Digital Signature

Content

- Introduction
- What is Digital Signature???
- Why Digital Signature???
- Basic Requirements….
- How the Technology Works
- Approaches
- Algorithm of Digital Signature
- Challenges and Opportunities
- Application
- Drawbacks
- Conclusion

INTRODUCTION

- The authenticity of many legal, financial, and other documents is done by the presence or absence of an authorized handwritten signature.
- “Digital Signature” is the best solution for authenticity in various fields.
- A digital signature is nothing but an attachment to any piece of electronic information, which represents the content of the document and the identity of the owner of that document uniquely[5].

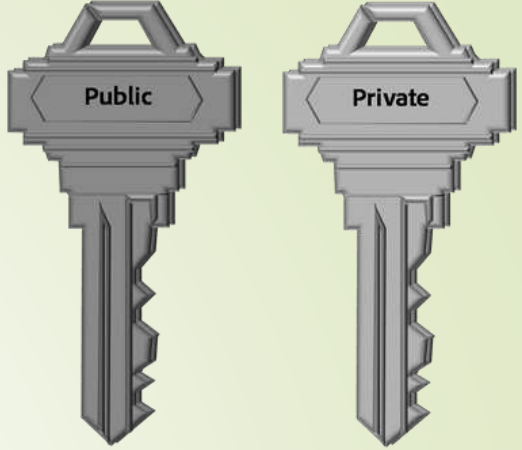
What is digital signature

- Hash value of a message when encrypted with the private key of a person is his digital signature on that e-Document.
- Digital Signature of a person therefore varies from document to document thus ensuring authenticity of each word of that document.
- As the public key of the signer is known, anybody can verify the message and the digital signature.

Why Digital Signatures???

- To provide Authenticity, Integrity and Non-repudiation to electronic documents.
- To use the Internet as the safe and secure medium for e-Commerce and e-Governance

BASIC REQUIREMENTS….



- **Private Key**

  The private key is one which is accessible only to the signer. It is used to generate the digital signature which is then attached to the message.[2]

- **Public Key**

  The public key is made available to all those who receive the signed messages from the sender. It is used for verification of the received message.[2]

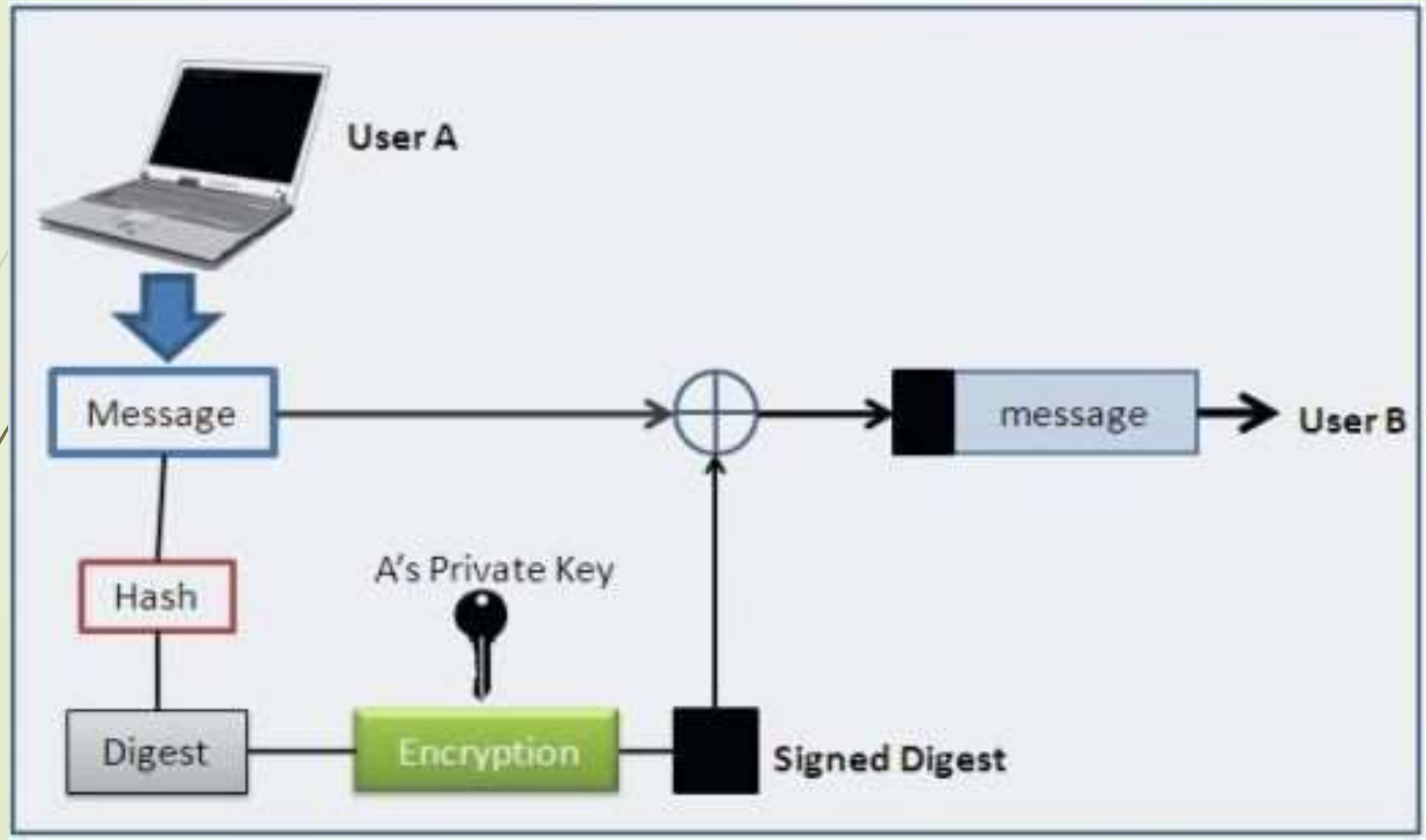
BASIC REQUIREMENTS…

- **Digital Signature Certificate**

  - A subscriber of the private key and public key pair makes the public key available to all those who are intended to receive the signed messages from the subscriber.[1]

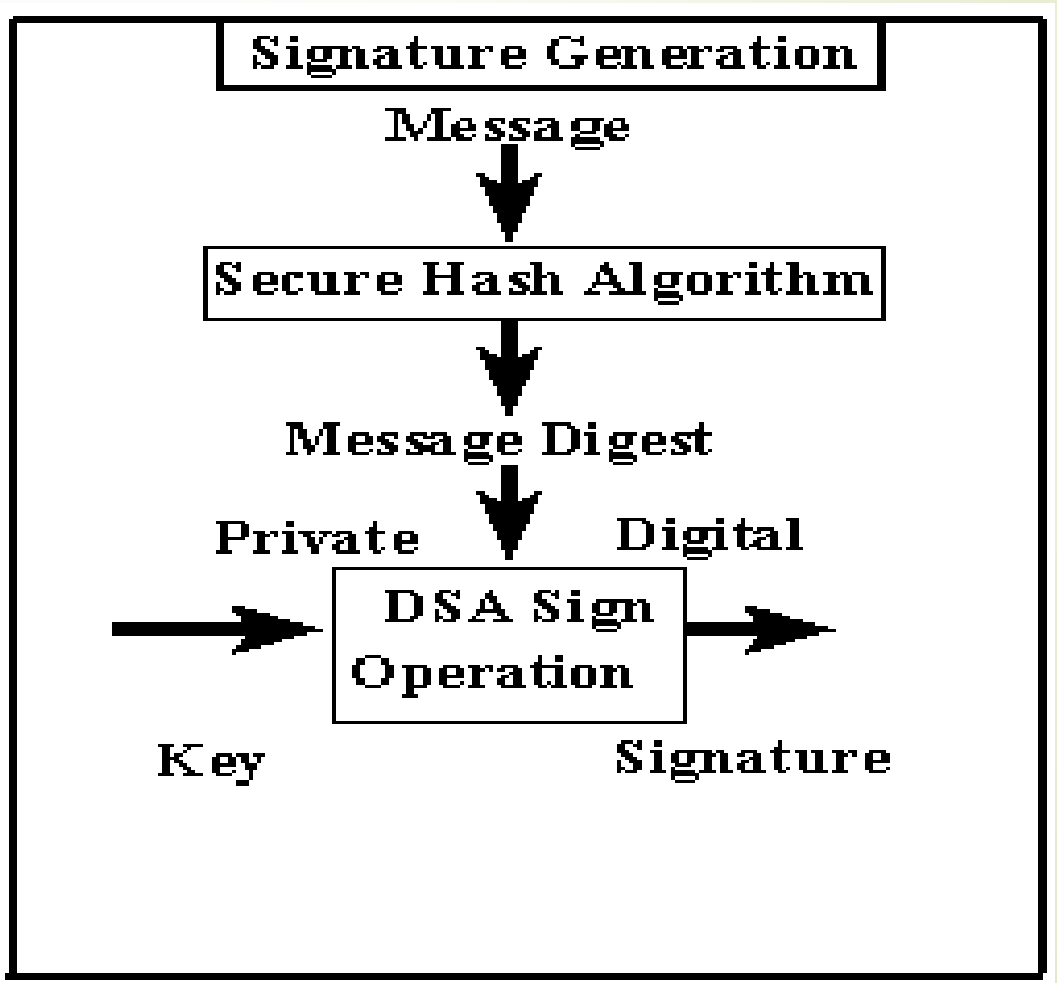
  - But in case of any dispute between the two sides, there must be some entity with the receiver which will allow the receiver of the message to prove that the message was sent by the subscriber of the key pair. This can be done with the Digital Signature Certificate.[1]

HOW THE TECHNOLOGY WORKS??



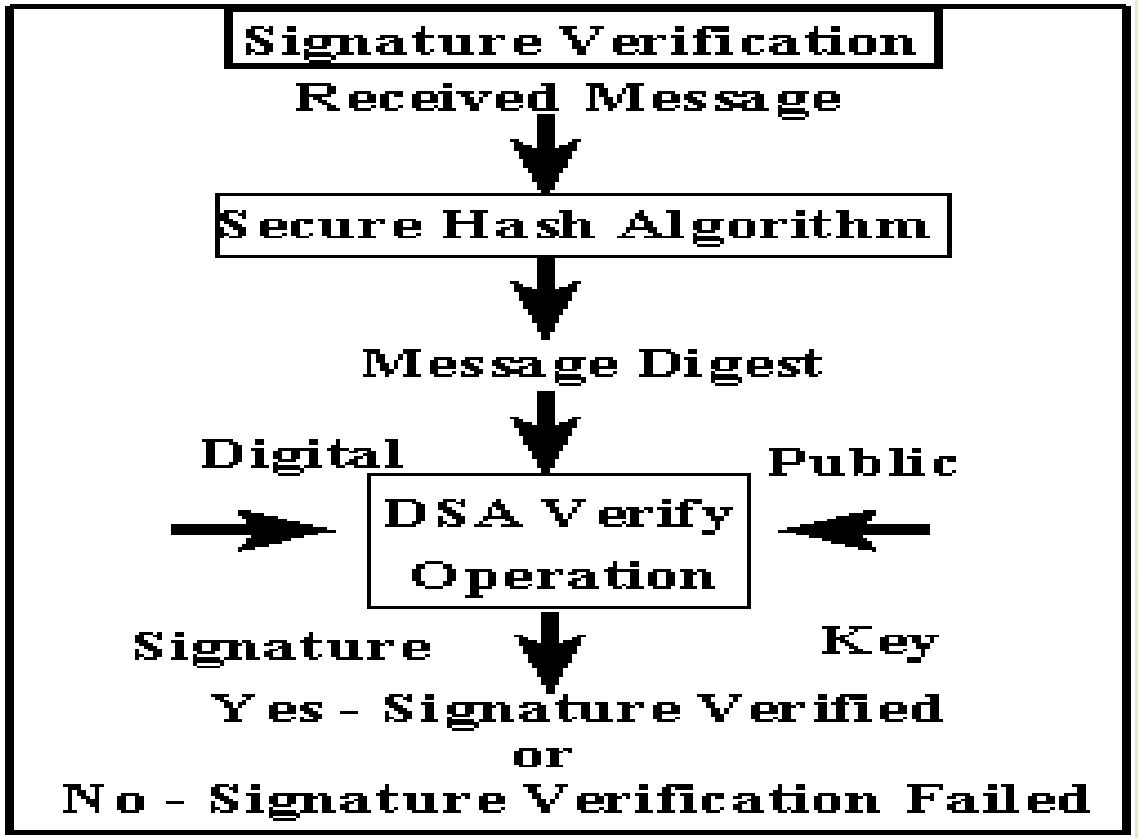
DIGITAL SIGNATURE ALGORITHM

- Digital Signature Generation



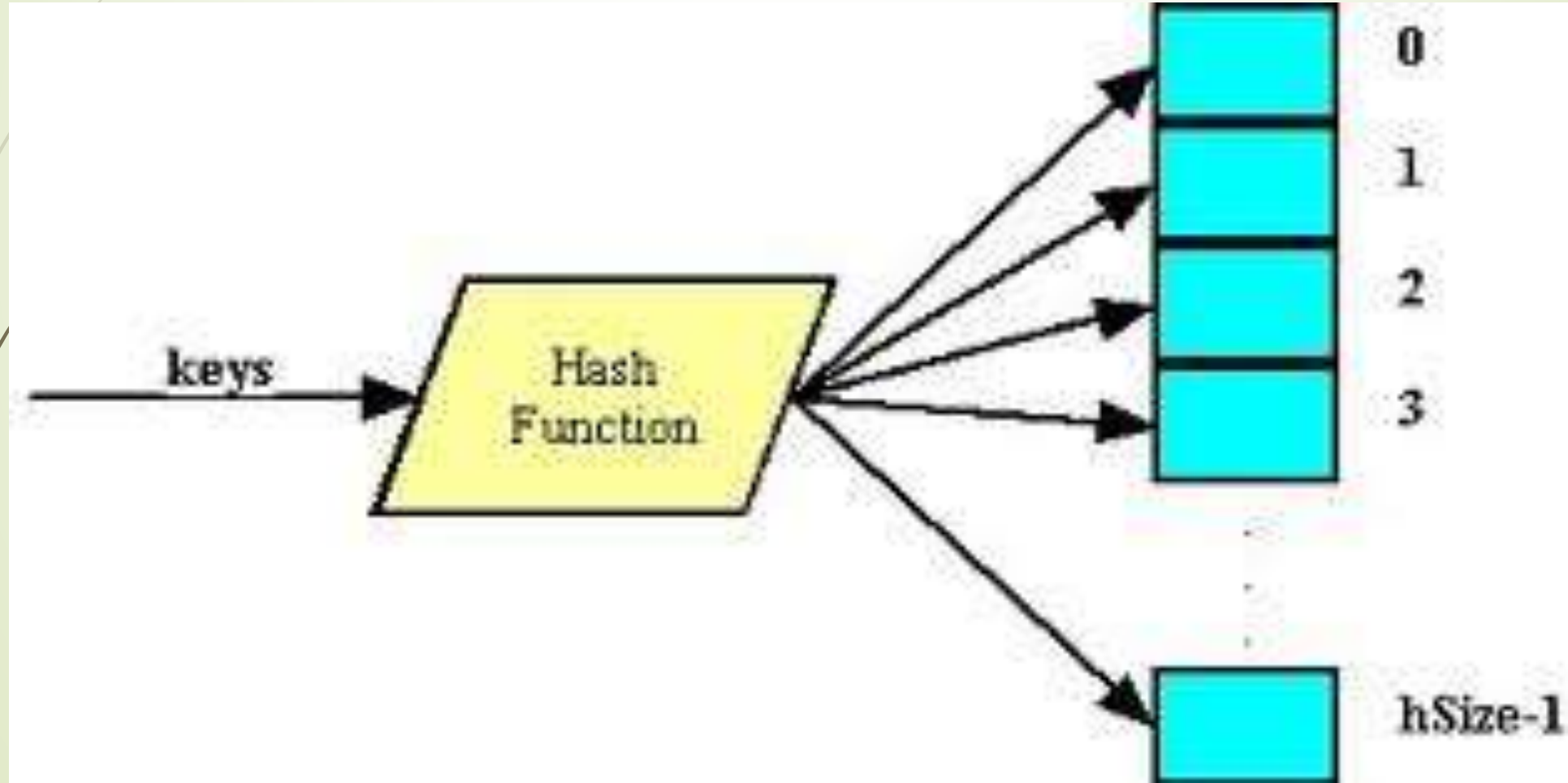
DIGITAL SIGNATURE ALGORITHM

- Digital Signature Verification



DIGITAL SIGNATURE ALGORITHM

- Secure Hash Algorithm



Digital Signatures

- I agree

  Efcc61c1c03db8d8ea8569545c073c814a0ed755
- My place of birth is at Gwalior.

  fe1188eecd44ee23e13c4b6655edc8cd5cdb6f25
- I am 62 years old.

  0e6d7d56c4520756f59235b6ae981cdb5f9820a0
- I am an Engineer.

  ea0ae29b3b2c20fc018aaca45c3746a057b893e7
- I am a Engineer.

  01f1d8abd9c2e6130870842055d97d315dff1ea3
- These are digital signatures of same person on different documents

Paper Signatures v/s Digital Signatures

Parameter	Paper	Electronic
Authenticity	May be forged	Can not be copied
Integrity	Signature independent of the document	Signature depends on the contents of the document
Non-repudiation	a. Handwriting expert needed b. Error prone	a. Any computer user b. Error free

Challenges and Opportunities

- **Institutional overhead:**

  The cost of establishing and utilizing certification authorities, repositories, and other important services, as well as assuring quality in the performance of their functions.

- **Subscriber and Relying Party Costs:**

  A digital signer will require software, and will probably have to pay a certification authority some price to issue a certificate. Hardware to secure the subscriber's private key may also be advisable.

APPLICATIONS …..

- Electronic Mail
- Data storage
- Electronic funds transfer
- Software Distribution
- Smart Cards
- MITRENET
- ISDN
- Time Stamped Signature
- Blind Signatures

DRAWBACKS

- The private key must be kept in a secured manner.[3]
- The process of generation and verification of digital signature requires considerable amount of time.[3]
- For using the digital signature the user has to obtain private and public key, the receiver has to obtain the digital signature certificate also.[3]

CONCLUSION

Digital signatures are difficult to understand. Digital signatures will be championed by many players that the public distrusts, including national security agencies, law enforcement agencies, and consumer marketing companies.

References

1. https://en.m.wikipedia.org/wiki/Digital_Signature
2. www.google.com
3. www.computerfun4u.blogspot.com
4. www.slideshare.net
5. Cryptography & Network Security : Principal & Practise ,William Stallings

Thanks…!!!