International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 08 Issue: 12 | Dec 2021 www.irjet.net p-ISSN: 2395-0072

Importance of Digital Signature for E-Governance Schemes

Shruti Jain[1]

[1]*Student, Final Year CSE, PES Modern College of Engineering, Pune.*

Abstract - *Recent development in E-Governance would like to leverage digital signature capabilities, which is usage of Information and Communication Technology by the government to provide and facilitate government services, exchange of information etc. Digital signature is a well-known mechanism to carry out digital authentication and verificationof electronic transactions in the online world. As it comes with the word online, the biggest concern is the security issue. To provide E-authentication to the user there are many cryptographic techniques available. This paper discusses increasing the security, reliability, and nonrepudiation of the user's data or information using Digital signature. It is a highly secured and well-known method to authenticate and verify an electronic transaction.*

***Key Words*: Digital Signature, Security, E-Governance, hash function.**

1. INTRODUCTION

E-governance is the platform of Information and Communication Technology where all the government services are delivered online, information is exchanged electronically carrying out important communication over the network, and transactions are performed electronically, over the traditional method. There are so many entities involved in this E-governance system like a citizen, businesses, and governments. Security is the crucial element to make sure E-commerce develops safely and orderly. It is also paid close attention to people. In traditional trade, we use a personal signature or seal to denote one's identity and duty. In E-commerce, signature is used to verifythe identity and truth of data.

1.1 Digital Signature Technology

When a person sends data through a document, it becomes essential to identify one's authenticity for security and safety reasons. Digital signatures are used for this identification. Authentication of the documents is used to prove that the signature and the seal of the document are genuine.These signatures are generated using various algorithms. One such example is Digital Signature Algorithm (DSA). DSA is a type of public-key encryption algorithm. It is used to generate an electronic signature. The digital signature is parallel to the written signature. It must have the following properties: The sender can cross-check the beneficiary's signature in the message. The sender can't deny his signature afterward. The recipient can't forge the sender's signature. Its basic principle works in the following steps: To from the digital signature the sender creates a fixed-length of digital digest from the message and later encrypts it. The digital signature is then appended to the communication and sent to the recipient with the message. While the receipt calculates the original message by Hash function and gets digital digest HI and then decrypts the signature phrase by the sender's public key and gains H2. If HI is the same as H2, the recipient knows that it is the holder of the sender's private key who sent the message. The digital digest is a method, which uses the one-way Hash function to avoid the messages from being changed. It can also turn large messages into a limited information range and send it combined with the message to the receipt, so it is more adapted to E-commerce.

1.2. One-way hash function

A Hash value is generated by a function H. It is of the form h= H (N). N stands for variable-length and H(N) stands for fixed-length hash. There are a lot of functions whose inputs are variable-length and outputs are fixed-length. One-way function has the following special properties: his relatively easy to compute for given M. Since H(N) is called the irreversibility, it is arithmetically absurd to find M. The major purpose of a one-way hash function is to produce a "fingerprint" of a file that others cannot forge. In some applications, only the "one-way "property is not enough, it also needs "collision resistance", they are: For any given block M it is arithmetically absurd to find N 7&N with H(N)= H(N). This is referred to as weak collision resistance. It is arithmetically absurd to find any pair (N, N) such that H(N)= H (N). This is referred to as strong collision resistance. Using any Hash algorithm, the hash value is generated and sender's private key is used to make it more secure. Now the signed message is passed by the sender and at the receiver side, the message is decrypted using sender's public key. After this again the hash value is applied to the message to read the original message send by the sender.

2. Implementation

Here, n stands for modulus, e stands for encryption exponent and d stands for secret exponent or decryption exponent. The algorithm is divided into 5 steps:

1. Key Generation,

2. Digital Signing,

3. Encryption,

4. Decryption and Signature Verification with their workingfunctions mentioned below:

Step-1: Key Generation

Randomly generate two large prime numbers: p and q. Calculate **n=p * q** .Calculate the totient by using the following formula: **Φ(n)= (p-1) * (q-1)** . Now select an integer 'e' such that **1< e <Φ(n)** and **gcd(e, Φ(n)) = 1** . Now calculate d, such that **d * e = 1 mod Φ(n)** . Public key is denoted by **(n,e)** and the private key is denoted by **(n, d).**

Step2: Digital Signing

Start created generate message of the document by using MD5 algorithm. The digest is represented as an integer m. Digital Signature S is generated using the private key **(n, d), S= md mod n.** Sender sends this signature S to the recipient.

Step 3: Encryption

The plain text is represented as a positive integer **m** by thesender. This converts the message into encrypted form by using the formula of receiver's public key (e, n).

C= m^e mod n

Sender sends this encrypted message to the recipient.

Step 4: Decryption

Recipient does the following operation: Using his private key (n, d); which converts the cipher text to plain text 'm' where **m= C^d mod n.**

Step 5: Signature Verification

Receiver does the followings to verify the signature: An integer V is generated using the sender's public key (n, e) and signature SV= Se mod n. It extracts the message digest M1, using the same MD5 algorithm from the given integer V.It then computes the message digest M2 from the signature

S. If both the message digests are identical i.e. M1= M2, thensignature is valid.

2.1. EXPERIMENTAL OBSERVATIONS

Step 1: Key Generation:

1) We have chosen two distinct prime numbers p=23 andq=53.

2) Compute n=p*q, thus n=23*53 =1219.

3) Compute Euler's totient function, Ø(n)=(p-1)*(q-1), thus

Ø(n)=(23-1)*(53-1)

Therefore **22*52 = 1144**.

4) Next choose any integer '**e**', such that **1 < e < 1144** i.e. gcd

(e, 1144) =1. Here, we chose e=3.

5) Calculate d, where d = **e-1(mod Ø(n)).**

Therefore d**=3-1(mod 1144) = 763.**

6) From the above result the Public-Key is (e, n) = (3, 1219) and the Private- Key is (d, n) = (763, 1219). The Private-Key is kept secret, and is only known by the user.

Step 2: Encryption:

1) The Public-Key (3, 1219) is given to the user who wishes to store the data.

2) Let the message to be send is "hello" which is converted to integer in the following manner: **A=0, B=1,a = 27, b=28,c=29** and so on. Hence the given message is encrypted to m= 49313829413931

3) Data is encrypted now by the Sender using the corresponding Public-Key which is shared by both the sender and the receiver.

C=memod

n=C=493138294139313(mod1219)

= 625535179657807535.

4) This encrypted data i.e., cipher text is send to the recipient.

Step 3: Digital Signature and Signature Verification:

1) First using MD5 algorithm the message gets converted to message digest i.e. to hexadecimal form.

2) **MD1=H(m)= 0x000c00f0000000f0426f00f0726000f0**.

3) Message digest in decimal form M1= 012024000024066111024011410802 40.

4) By using the private key d, digitally sign the message digest MD1 to generate digital signature S.

5) S=(MD1)dmod

n= 088702580002588392960258850124025 8.

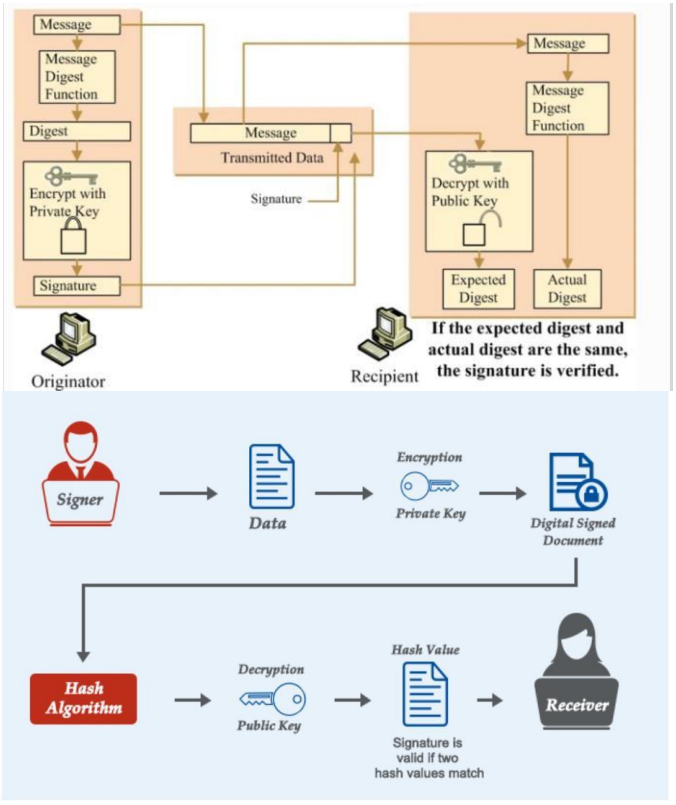
6) Sender then sends the digital signature S to the recipient.

7) Receiver then computes the integer V using S, e and n.
8) V= Se mod n= 012024000024066111024011410802 40.

9) Receiver the computes the message digest from S using MD5 algorithm.

10) **MD2 = 012024000024066111024011410802 40**.

11) Hence the signature is verified as V = MD2.



Digital Signature Mechanism

3. CONCLUSION

As an important component of E-commerce security, Digital signature will imposes higher requirements for security technology. Thus, we should continue to explore new methods so that we can find a more safe and simple signature method. We also got to know how digital signatureis implemented using the MD5 algorithm.

REFERENCES

[1] Abhishek Roy1, Sunil Karforma "Authentication of User in E-Governance: A Digital Certificate Based Approach" International Journal of scientific research and management (IJSRM) Volume-2 Issue-8, Pages 1212- 1221, 2014, ISSN (e): 2321-3418M. Young, The Technical Writer's Handbook. Mill Valley, CA: UniversityScience, 1989.

[2] Mr. D.Shiva, Rama Krishna "Providing Security to Confidential Information Using Digital signature" International Journal for Innovative Research in Science& Technology, Vol-2 Issue-6, 2015.

[3] T. Sivasakthi, Dr. N Prabakaran "Applying Digital Signature with Encryption Algorithm of User Authentication for Data Security in Cloud Computing" International Journal of Innovative Research in Computer and Communication Engineering Vol. 2, Issue 2, February 2014 ISSN(Online): 2320-9801

[4] Henon M, "A two-dimensional mapping with a strange attractor", Comm Math Phys,1976,Vol.50:69-70.

[5] Wojciech Kinastowski "Digital Signature as a Cloud-based Service" CLOUD COMPUTING 2013: The Fourth International Conference on Cloud Computing, GRIDs, and Virtualization

[6] D.C.Lou, J.L.Liu , "Fault resilient and compression tolerant digital signature for image authentication", IEEE Transactions on Consumer Electronics, 2000, 46(1): 31-39.

[7] Shaikh Imtiyaj, Er. Ratan kumar Agrawal, Dr A K Hota "Digital Signature Certificate: A Great scientific Knowledge for Nation Development" IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 19, Issue 4, Ver. IV. (Jul.-Aug. 2017), PP 56-60

[8] Shivendra Singh, Md. Sarfaraz Iqbal, Arunima Jaiswal "Survey on Techniques Developed using Digital Signature: Public key Cryptography" International Journal of Computer Applications (0975 – 8887) Volume 117 – No. 16, May 2015

[9] T. Sivasakthi, Dr. N Prabakaran "Applying Digital Signature with Encryption Algorithm of User Authentication for Data Security in Cloud Computing" International Journal of Innovative Research in Computer and Communication Engineering Vol. 2, Issue 2, February 2014 ISSN(Online): 2320-9801

[10] Nikhilesh Barik & Dr. Sunil Karforma "A Study on Efficient Digital Signature Scheme for E-Governance Security" Global Journal of Computer Science and Technology, Volume 10 Issue 3, February-2012 Online ISSN : 0975-4172