Digital Signatures

[#]Pankaj Kumar Varshney,
[#]Anmol Kukreja, [#]Shivam Dewan
[#]*Institute of Information Technology & Management, Janakpuri, New Delhi, India*
[1]pankaj.surir@gmail.com,[2] anmolkukreja123@gmail.com, [3]shivam377@gmail.com

Abstract*—There are different types of encryption techniques used to ensure the privacy of data transmitted over internet. Digital Signature is a mathematical scheme that ensures the privacy of conversation, integrity of data, authenticity of digital message/sender and non-repudiation of sender. Digital Signature is embedded in some hardware device or also exits as a file on a storage device. Digital Signature are signed by third party some certifying authority. This paper describes the different key factor of digital signature with the working, through various methods and procedures involved in signing the data or message by using digital signature. It introduces algorithms used in digitalsignatures.*

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 nonrepudiation. Just as signatures facilitate validation and verification of the authenticity of paper documents, digital signatures serve the purpose of validation and authentication of electronic documents. This technology is rather new and emerging and expected to experience growth and widespread use in the coming years.

Keywords: *Digital Signature, Validation, Authentication*

I. INTRODUCTION

A digital signature is an electronic analogue of a written signature; the digital signature can be used to provide assurance that the claimed signatory signed the information. In addition, a digital signature may be used to detect whether or not the information was modified after it signed (i.e., to detect the integrity of the signed data). Often-ally digital signature is generated critical consideration when establishing. A signed message that includes the (purported) signing time provides no assurance that the private key was used to sign the message at that time unless the accuracy ofthe time can be trusted. With the appropriate use of 1) timestamps that are digitally signed by a Trusted Timestamp Authority (TTA), and/or 2) verifier-supplied data that is included in the signed message, some level of assurance about the time that the message was signed can be provided. A discussion of the establishment and management of a TTA is outside the scope of thisRecommendation.

Nowadays the speed of business connections is increasing rapidly. In order to be in the frontline of the world competition, companies are adopting new technologies such as web conferences, distant work places, internet banking, & usage of electronic documents. Electronic documents are efficient in commercial, cost and environment perspectives. Electronic signature concept is growing in its popularity, the new wave of electronic office concept will flow over the business world very soon. There are strong drives to replace paper-based document circulation with electronic one, replace handwritten signature with electronic one. However, doing business via internet or signing e-documents require more security, trust, traceability and accountability. The new technology of advanced digital signature has created a base for a secured paperless office. Enforceability of electronic documents & digital signatures allows easily exchange legal electronic documents, reduce the process costs & time connecting with mail and printing. Digital signature provides more authenticity in comparison to handwritten signature [4].

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

Following are some security requirements that must be taken into count during any type of communication through Internet: -

- Integrity: If the message content changes after being sent from the sender, and before reaching to the recipient, then we will take this as a loss of integrity. Hence the message content must not be affected during its travellingtime.

- Availability: As per the principles of availability, resources should be available to authorized persons at all time.

- Confidentiality: It specifies that contents of message are accessible to nobody, except the sender and intended receiver.

- Authentication: It ensures the proof of identity. The sender and the intended receiver of the message must be correctlyidentified.

- Nonrepudiation: Neither sender nor receiver can deny the existence ofmessage.

.

II. CONVENTIONAL AND DIGITAL SIGNATURE CHARACTERISTICS

A conventional signature has the following salient characteristics: relative ease of establishing that the signature is authentic, the difficulty of forging a signature, the non-transferability of the signature, the difficulty of altering the signature, and the nonrepudiation of signature to ensure that the signer cannot later denysigning.

A digital signature should have all the aforementioned features of a conventional signature plus a few more as digital signatures are being used in practical, but sensitive, applications such as secure e-mail and credit card transactions over the Internet. Since a digital signature is just a sequence of zeroes and ones, it is desirable for it to have the following properties: the signature must be a bit pattern that depends on the message being signed (thus, for the same originator, the digital signature is different for different documents); the signature must use some information that is unique to the sender to prevent both forgery and denial; it must be relatively easy to produce; it must be relatively easy to recognize and verify the authenticity of digital signature; it must be computationally infeasible to forge a digital signature either by constructing a new message for an existing digital signature or constructing a fraudulent digital signature for a given message; and it must be practical to ret copies of the digital signatures in storage for arbitrating possible disputes later.

To verify that the received document is indeed from the claimed sender and that the contents have not been altered, several procedures, called authentication techniques, have been developed. However, message authentication techniques cannot be directly used as digital signatures due to inadequacies of authentication techniques. For example, although message authentication protects the two parties exchanging messages from a third party, it does not protect the two parties against each other. In addition, elementary authentication schemes produce signatures that are as long as the message themselves.

III. BASIC NOTATIONS ANDTERMINOLOGOIES

Digital signatures are computed based on the documents (message/ information) that need to be signed and on some private information held only by the sender. In practice, instead of using the whole message, a hash function is applied to the message to obtain the message digest. A hash function, in this context, takes an arbitrary-sized message as input and produces a fixed-size message digest as output. Among the commonly used hash functions in practice are MD-5 (message digest 5) and SHA (secure hash algorithm). These algorithms are fairly sophisticated and ensure that it is highly improbable for two different messages to be mapped to the same hash value. There are two broad techniques used in digital signature computation—symmetric key cryptosystem and public-key cryptosystem (cryptosystem broadly refers to an encryption technique). In the symmetric key system, a secret key known only to the sender and the legitimate receiver is used [1]. However, there must be a unique key between any two pairs of users. Thus, as the number of user pairs increases, it becomes extremely difficult to generate, distribute, and keep track of the secret keys [3].

A public key cryptosystem, on the other hand, uses a pair of keys: a private key, known only to its owner, and a public key, known to everyone who wishes to communicate with the owner. For confidentiality of the message to be sent to the owner, it would be encrypted with the owner's public key, which now could only be decrypted by the owner, the person with the corresponding private key. For purposes of authentication, a message would be encrypted with the private key of the originator orsender, who we will refer to as A. This message could be decrypted by anyone using the public key of A. If this yields the proper message, then it is evident that the message was indeed encrypted by the private key of A, and thus only A could have sentit.

IV. CREATING AND VERIFYING A DIGITAL SIGNATURES

A simple generic scheme for creating and verifying a digital signature. A hash function is applied to the message that yields a fixed-size message digest. The signature function uses the message digest and the sender's private key to generate the digital signature. A very simple formof the digital signature is obtained by encrypting the message digest using the sender's private key. The message and the signature can now be sent to the recipient [6]. The message is unencrypted and can be read by anyone. However, the signature ensures authenticity of the sender (something similar to a circular sent by a proper authority to be read by many people, with the signature attesting to the authenticity of the message). At the receiver, the inverse signature function is applied to the digital signature to recover the original message digest. The received message is subjected to the same hash function to which the original message was subjected. The resulting message digests

compared with the one recovered from the signature. If they match, then it ensures that the message has indeed been sent by the (claimed) sender and that it has not been altered.

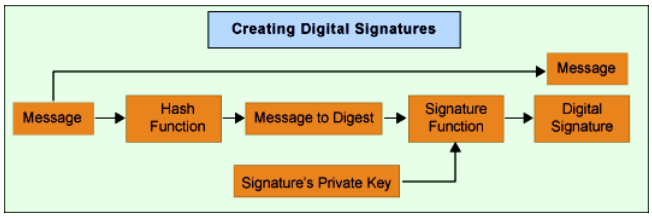

Fig. 1 creating a digital signature

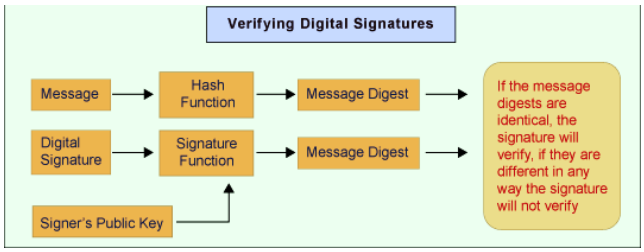

Fig. 2 verifying a digitalsignature

I. CREATING AND OPENING A DIGITAL ENVELOPE

A digital envelope is the equivalent of a sealed envelope containing an unsigned letter. The outline of creating a digital envelope is shown in Fig. 3. The message is encrypted by the sender using a randomly generated symmetric key. The symmetric key itself is encrypted using the intended recipient's public key. The combination of the encrypted message and the encrypted symmetric key is the digital envelope. The process of opening the dig-ital envelope and recovering the contents is shown in Fig. 4. First, the encrypted symmetric key is recovered by a decryption using the recipient's private key [7]. Subsequently, the encrypted message is decrypted using the symmetric key.

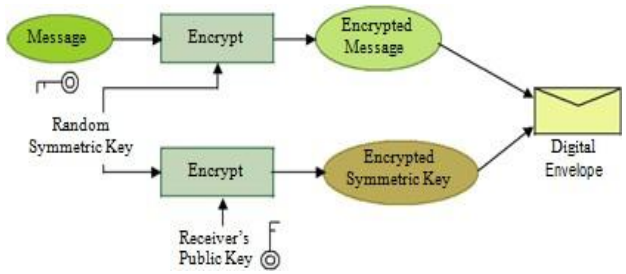

Fig. 3 creating a digital envelope

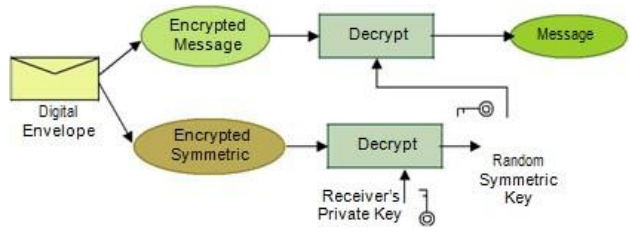

Fig. 4 Opening a digital envelope

II. CREATING AND OPENING DIGITAL ENVELOPES CARRYING SIGNEDMESSAGES

The process of creating a digital envelope containing a signed message is shown in Fig. 5. A digital signature is created by the signature function using the message digest of the message and the sender's private key[2]. The original message and the digital signature are then encrypted by the sender using a randomly generated key and a symmetric key algorithm. The symmetric key itself is encrypted using the recipient's public key. The combination of encrypted message and signature, together with the encrypted symmetric key, form the digital envelope containing the signed message. Figure 6 shows the process of opening a digital envelope, recovering the message, and verifying the signature. First, the symmetric key is recovered using the recipient's privatekey.

This is then used to decrypt and recover the message and the digital signature. The digital signature is then verified as describedearlier

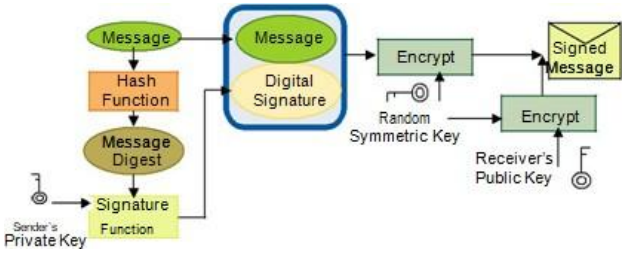

Fig. 5 Creating a digital envelope carrying a signed message

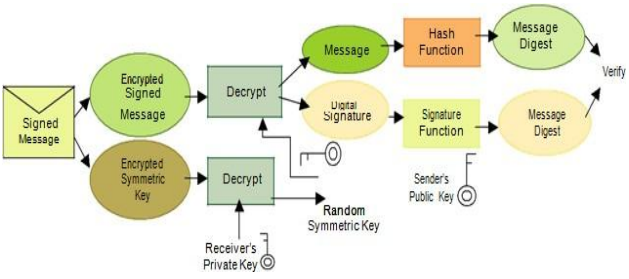

Fig. 6 Opening a digital envelope and verifying a digital signature

V. DIRECT AND ABRITRATED DIGITAL SIGNATURES

A variety of modes have been pro-posed for digital signatures that fall into two basic categories: direct and arbitrated. The direct digital signature involves only the communicating parties, sender and receiver. This is the simplest type of digital signature. It is assumed that the recipient knows the public key of the sender. In a simple scheme, a digital sig-nature may be formed by encrypting the entire message or 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 encryption or the shared secret key, which is conventional encryption. A sender may later deny sending a particular message by claiming that the private key was lost or stolen and that someone else forged his signature. One way to overcome this is to include a time stamp with every message and requiring notification of loss of key to the proper authority. In case of dispute, a trusted third party may view the message and its signature to arbitrate thedispute.

In the arbitrated signature scheme, there is a trusted third party called the arbiter. Every signed message from a sender A to a receiver B goes first to an arbiter T, who subjects the message and its signature to a number of tests to check its origin and content. The message is then dated and sent to B with an indication that it has been verified to the satisfaction of the arbiter. The presence of T solves the problem faced by direct signature schemes, namely that A might deny sending a message. The arbiter plays a sensitive and crucial role in this scheme, and all parties must trust that the arbitration mechanism is working properly. There are many variations of arbitrated digital- signature schemes. Some schemes allow the arbiter to see the messages, while others don't. The particular scheme employed depends on the needs of the applications. Generally, an arbitrated digital-signature scheme has advantages over a direct digital-sig-nature scheme such as the trust in communications between the parties provided by the trusted arbiter and in the arbitration of later disputes, if any.

VII. A PUBLIC VERSUS A PRIVATE APPROACH TO DIGITALSIGNATURES

Another way of classifying digital sig-nature schemes is based on whether a private-key system or a public-key system is used. The public-key system based digital signatures have several advantages over the private-key system based digital signatures. The two most popular and commonly used public-key system based digital signature schemes are the RSA (named after Rivest, Shamir, and Aldeman, the Inventorsof the RSA public-key encryption scheme) and the digital signature algorithm (DSA) approaches. The DSA is incorporated into the Digital Signature Standard (DSS), which was published by the National Institute of Standards and Technology as the Federal Information Processing Standard. It was first proposed in 1991, revised in 1993, and further revised with minor changes in1996.

RSA is a commonly used scheme for digital signatures. In a broad outline of the RSA approach, the message to be signed is input to a hash function that produces a secure hash code of fixed length. This hash code is then encrypted using the sender's private key to form the signature. Both the signature and the message are then concatenated and trans-mitted. The recipient takes the message and produces a hash code. The recipient also decrypts the signature using the sender's public key. If the calculated hash code matches the decrypted signature, the signature is accepted as valid. This is because only the sender knows the private key, and thus only the sender could have produced a valid signature. The sig-nature generation and verification using RSA is identical to the schemes shown in Figs. 1 and 2, respectively.

VI. DIGITAL SIGNATURES IN REAL APPLICATIONS

Increasingly, digital signatures are being used in secure e-mail and credit card transactions over the Internet. The two most common secure e-mail systems using digital signatures are Pretty Good Privacy and Secure/Multipurpose Internet Mail Extension. Both of these systems support the RSA as well as the DSS-based signatures. The most widely used system for the credit card transactions over the Internet is Secure Electronic Transaction (SET). It consists of a set of security protocols and formats to enable prior existing credit card payment infrastructure to work on the Internet [5]. The digital signature scheme used in SET is similar to the RSAscheme.

III. CONCLUSION

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. Just as signatures facilitate validation and verification of the authenticity of paper documents, digital signatures serve the purpose of validation and authentication of electronic documents.

This technology is rather new and emerging and is expected to experience growth and widespread use in the comingyears.

Real-time updates are also changing the face of how we interact with digital signage. Real estate agents, restaurants, and retailers are using this level of technology to keep customers up to date with inventory availability.

REFERENCES

[1] F.E.S.,Dunbar, 2002. Digital Signature Scheme Variation, presented in University of Waterloo.

[2] Rivest R. The MD5 message-digest algorithm.2015.

[3] Matricial public key cryptosystem-with-digital-signature

[4] A comprehensive study on digital signature for internet security.2016.

[5] Digital-signature-scheme-based-on-factoring-and-discrete logarithms.

[6] Hartman B, Flinn DJ, Beznosov K, Kawamoto S Mastering web services security. John Wiley & Sons; 2018.

[7] http://www.engpaper.com/digital-signature-scheme-based-on-factoring-and-discrete-logarithms.htm

[8] http://www.engpaper.com/asymptotically-efficient-lattice-based-digital-signatures.htm