The Role of Digital Signature In Cryptography

Tanvi Panjari
Masters *Of Science in*
Computer Science Student
Chikitsak Samuha's Sir Sitaram
& Lady Shantabai Patkar
College of Arts & Science and
V.P. Varde College of
Commerce &
Economics,Mumbai
Email: tanvipanjari06@gmail.com

***Abstract*—**A digital signature is a mathematical technique used to validate the authenticity and integrity of a digital document, message or software. It's the digital equivalent of a handwritten signature or stamped seal, but it offers far more inherent security. A digital signature is intended to solve the problem of tampering and impersonation in digital communications.

Digital signatures can provide evidence of origin, identity and status of electronic documents, transactions or digital messages. Signers can also use them to acknowledge informed consent. In many countries, including the U.S., digital signatures are considered legally binding in the same way as traditional handwritten document signatures

Key Words: Cryptography, **Digital Signature, public Key Infrastructure(PKI), Certificate Authority**

I. Introduction

Digital signatures function similarly to digital “fingerprints.” The digital signature, which takes the form of a coded message, securely links a signer with a document in a recorded transaction. Digital signatures rely on a universally accepted format known as Public Key Infrastructure (PKI) to ensure enhanced security. They are a subset of electronic signature technology (eSignature).

It is a mathematical scheme for demonstrating the authenticity of digital messages or documents. It is a virtual fingerprint that is unique to a person and is used to identify signers and secure data in digital documents. It is a type of electronic signature that ensures compliance with legal regulations by providing the validity and authenticity of a digital document and the signer’s identity. Digital signatures can provide proof of origin, time, identity, and status of a digital document. A signature confirms that the data emanated from the signer and has not been tampered with during transit.[1]

A digital signature is a type of electronic signature where a mathematical algorithm is routinely used to validate the authenticity and integrity of a message (e.g., an email, a credit card transaction, or a digital document). Digital signatures create a virtual fingerprint that is unique to an individual or entity and are used to identify users and protect the information in digital messages or documents and ensure no distortion occurs when in transit between signer and receiver. In emails, the email as a whole also becomes a part of the digital signature. Digital signatures are significantly more reliable and secure than other forms of electronic signatures

WHY ARE DIGITAL SIGNATURES CONSIDERED SECURE?

Digital signatures work using public-key cryptography. Public key cryptography is a cryptographic method that uses a key pair system, private and public. The private key encrypts the data and is available only to the signer. The public key decrypts the data pertaining to the digital document and is given to the receiver. However, both parties must have a registered digital certificate from an issuing certificate authority to connect the signer and their signature. Public key cryptography ensures the security, accuracy, and authenticity of the document. Encryption is the process of encoding data send to the receiver in a form that can only be decoded by the receiver. Authentication is the process of validating the information from the sender is genuine and has not been altered in transit.
Just like every handwritten signature is unique, every signer is given a unique digital identity from a trusted service provider. When the signer signs a document, the signer’s identity is validated and the signature is encrypted using public key infrastructure technology.[3]

What Is Digital Signature in Cryptography?

Digital signature uses public key cryptography to validate and ensure authenticity and integrity of the signed information. Let's have a look at how digital signature uses public key cryptography for signing and verification operations.

- **Authentication:** When a verifier validates a digital signature using sender's public key, he is confident that the signature is of the sender with associated secret private key.
- **Data Integrity:** If an attacker edits the data, the digital signature verification at the receiver end fails. The hash of updated data and the verification algorithm's result will not match. As a result, the receiver can securely reject the message.
- **Non-repudiation:** Because the signature key is known only to the signer, he can create a unique signature on a given data. In the event of a future disagreement, the receiver might offer the data and digital signature to a third party as evidence.[5]

WHAT IS THE IMPORTANCE OF DIGITAL SIGNATURES?

Agreements and transactions that were once signed on paper and delivered physically are now being replaced with fully digital documents and workflows as more businesses are conducted online. Malicious actors who want to steal or manipulate data for their own gain are often present whenever precious or sensitive data is shared. To minimize the risk of document tampering by malicious parties, businesses must be able to check and authenticate that these critical business documents, data, and communications are trusted and delivered securely.

In addition to protecting sensitive online data, digital signatures do not impede the effectiveness of online document workflows; in fact, when compared to paper processes, they often help improve document management. When digital signatures are in place, signing a document becomes simple and can be done on any computer or mobile device. And, since the digital signature is embedded in the file, it can be used anywhere it is transmitted and on any device. By providing the status of all documents, determining whether or not they've been signed, and watching an audit trail, digitally signed documents are also simple to control and keep track of.[2]

Of course, it's critical that these digitally signed agreements are legally recognized. Digital signatures comply with key standards such as the ESIGN Act of the United States and the US-EU Safe Harbor.

II. How do digital signatures work?

The mathematical algorithm generates a public key and a private key that is linked to each other. When a signer electronically signs a document, the mathematical algorithm generates data pertaining to the signed document by the signer, and the data is then encrypted. This data is also called a cryptographic hash. A hash function is a fixed-length string of numbers and letters generated from a mathematical algorithm. This generated string is unique to the file being hashed and is a one-way function, a computed hash cannot be reversed to find other files that may generate the same hash value. The signer has sole access to the private key and this private key is used to encrypt the document data. The encrypted information or encrypted hash is then transmitted and can be decrypted only by the signer's public key. The receiver who receives the document also receives a copy of the signer's public key which is used to decrypt the signature. A cryptographic hash is again generated on the receiver's side. Both cryptographic hashes are checked to validate their authenticity. The document is considered genuine if they match.[1]

Certificate Authority who are Trust Service Providers(TSP) provides digital certificates to ensure that the keys generated and documents signed are created in a secure environment.

Digital certificates help to validate the holder of a certificate. Digital certificates contain the public key of the sender and are digitally signed by a Certificate authority.

Public key infrastructure (PKI) includes regulations, protocols, rules, people, and systems that aid the distribution of public keys and the identity validation of users with digital certificates and a certificate authority.[2]

The steps followed in creating digital signature are:

Message digest is computed by applying hash function on the message and then message digest is encrypted using private key of sender to form the digital signature. (digital signature = encryption (private key of sender, message digest) and message digest = message digest algorithm(message)).

1. Digital signature is then transmitted with the message.(message + digital signature is transmitted)

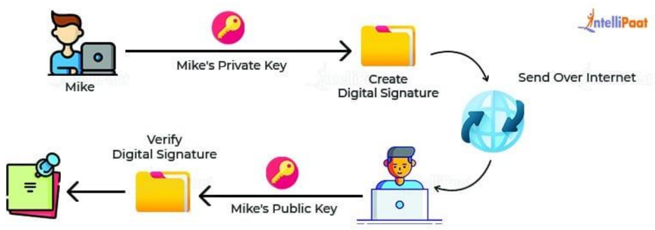
2. Receiver decrypts the digital signature using the public key of sender.(This assures authenticity, as only sender has his private key so only sender can encrypt using his private key which can thus be decrypted by sender's public key).

3. The receiver now has the message digest.

4. The receiver can compute the message digest from the message (actual message is sent with the digital signature).

5. The message digest computed by receiver and the message digest (got by decryption on digital signature) need to be same for ensuring integrity.[1]

Message digest is computed using one-way hash function, i.e. a hash function in which computation of hash value of a message is easy but computation of the message from hash value of the message is very difficult.



Benefits of Digital Signatures

- **Legal documents and contracts:** Digital signatures are legally binding. This makes them ideal for any legal document that requires a signature authenticated by one or more parties and guarantees that the record has not been altered.

- **Sales contracts:** Digital signing of contracts and sales contracts authenticates the identity of the seller and the buyer, and both parties can be sure that the signatures are legally binding and that the terms of the agreement have not been changed.

- **Financial Documents:** Finance departments digitally sign invoices so customers can trust that the payment request is from the right seller, not from a bad actor trying to trick the buyer into sending payments to a fraudulent account.

- **Health Data:** In the healthcare industry, privacy is paramount for both patient records and research data. Digital signatures ensure that this confidential information was not modified when it was transmitted between the consenting parties.

- **Shipping Documents:** Helps manufacturers avoid costly shipping errors by ensuring cargo manifests or bills of lading are always correct. However, physical papers are cumbersome, not always easily accessible during transport, and can be lost. By digitally signing shipping documents, the sender and recipient can quickly access a file, check that the signature is up to date, and ensure that no tampering has occurred.

- **Workflow efficiency**: With lesser delays, digital signatures ensure better efficiency in workflow. Managing and tracking documents are made easier, with lesser effort and time involved. Many features of digital signatures help speed up the work process. For instance, email notifications help remind the person to sign, while status tracking, help to know at which stage the document is at.

- **Better customer experience**: Digital signatures provide the convenience of signing important documents where ever a customer or the person to sign is located. Salespersons do not have to wait for the customer to come to the bank or office. Documents can be signed off at the doorstep. This is ideal, especially in remote areas and smaller townships providing improved and personalized services. The customer has the freedom to be anywhere, and engage with a company, making services and businesses far more easy, quick, and user–friendly.

- **Security**: When it comes to signatures, authenticity, and security are a priority. Digital signatures reduce the risk of duplication or alteration of the document itself. Digital signatures ensure that signatures are verified, authentic and legitimate. Signers are provided with PINs, passwords, and codes that can authenticate and verify their identity and approve their signatures. Time stamping provides the date and time of the signature and thus provides a track of the document, minimizing any risk of tampering or fraud. Security features embedded in digital signatures ensure that documents have not been altered without authorization.

- **Legal validity**: Digital signatures provide authenticity and ensure that the signature is verified. This can stand in any court of law like any other signed paper document. Time stamping and the ability to track and easily archive documents improve and simplify audit and compliance.[4]

Drawbacks of Digital Signatures

Dependence on Key Management: Digital signatures rely on the secure management of cryptographic keys. This means that the sender must keep their private key safe and secure from unauthorized access, while the recipient must verify the sender's public key to ensure its authenticity. Any failure in key management can compromise the security of the digital signature.

Complexity: Digital signatures require a complex process of key generation, signing, and verification. This can make them difficult to implement and use for non-technical users.

Compatibility: Different digital signature algorithms and formats may not be compatible with each other, making it difficult to exchange signed messages across different systems and applications.

Legal Recognition: Although digital signatures have legal recognition in many countries, their legal status may not be clear in all jurisdictions. This can limit their usefulness in legal or regulatory contexts.

Revocation: In case of key compromise or other security issues, digital signatures must be revoked to prevent their misuse. However, the revocation process can be complex and may not be effective in all cases.

Cost: Digital signatures may involve additional costs for key management, certificate issuance, and other related services, which can make them expensive for some users or organizations.

Limited Scope: Digital signatures provide authentication and integrity protection for a message, but they do not provide confidentiality or protection against other types of attacks, such as denial-of-service attacks or malware.[4]

III. Conclusion

In this paper we got to know that, 'digital signature' under the Information Technology Act, 2000, that this is not only essential aspect for creating secure environment for electronic transactions, but it create a sense of authentication and non-repudiation and thus ultimately achieve its objectives of facilitating e-commerce. Thus in its application, digital signature has not only proved an essential techno-legal requirement, but it has made the e-commerce meaningful.

IV. References

[1] https://www.techjockey.com/blog/digital-signature-in-cryptography

[2] https://www.emptrust.com/blog/benefits-of-using-digital-signatures/

[3] https://docs.oracle.com/cd/E19424-01/820-4811/aakfx/index.html

[4] https://www.geeksforgeeks.org/digital-signatures-certificates/

[5] https://vakilsearch.com/blog/digital-signature-in-cryptography/#:~:text=It%20enables%20a%20computer%20system,connect%20on%20the%20same%20network.