Journal Of Harmonized Research (JOHR)

Journal Of Harmonized Research in Engineering
1(2), 2013, 80-86

ISSN 2347 – 7393

Review Article

ENHANCES SECURITY REDUCES TIME: DIGITAL SIGNATURES

Nikita Chhillar, Nisha Yadav, Neha Jaiswal

Department of Computer Science and Engineering,
Dronacharya College of Engineering, Khentawas,
Farukhnagar, Gurgaon, India

Abstract:
A **DIGITAL SIGNATURE** is a mathematical scheme for demonstrating the authenticity of a digital message or document. It provides authentication, non repudiation and integrity to the message. Digital signatures are commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery or tampering and they are also known as the **"**CRYPTOGRAPHIC SIGNATURES OR ELECTRONIC SIGNATURES**".** With the development of Internet, digital signature becomes more and more important for the electronic commerce security because of its data integrity protecting and privacy. Anyone can verify this signature using the corresponding publicly revealed encryption key. Considered by the electronic signature industry as the most reliable way to sign of the three types of electronic signatures and the only standard signing solution available, digital signatures are a thoroughly-tested and well established technology.

Keywords: digital signatures, Key Pair Generator, Secure Electronic Transaction, Electronic Commerce

Introduction:

With the development of network and software technology, applications of internet has made enormous persuade on traditional working. Simultaneously E-commerce came into sight and developed swiftly, playing great role in business activity. In contrast the conventional or traditional business pattern, E-commerce has attributes of great convenience and high efficiency. Applications such as banking, stock

For Correspondence:
nikitachhillar@yahoo.com
Received on: October 2013.
Accepted after revision: November 2013.

trading, and the sale and purchase of merchandise are increasingly accentuating electronic transactions to reduce operational costs and provide enhanced services.

This has led to phenomenal increases in the amounts of electronic documents that are generated, processed, and stored in computers and transmitted over networks.

This electronic information handled in these applications is valuable and sensitive and must be protected against tampering by malicious third parties i.e. they are neither the senders nor the recipients of the information. Sometimes, there is a need to prevent the information or items related to it such as date or time it was created, sent, and received from being tampered with by the originator and/or the recipient. Traditionally, paper documents are validated and certified by written signatures, which work fairly well as a means of providing authenticity. For electronic documents, a similar mechanism is necessary. Digital signatures, which are nothing but a string of ones and zeroes generated by using a digital signature algorithm, serve the purpose of validation and authentication of electronic documents Validation refers to the process of certifying the contents of the document, while authentication refers to the process of certifying the sender of the document.

Characteristics of Digital Signatures

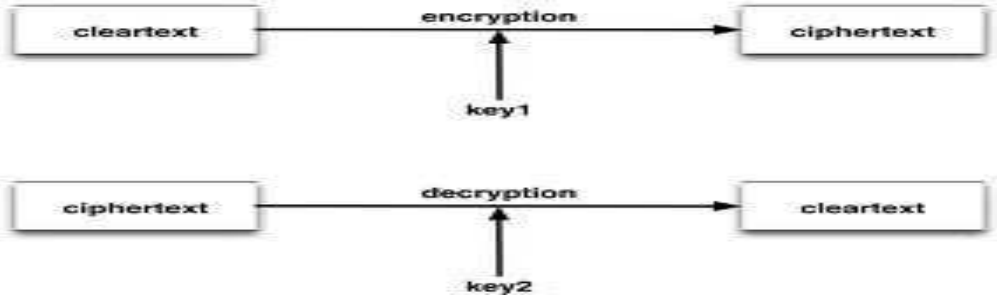
A digital signature should have all the characteristics and features of a conventional signature including a few more features as digital signatures are being used in practical, but susceptible, applications such as secure e-mail and credit card transactions over the Internet. Digital signature is basically a sequence of zeroes and ones a good digital signature should possess 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 should be easy to generate.
- It must be easy to recognize and substantiate 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
- It must be practical to ret-copies of the digital signatures in storage for arbitrating possible disputes later.

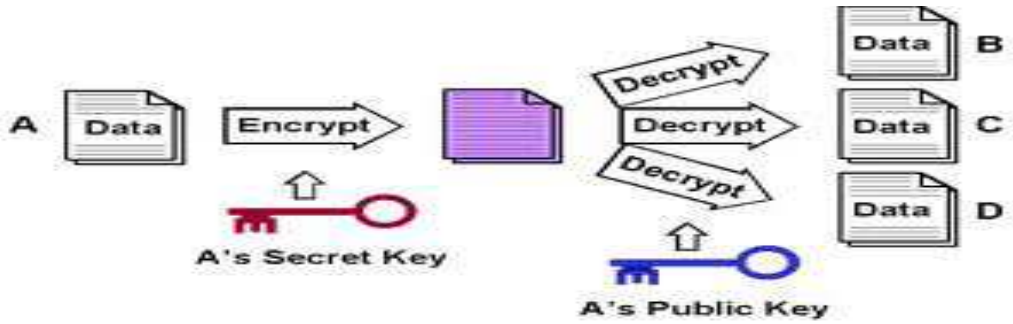
To authenticate that the received document is indeed from the claimed sender and that the contents have not been altered, several procedures, called authentication techniques, have been developed. However, message authentication techniques cannot be directly used as digital signatures due to inadequacies of authentication techniques

Technologies of Digital Signature

Public Key Encrypting Scheme: The base of digital signature technology is public key encrypting technology. In the traditional cryptography system, the cipher code is used in the process of encrypting plain text into cipher text and in the inverse process is the same. This method is called symmetric cryptography technology. Public key encrypting scheme is a kind of Asymmetric cryptography technology.



The basic idea is that the keys of the two parties are different. Every user has a key pair. One is private key which is saved by the user himself, another one is issued in public places such as internet for downloading or enquiring. Public key algorithm is very slow with contrast to private algorithm. It is designed for a little data, but not for much data. It is usually used together with hash function in digital signature.



Hash Algorithm: Hash algorithm is an algorithm which is used to compute a data fingerprint of a data block. It is a one-way function which satisfies the following conditions:

1) can receive data with any length;
2) can produce abstract with fixed length;
3) can compute abstract easily;
4) cannot compute message from abstract;
5) It is impossible to find two different messages which have same abstract.

Hash function can make short abstract with fixed length for the binary data with any length. The popular hash algorithms are MD5, Secure Hash Algorithm SHA, having all kinds of security level and so on.

Selection of best digital signatures: The best digital signature systems can perform the following functions and prove themselves to be useful:

- Verify recipients outside of an organization
- Enable employees to sign documents while traveling
- Enable cross platform capabilities
- Enable the use of numerous applications, such as Microsoft Word®, Adobe Acrobat®, and TIFF images.

When it comes to select a digital signature system, an enterprise needs to be aware of several important criteria. Some points are highlighted below which are very important while selecting a digital signature:

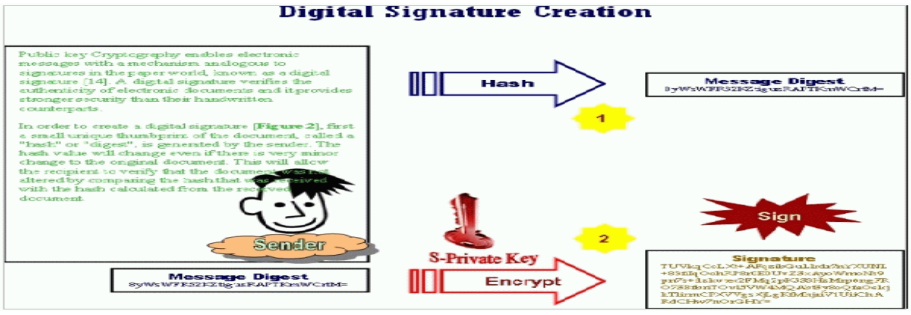
1. **Sealing Documents**: A digital signature must be able to seal any electronic document and guarantee that it is tamperproof. It uses a one-time

"fingerprint", unique to both the signer and the document to ensure that the signer is indeed the originator or owner of the document. This "fingerprint" cannot be reused or reassigned and proves that the message has not been altered in any way.

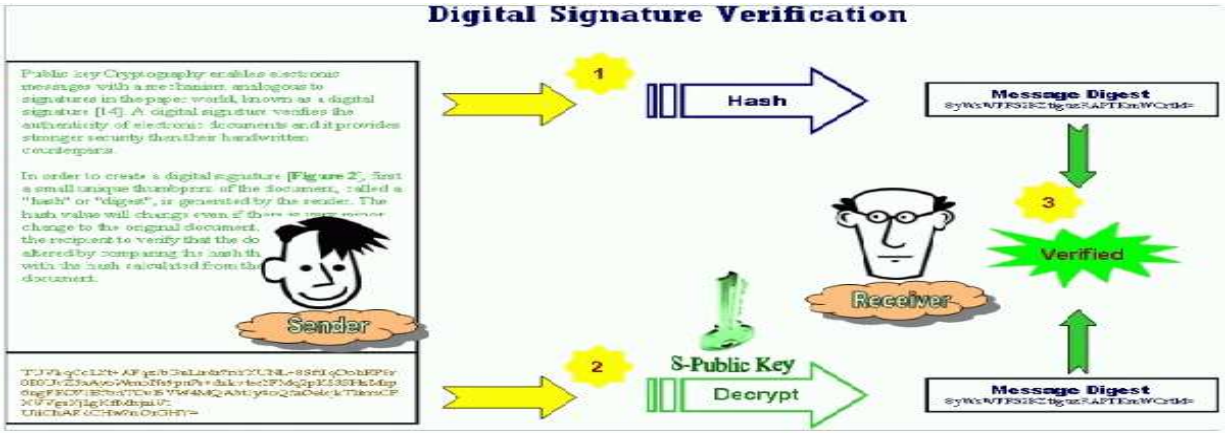
2. **Multiple Application Support:** The best digital signature system supports multiple applications i.e. it can work on many platforms irrespective of the application type.
3. **Graphical Signatures:** Visual graphical signatures do not really add security to the document, but they are important from a user's acceptance point of view, as they provide a natural user indication that the document is indeed signed.
4. **Multiple Signatures:** The best digital signature system enables documents to be signed by more than one person in more than one place. In the virtual world, an effective digital signature system should enable "sectional signing", which allows signatories to edit and sign their portion of the document.
5. **Zero It Management:** The best digital signature system is easily installed, intuitive to use and does not require a dedicated support staff - it will work from the moment it is installed.
6. **Compliance:** The best digital signature system complies with all legal requirements which are authenticity, integrity, privacy, non refutability and enforceability.
7. **Transportability:** An effective digital signature system should ensure **transportability.** If a company implements a digital signature solution and sends a signed document to a client who has not installed the same digital signature system, they will not be able to verify the document.
8. **Seamless User Sign Up**: Once a digital signature system has been deployed, it should be both simple to use and as transparent as possible. Neither the users, nor the IT person, should be aware of how a certificate is generated or maintained.
9. **Simple To Use**: In the virtual paperless world, signing a document should be just as easy. It should take no more than 10 seconds or 1-2 mouse clicks – to ensure that the document is signed, sealed and legally compliant.
10. **Total Cost of Ownership:** The digital signature system has no hidden operation and management costs this adds to its features.

Creation and Verification of Digital Signatures

A simple generic scheme for creating and verifying a digital signature is shown in Figs. 1 and 2, respectively. 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 form of 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.



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 digest is 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.



Realizing Digital Signature in Java

Java has superiority in realizing digital signature. We produce a digital signature for data using JAVA security API and prove its correctness. The first job to make digital signature is to produce a key-pair. Key is produced in random integer generator. In Java, it is generated by class of Key Pair Generator. In this case, a "DSA" key-pair with the length of 1024 bit is
generated as following:

Step 1: **Program Structure**

The digital methods are included in java security software pack, so all content of the pack should be inserted. The software pack of java.io should be inserted too, because it includes the methods of input of files.

Import java.io.*;
Import java.security.*;

Step2: Generating Public Key and Private Key

Key-pair is generated by class of Key Pair Generator. In this case, DSA" key-pair with the length of 1024 bit is generated as following:

1) Create a key-pair generator
KeyPairGenerator
KeyGen=KeyPairGenerator.getInstance("DSA ")

2) Initialize the key-pair generator

Using empty constructing function of Secure Random, a "seed" value needed by a random integer generator is generated:

KeyGen. initialize(1024, new SecureRandom());

Step 3: Sign Digital Signature

After key-pair generating, the signature will be made. In this case, class of Signature is used to make signature, the signing steps:

1) Signature object (object). A signature object which is generated and verified with DSA algorithm can be produced as following:

Signature dsa=Signature.getInstance ("SHA/DSA");
2) Initialize the signature object. Before being used in signing(or verifying), the signature object should be initialized first. A private key is needed in the initializing procession: PrivateKey Priv=Priv.getprivate( );
Dsa.initSign(Priv);
3) Data being signed should be provided to signature object. In case of data in file, the data should be read once a word.

Step 4: **Validate the Signature**

It needs three aspects to validate the signature: the date, the signature and the public key corresponding to the private key using in signature. There is an example for using Signature:
Signature dsa=Signature.getInstance("DSA");
1) First, you must initialize the signature objects in order to validate it. This needs a public key to finish the initialization, which can be drawn from the private keys produced in step 2.
PublicKey pub=pair.getPublic( );
Dsa.initVerify(pub);
2) Offer the data which needs to be validated to the signature objects. Just like what's done in signing, only one byte is read in document. The data is provided to signature objects by transferring. Just as step 3, the computing method is omitted.
3) Validate the signature
Whether the signature is ture or not can be validated once the signature objects are given.
Boolean verifies=dsa.verify(sig);
System.out.println("Signature verifies:"+verifies);
In this step, only primary computing methods are given and some in normal situations in executing and basic inputting and outputting sentences are not considered.

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. The digital signature scheme used in SET is similar to the RSA scheme.

Conclusions

The conclusion comes out that the digital signatures reduce time as well as efforts by increasing the security. As we know conventional and novel businesses and applications have freshly been carrying out enormous amounts of electronic transactions,

which have led to a significant 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.

References

- M. Bishop, *Introduction to Computer Security*. Reading, MA:Addison-Wesley, 2005.
- J. Feghhi and P. Williams, *Digital Certificates: Applied Internet Security* 1st Reading, MA: Addison-Wesley, 1999
- digital signatures by S.R.Subramanya
- **www.arx.com**
- Research on Digital Signature in Electronic Commerce Hongjie Zhu, Daxing Li A New Efficient Digital Signature Scheme Algorithm based on Block cipher
- Prakash Kuppuswamy, Peer Mohammad Appa, Dr. Saeed Q Y Al-Khalidi Di, W., and Hellman, M. Exhaustive cryptanalysis of the NBS data encryption standard. Computer 10 (June 1977), 74-84.
- Knuth, D. E. The Art of Computer Programming, Vol 2: Seminumerical Algorithms. Addison-Wesley, Reading, Mass., 1969.
- Levine, J., and Brawley, J.V. Some cryptographic applications of permutation polynomials. Cryptologia 1 (Jan. 1977), 76-92.
- Merkle, R. Secure communications over an insecure channel. Submitted to Comm. ACM.
- Miller, G.L. Riemann's hypothesis and tests for primality. Proc. Seventh Annual ACM Symp. on the Theory of Comptng. Albuquerque, New Mex., May 1975, pp.
- 234-239; extended vers. Available as Res. Rep. CS-75-27, Dept. of Comptr. Sci., U. of Waterloo, Waterloo, Ont., Canada, Oct. 1975.
- Niven, I., and Zuckerman, H.S. An Introduction to the Theory of Numbers. Wiley, New York, 1972.