A

Seminar report

on

Digital Signature

Submitted in partial fulfillment of the requirement for the award of degree
Of Computer Science

SUBMITTED TO:

www.studymafia.org

SUBMITTED BY:

www.studymafia.org

Preface

I have made this report file on the topic **Digital Signature;** I have tried my best to elucidate all the relevant detail to the topic to be included in the report. While in the beginning I have tried to give a general view about this topic.

My efforts and wholehearted co-corporation of each and everyone has ended on a successful note. I express my sincere gratitude to ……..who assisting me throughout the prepration of this topic. I thank him for providing me the reinforcement, confidence and most importantly the track for the topic whenever I needed it.

CONTENT

- **Introduction**
- **History**
- **What is Digital Signature**
- **Basic Requirements**
- **How the Technology Works**
- **Approaches**
- **Purpose of Digital Signature**
- **Algorithm**
- **DSA Parameters**
- **Challenges and Opportunities**
- **Application**
- **Drawbacks**
- **Conclusion**

INTRODUCTION

The authenticity of many legal, financial, and other documents is determined by the presence or absence of an authorized handwritten signature. The recipient of the signed document can verify the claimed identity of the sender using the signature. Also, if the sender later repudiates the contents of the document, then recipient can use the signature to prove the validity of the document.

With the computerized message systems replacing the physical transport of paper and ink documents, an effective solution for authentication of the electronic data is necessary. Various methods have been devised to solve this problem, but the use of 'digital signature' is definitely the best solution amongst them.

A digital signature is nothing but an attachment to any piece of electronic information, which represents the content of the document and the identity of the originator of that document uniquely. 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.

When a message is received, the recipient may desire to verify that the message has not been altered in transit. Furthermore, the recipient may wish to be certain of the originator's identity. Both of these services can be provided by the digital signature. A digital signature is an electronic analogue of a written signature in that the digital signature can be used in proving to the recipient or a third party that the message was, in fact, signed by the originator. Digital signatures may also be generated for stored data and programs so that the integrity of the data and programs may be verified at any later time.

Although there are various approaches to implement the digital signature, this report discusses the 'Digital Signature Standard'. It specifies the Digital Signature Algorithm (DSA) which is appropriate for applications requiring a digital rather than written signature. 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.

The first section of this report deals with the basic requirements for using the digital signature. The next sections contain detailed explanation of the process of generation and verification of the digital signature. In addition to this the applications of the digital Signature are also discussed. The report also focuses on some legal aspects of digital signature, with reference to the Information Technology Act. The use of digital signature has been illustrated with an example in a practical scenario.
This report is an attempt to make the readers familiar with the concepts related to the digital signature and give them an idea of usefulness of a digital signature in the world of electronic information exchange.

HISTORY

It is probably not surprising that the inventors of writing, the Sumerians, were also the inventors of an authentication mechanism. The Sumerians used intricate seals, applied into their clay cuneiform tablets using rollers, to authenticate their writings. Seals continued to be used as the primary authentication mechanism until recent times.

Use of signatures is recorded in the Talmud (fourth century), complete with security procedures to prevent the alteration of documents after they are signed. The Talmud even describes use of a form of "signature card" by witnesses to deeds.

The practice of authenticating documents by affixing handwritten signatures began to be used within the Roman Empire in the year AD 439, during the rule of Valentinian III. The subscripto - a short handwritten sentence at the end of a document stating that the signer "subscribed" to the document - was first used for authenticating wills.

The practice of affixing signatures to documents spread rapidly from this initial usage, and the form of signatures (a hand-written representation of one's own name) remained essentially unchanged for over 1,400 years.

It is from this Roman usage of signatures that the practice obtained its significance in Western legal tradition.

What is digital signature

Basically, the idea behind digital signatures is the same as your handwritten signature. You use it to authenticate the fact that you promised something that you can't take back later. A digital signature doesn't involve signing something with a pen and paper then sending it over the Internet. But like a paper signature, it attaches the identity of the signer to a transaction. Having a digital certificate is like using your driver's license to verify your identity. You may have obtained your license from Maryland, for example, but your Maryland license lets you drive in Nevada and Florida. Similarly, your digital certificate proves your online identity to anybody who accepts it.

A digital signature can also be used to verify that information has not been altered after it was signed. A digital signature is an electronic signature to be used in all imaginable type of electronic transfer. Digital signature significantly differs from other electronic signatures in term of process and results. These differences make digital signature more serviceable for legal purposes.

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 creates and distributes signatures. A digital signature is a cryptographic means through which many of these may be verified. 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).

Digital Signatures and hand – written signatures both rely on the fact that it is very hard to find two people with the same signature. 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.

There is a potential problem with this type of digital signature. Alice not only signed the message she intended to but also signed all other messages that happen to hash to the same message digest. 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.

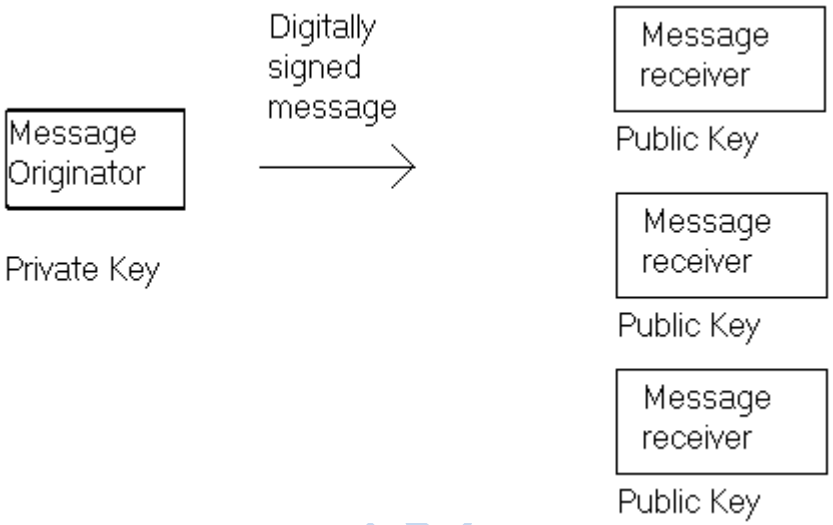
However, there is an attack called the birthday attack that relies on the fact that it is easier to find two messages that hash to the same value than to find a message that hashes to a particular value. Its name arises from the fact that for a group of 23 or more people the probability that two or more people share the same birthday is better than 50%.

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.

BASIC REQUIREMENTS

Any individual who wishes to use the digital signature must have a unique private key for generation of the signature. The recipients who receive digitally signed messages must have the public key, corresponding to the private key used for the generation of the digital signature, for verification of the signature. Also the recipients must obtain the digital signature certificate which acts as a proof of the association between the public key and the private key. Once all these requirements are satisfied, then only the subscriber can use the digital signature.



Private Key.

The private key is one which is accessible only to the signer. It is used to generate the digital signature which is then attached to the message. It is very important to have a unique private key for each user, so that the signature generated by that key for a given message can not be duplicated by any other key.

The security of a digital signature system is dependent on maintaining the secrecy of users' private keys. Users must therefore guard against the unauthorized acquisition of their private keys.

Public Key.

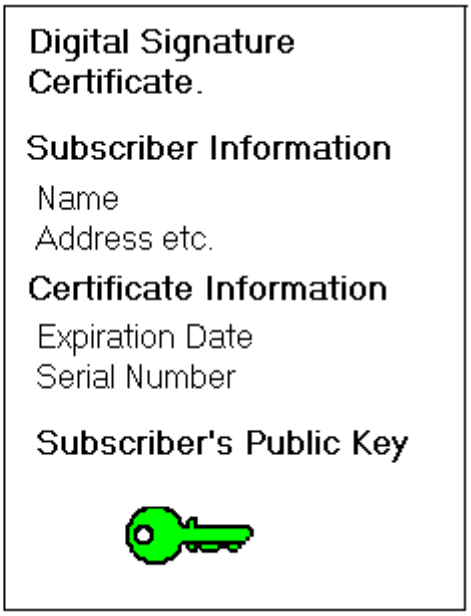
The public key is made available to all those who receive the signed messages from the sender. It is used for verification of the received message. Although the public key is uniquely associated with the private key, there is no recognizable similarity between them. This is done purposefully to avoid discovery of the private key from the public key. Thus the holder of a public key can just verify the message received from the sender. Any person who digitally signs his messages must distribute the public key to the recipients of his messages, so that they can verify the validity of these messages.

Digital Signature Certificate.

A subscriber of the private key and public key pair makes the public key available to all those who are intended to receive the signed messages from the subscriber. But in case of any dispute between the two sides, there must be some entity with the receiver which will allow the receiver of the message to prove that the message was indeed sent by the subscriber of the key pair.

This can be done with the Digital Signature Certificate. This certificate lists the subscriber's public key. So, it acts as a binding between the private and public keys. Any message verified by the public key listed on the certificate is implicitly assumed to be signed and sent by the corresponding subscriber.

A digital signature certificate is issued by the Certifying Authority to the applicants. For obtaining this certificate the applicant must produce the private key and public key pair before the certifying authority. After checking the functioning of the key pair the certifying authority issues a certificate to the applicant.



HOW THE TECHNOLOGY WORKS

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.

APPROACHES

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

- Direct approach
- Arbitrated approach

Direct digital signature:

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.

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.

PURPOSE OF DIGITAL SIGNATURE

- **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.

- **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.

- **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.

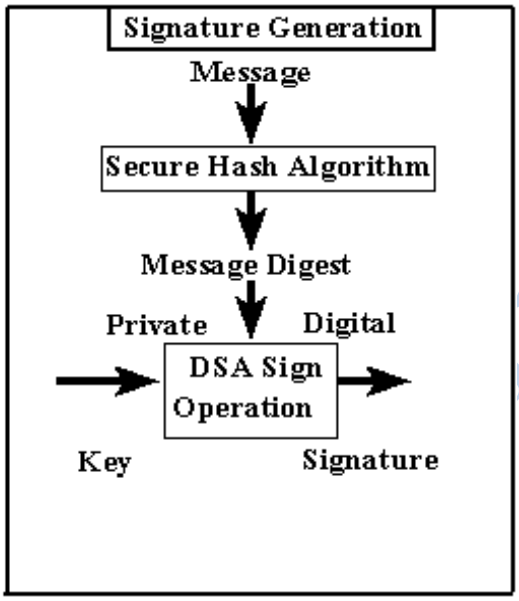
- **Integrity :**

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.

DIGITAL SIGNATURE ALGORITHM

The digital signature algorithm specifies the procedure to generate and verify the digital signature.

Digital Signature Generation.



The above diagram shows the process of Digital Signature Generation. It consists of following steps:-

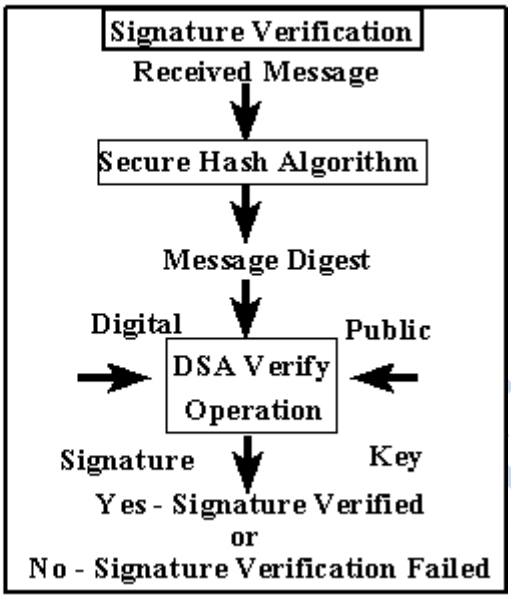
1. The user of Digital Signature can use this facility optionally. So if he chooses to send the message without a signature, then the message is directly send to the other end. But, if he wishes to digitally sign the message, then he is asked for the Private Key by the digital signature Generation system.

2. A Secure Hash Algorithm (SHA) is used in the signature generation process to obtain a condensed version of message, called a message digest. The SHA is such that it generates different message digest for each different message. In other words, no two messages have the same message digest.

3. The DSA sign unit accepts the message digest from the SHA and the private key from the user. Then a digital signature is generated as a function of both, the private key and the message digest. Number of other parameters called as DSA parameters, are also used in this process. These parameters are discussed in details in the next section.

4. Once a signature is generated, it is attached to the original message. Then this message is send to the other end.

Digital Signature Verification.



The above diagram shows the process of Digital Signature Verification. It consists of following steps:-

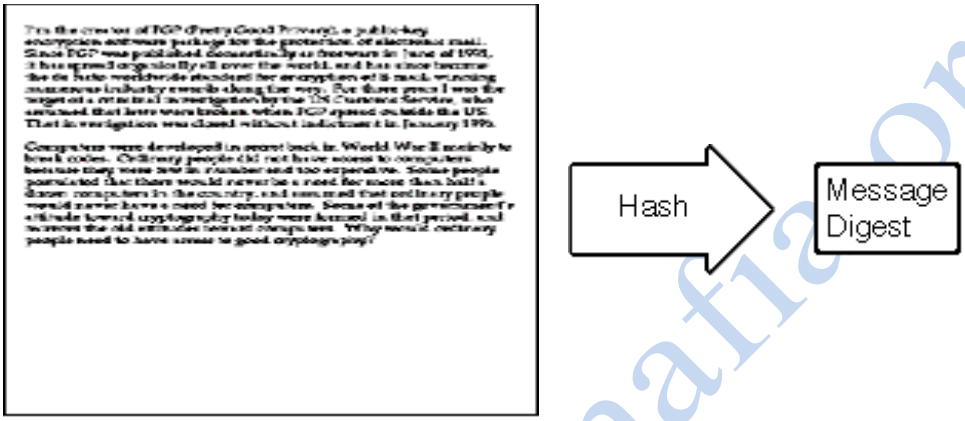
1. A user can receive messages from different senders. Some of them may be using a digital signature and some may not. If a message is not digitally signed then the user accepts it without any verification. But in case of digitally signed message, he can verify the message with the help of public key corresponding to the sender.
2. The received message is fed to the SHA for generation of the message digest. The SHA used by the receiver must be same as that used by the sender. So, if the message content remains unaltered during the transport, then SHA will generate the same message digest.

3. The DSA verify unit accepts the message digest from the SHA and the public key from the receiver. Using the DSA parameters, public key, message digest the received digital signature is verified. If the signature gets verified, then integrity of the message as well as the identity of sender is confirmed. But if it doesn't get verified, then either the message has been corrupted during the transport or the private key used is not matching with the public key. In either case the message is considered invalid and should be rejected by the receiver.

Secure Hash Algorithm

This Standard specifies a Secure Hash Algorithm (SHA), for computing a condensed representation of a message or a data file. When a message of any length $< 2^{64}$ bits is input, the SHA produces a 160-bit output called a message digest. The message digest can then be input to

the Digital Signature Algorithm (DSA) which generates or verifies the signature for the message. Signing the message digest rather than the message often improves the efficiency of the process because the message digest is usually much smaller in size than the message. The same hash algorithm must be used by the verifier of a digital signature as was used by the creator of the digital signature.



The SHA is called secure because it is computationally infeasible to find a message which corresponds to a given message digest, or to find two different messages which produce the same message digest. Any change to a message in transit will, with very high probability, result in a different message digest, and the signature will fail to verify.

DSA PARAMETERS

Specification of parameters.

The DSA (Digital Signature Algorithm) makes use of the following parameters:

1. p is a prime number, where $2^{L-1} < p < 2^{L}$ for 512 <= L <= 1024 and L a multiple of 64.
2. q is a prime divisor of p - 1, where $2^{159} < q < 2^{160}$.
3. $g = h^{(p-1)/q} \bmod p$, where h is any integer with $1 < h < p - 1$ such that

   $h^{(p-1)/q} \bmod p > 1$ (g has order q mod p)
4. x = a randomly generated integer with $0 < x < q$
5. $y = g^{x} \bmod p$
6. k = a randomly or generated integer with $0 < k < q$

The integers p, q, g can be public and they can be common to a group of users. A user's private and public keys are x and y, respectively. They are normally fixed for a period of time. Parameters x and k are used for signature generation only, and must be kept secret. Parameter k must be regenerated for each signature.

Signature Generation.

The signature of a message M is the pair of numbers r and s computed according to the equations below.

$r = (g^{k} \bmod p) \bmod q$ and

$s = (k^{-1}(SHA(M) + xr)) \bmod q$.

The value of SHA (M) is a 160-bit string output by the Secure Hash Algorithm. For use in computing s, this string must be converted to an integer. As an option, one may wish to check if r = 0 or s = 0. If either r = 0 or s = 0, a new value of k should be generated and the signature should be recalculated (it is extremely unlikely that r = 0 or s = 0 if signatures are generated properly).

The signature is transmitted along with the message to the verifier.

Signature Verification.

Prior to verifying the signature in a signed message, p, q and g plus the sender's public key and

identity are made available to the verifier in an authenticated manner.

Let M', r' and s' be the received versions of M, r, and s, respectively, and let y be the public key of the signatory. To verifier first checks to see that $0 < r' < q$ and $0 < s' < q$; if either condition is violated the signature shall be rejected. If these two conditions are satisfied, the verifier computes

$$w = (s')^{-1} \bmod q$$

$$u1 = ((SHA\ (M')\ w) \bmod q$$

$$u2 = ((r')\ w) \bmod q$$

$$v = (((g)^{u1}\ (y)^{u2}) \bmod p) \bmod q.$$

If v = r', then the signature is verified and the verifier can have high confidence that the received message was sent by the party holding the secret key x corresponding to y. For a proof that v = r' when M' = M, r' = r, and s' = s, see Appendix1.

If v does not equal r', then the message may have been modified, the message may have been incorrectly signed by the signatory, or the message may have been signed by an impostor. The message should be considered invalid.

Challenges and Opportunities

The prospect of fully implementing digital signatures in general commerce presents both benefits and costs. The costs consist mainly of:

- Institutional overhead: The cost of establishing and utilizing certification authorities, repositories, and other important services, as well as assuring quality in the performance of their functions.
- Subscriber and Relying Party Costs: A digital signer will require software, and will probably have to pay a certification authority some price to issue a certificate. Hardware to secure the subscriber's private key may also be advisable. Persons relying on digital signatures will incur expenses for verification software and perhaps for access to certificates and certificate revocation lists (CRL) in a repository.

On the plus side, the principal advantage to be gained is more reliable authentication of messages. Digital signatures if properly implemented and utilized offer promising solutions to the problems of:

- Imposters, by minimizing the risk of dealing with imposters or persons who attempt to escape responsibility by claiming to have been impersonated;
- Message integrity, by minimizing the risk of undetected message tampering and forgery, and of false claims that a message was altered after it was sent.

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 generated by the SHA 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.

DRAWBACKS OF USING DIGITAL SIGNATURE

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.

CONCLUSION

Digital signatures are difficult to understand. Digital signatures will be championed by many players that the public distrusts, including national security agencies, law enforcement agencies, and consumer marketing companies. Digital signatures will inevitably be associated with cards. Digital signatures will inevitably be associated with biometric identifiers.

As a result, it appears that digital technology is rapidly becoming pervasive, the public not find this comforting. They will demand explicit privacy protections, far more substantial than the weak and patchy regime that is presently in place.

The protections are also quite inadequate, though promising in some respects. Successful implementation of digital signatures will require far more attention to privacy issues by policy-makers and business interests.