IJFEAT

INTERNATIONAL JOURNAL FOR ENGINEERING APPLICATIONS AND TECHNOLOGY

# DIGITAL SIGNATURE

**Sejal Lunawat[1], Paridhi Jain[2], Pranjali Dethe[3]**

[1]*Student, Department of CSE, Jawaharlal Darda Institute of Engineering and Technology Yavatmal, Maharashtra, India,* ***sejallunawat70@gmail.com***

[2]*Student, Department of CSE, Jawaharlal Darda Institute of Engineering and Technology Yavatmal, Maharashtra, India,* ***paridhijain26@gmail.com***

[3]*Student, Department of CSE, Jawaharlal Darda Institute of Engineering and Technology Yavatmal, Maharashtra, India,* ***pranjalidethe03@gmail.com***

**Abstract**

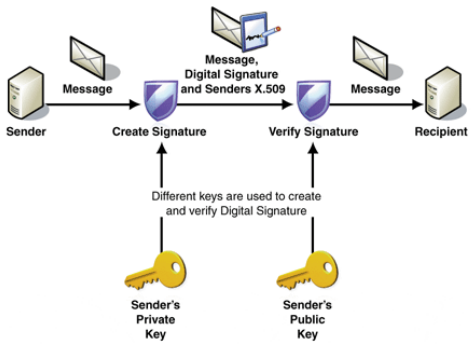
*A digital signature is a mathematical technique used to validate the authenticity, integrity and Non-Repudiation of a message, software or digital document. With the development of internet network and software technology digital signature has become more important for information security. As nowadays, security plays a major role in communication. There are different types of techniques that have been used to secure the data transmitted over internet. Here we have used DSA algorithm .This algorithm provides the functionality to generate and verify signal using public key, and private key. In this paper we have describe the concept of digital signature. There is also history, applications, advantages and disadvantages of digital signature.*

*Keywords: - Digital signature, Information security, Public key, Private key.*

---------- *** ----------

## 1. INTRODUCTION TO DIGITAL SIGNATURE

The documents are commonly authenticated by the signature. Even when the document is signed physically one is authenticating its contents. In the same manner digital signature is a method which is used to authenticate the contents of the electronic documents, which can be used with PDF, e-mail, word processing etc. in this digital ID is required for signing documents. This ID can be obtained from various certification authorities on the web like the VeriSign and EchoSign. The documents you sign contain the digital signature which is simply a small block of data. It is generated from the digital ID that includes public key and private key. The signature is applied to the document with the help of private key while the public key is send to the file.




**[4] Fig-1: General Idea Digital Signature**

DSA defines a technique for generating and validating digital signature. This technique is supposed to provide data integrity and non-repudiation of the origin and content of a digital message. Digital signature is also a sort of Cryptography. Cryptography means keeping communications private. It is art to convert message or data into a different form, such that without having access to the 'key' no one can read them. The message may be converted using a 'code' or 'cipher'. It deals with encryption, decryption and authentication.

## 2. HISTORY OF DIGITAL SIGNATURE

[1]Many people think that digital signature technology is some new, untested trend. The truth is that digital signatures have been around for decades, and they are gaining popularity in the mainstream.

In 1976, Whitfield Diffie and Martin Hellman first described the perception of a digital signature scheme, which were existed based on functions that are trapdoor one-way transformation. After that, Ronald Rivest, Adi Shamir, and Len Adleman created the algorithm, which could be used to produce primitive digital signature, i.e. the RSA algorithm (but RSA signature are not secure).In 1984,ShafiGoldwasser, Silvio Micali, and Ronald Rivest anxiously define the security requirement of digital signature schemes. The first such scheme which is based on family of functions with a much weaker required property of one- way permutation was presented by Moni Naorand Moti Yung. This scheme is not based on trapdoor functions. [7] In 1988, Lotus Notes 1.0 becomes the first widely marketed software package to offer digital signature, which used the RSA algorithm. DSA refers to as digital signature algorithm was introduced in 1991 by National Institute of Standards and Technology (NIST) as a better method

of creating digital signature. This algorithm provides the functionality to generate and verify signal.

## 3. DIFFERENCE BETWEEN ELECTRONIC SIGNATURE AND DIGITAL SIGNATURE

Electronic signature is same as digital signature, an amendment to IT act in 2008 has introduced the term electronic signature.

An electronic signature is a way of representing your signature on computerized document, for example delivery slips. Electronic signature means authentication of an electronic record by a subscriber by means of electronic techniques. Electronic signatures are open to tampering. And it is much harder to verify.

Digital signature is much more than electronic signature. Digital signature becomes intrinsically linked to the content of Digital document using encryption. Digital signatures are like a lock on a document. If the document change after the signature is applied, it will show up as an invalidated signature. It is an implementation of electronic signature.

## [3]4. DIGITAL SIGNATURE ALGORITHM

In this section we have describes the DSA (Digital Signature Algorithm) algorithm, which consists of 2 parts: generation of a pair of public key and private key; generation and verification of digital signature.

DSA is a United States Federal Government standard for digital signatures. In August 1991, it has been suggested and standardized by the National Institute of Standards and Technology (NIST) for use in their Digital Signature Standard (DSS).

### 3.1 Key Generation

In this part of the DSA algorithm we have described the public key and private key generation as follows:

I. Choose a prime number q, which is called the prime divisor.
II. Choose another primer number p, such that p-1 mod q = 0. p is called the prime modulus.
III. Choose an integer g, such that 1 < g < p, g**q mod p = 1 and g = h** ((p–1)/q) mod p. q is also called g's multiplicative order modulo p.
IV. Choose an integer, such that 0 < x < q.
V. Compute y as g**x mod p.
VI. Package the public key as {p, q, g, y}.
VII. Package the private key as {p, q, g, x}.

### 3.2 Signature Generation

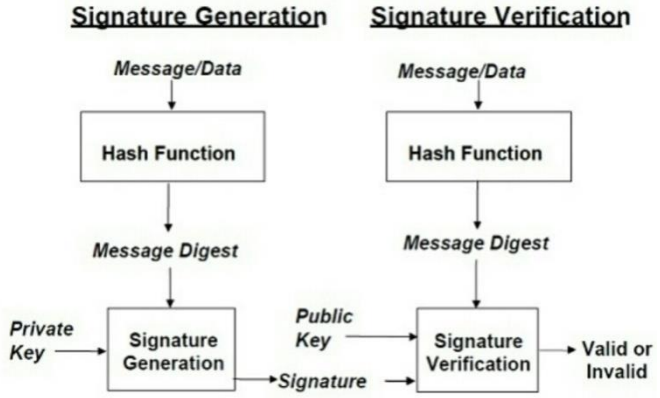
In this part of the DSA algorithm Signature generation and Signature verification is described as follows:

**3.2.1 To generate a message signature, the sender can follow these steps:**

I. Generate the message digest h, using a hash algorithm like SHA1.
II. Generate a random number k, such that 0 < k < q.
III. Compute r as (g**k mod p) mod q. If r = 0, select a different k.
IV. Compute i, such that k*i mod q = 1. i is called the modular multiplicative inverse of k modulo q.
V. Compute s = i*(h + r*x) mod q. If s = 0, select a different k.
VI. Package the digital signature as {r, s}.

**3.2.2 To verify a message signature, the receiver can follow these steps:-**

I. Generate the message digest h, using the same hash algorithm.
II. Compute w, such that s*w mod q = 1. w is called the modular multiplicative inverse of s modulo q.
III. Compute u1 = h*w mod q.
IV. Compute u2 = r*w mod q.
V. Compute v = (((g**u1)*(y**u2)) mod p) mod q.
VI. If v== r, the digital signature is valid.




**[3] Fig-2 DSA Algorithm**

## 4. ADVANTAGES AND DISADVANTAGES OF DIGITAL SIGNATURE

### 4.1 Advantage

[6]Digitalization is being added to anything which makes the thing faster than the non-digital things. Almost instantaneously, Digital Signature are used to send the documents such as via email and do not need to be delivered via courier. Thus this also reduces the cost of sending documents.

Risks of documents that are being intercepted, destroyed, or altered during the transition is get reduce by using this digital signature.

Digital Signature can also be tracked and located in very less amount of time.

It is also easy to import data from one system to another as it is easily integrated with other systems. It also gives us the authenticity that an e-document signed with a digital signature can stand up in court just as any other signed paper document with date and time.

### 4.2 Disadvantage

In digital signature, the sender and recipient both of them may have to buy digital certificates at some cost given by trusted certification authorities. Also they have to buy verification software. The speed of communication will may reduce as the process of generation and verification of digital signature requires

considerable amount of time. The private key must be kept absolutely private by the owner, if it loss then it will cause severe damage.

## 5. APPLICATIONS OF DIGITAL SIGNATURE

Digital signature is used in any field in which the integrity and validity of the data is crucial. In terms of e-mail, no person should be able to send e-mail in the disguise of another person. If any changes occur in the e-mail it 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.

Software developer can use this digital signature in order to ensure that the software remains unmodified and its source is genuine as they often distribute their software using some/ electronic media.

The money transaction or credit card is also done through Secure Electronic Transaction(SET). It consists of a set of security protocol and formats to enable prior existing credit card payment infrastructure to work on the Internet.

## 6. CONCLUSION

Now days, there is increase in electronic transmissions of message, software or digital document; which needs security that the message has not been altered during transmission from sender to receiver. In this paper we describe the digital signature using DSA algorithm which provides security during electronic transmissions. In this paper we used DSA algorithm for digital signature scheme. Behalf of this algorithm we can secure the communication. In this algorithm there are three parameters such as key generation, signature generation, signature verification and this algorithm is more secure than RSA algorithm.

## REFERENCES

[1]. https://en.m.wikipedia.org/wiki/Digital_signature#Notions_of_security.

[2]. G.Ranjith, B.Prathusha, and P.Sagarika "Arbitrated Digital Signature for E-Authentication Technique of a Digital Message" International Journal of Advances in Engineering & Technology, Oct., 2015.©IJAET ISSN: 22311963Vol. 8, Issue 5, pp. 753-7613

[3]. http://www.herongyang.com/Cryptography/DSA-Introduction-What-Is-DSA-Digital-Signature-algorithm.html

[4]. https://lerablog.org/technology/data-security/advantages-and-disadvantages-of-digital-signatures/

[5]. Shraddha Kalbhor, Anita Gaikwad, Kajal Bhise, Prof. Dipmala Salunke, Varsha Bangar "A Survey on Digital Signature" International Journal of Emerging Technology and Advanced Engineering www.ijetae.com ,(ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 5, Issue 1, January 2015)

[6]. http://digitalindiainsight.com/advantages-and-disadvantages-of-digital-signature/

[7]. https://www.signix.com/blog/bid/108804/Infographic-The-History-of-Digital-Signature-Technology