding resources for processing.

H. Applications of Digital Signature

The scope of Digital Signature is not just limited to exchange of messages. The handwritten signature is commonly used in all kinds of applications to prove the identity of the signer. In the same way, a digital signature can be used for all kinds of electronic records. Any field in which the integrity and validity of the data is crucial, can make use of a Digital Signature. Here we discuss a few of these applications.

1) Electronic Mail:

When we send an e-mail to a mailbox, it is desired that the owner of the mailbox should get the e-mail in its original form. If during transport, the content changes either accidentally or due to intrusion by a third party, then the receiving end should be able to recognize this change in the content. Also no person should be able to send e-mail in the disguise of another person. Both these factors are taken care of by the Digital signature. Any change in the e-mail will affect the message digest and thus the digital signature will be marked as unverified. So the recipient will reject that message.

2) Data storage:

This is one more interesting application of Digital Signature. Suppose a large amount of data is stored on a computer. Only authorized people are allowed to make changes to the data. In such case, along with the data, a signature can also be stored as an attachment. This signature is generated from the data digest and the private key. So if any changes are made in the data by some unauthorized person, then they will get easily recognized at the time of signature verification and thus that copy of data will be discarded.

3) Electronic funds transfer:

Applications like online banking, e-commerce come under this category. In these applications the information being exchanged by the two sides is vital and thus extreme secrecy and authenticity must be maintained. A digital signature can ensure the authentication of the information but, the secrecy should be maintained by using some encryption techniques. So before generating the message digest, the message should be encrypted. Then the digital signature is generated and attached to the message. At the receiving end after verification of signature, the message is decrypted to recover the original message.

4) Software Distribution:

Software developers often distribute their software using some electronic media, for example, the internet. In this case, in order to ensure that the software remains unmodified and its source is genuine, Digital Signature can be used. The developer signs the software and the users verify the signature before using it. If signature gets verified, then only the users can be sure about the validity of that software.

I. Legal Aspects of Digital Signature

In various countries the complete process of using digital signature has been standardized, under the protection of law. The Indian Information Technology Act 2000 (‘Act’) came into effect from October 17, 2000. The Act is by and large based on the United Nations Commission on International Trade Law (UNCITRAL) model law on electronic commerce.

The objective of the Act is to provide for legal recognition of electronic transactions and digital signatures. Section 5 of the Act gives legal recognition to digital signatures. Digital signatures have been legalised in India since 2000. However, since then, hardly any provisions of the Act have been implemented, except for the appointment of the Certifying Authority which took place in 2001.

In India, the Indian IT Act authorises the Controller of Certifying Authorities (CCA) to licence and regulate the working of CAs, who, in turn, issue digital signature certificates for electronic authentication of users.

At present, the organisations acting as licenced CAs are the National Informatics Centre, Customs and Central Excise, Institute for Development & Research in Banking Technology, SafeScrypt, Tata Consultancy Services, MTNL and (n) Code Solutions.

IV. CONCLUSIONS

Although Digital Signatures facilitate many of the desired attributes of electronic commerce such as speed of transactions and reduced paper-work digital signatures are still not a widely-accepted concept in India. Because of the technicalities involved this is very much the norm, except in certain cases where the use of digital signatures has been mandated by law, such as filings with the Ministry of Company Affairs. Though the concept of digital signatures is a powerful tool, it has been difficult to move the concept from theory to reality because of multiple reasons. Some of the reasons include cultural reticence, unequal access to technology, and the lack of an adequate legal and service infrastructure to support such a major shift.

In India, the adoption of digital signatures is still at an early stage. There is nothing new however, in the concept of the seal, it’s the scale and potential of usage that has changed and which must be reflected in the development of international security standards and guidelines. Till this resistance abates, digital signatures will have to struggle for recognition.

REFERENCES

[1] Behrouz A Forouzan, *Data Communication and Networking*.
[2] Andrew S. Tanenbaum, *Computer Networks*, 3rd Edition.
[3] http://en.wikipedia.org/wiki/Digital_signature
[4] http://www.digitalsignature.in