4 Digital Signature Schemes and Authentication Protocol

Module 4

Syllabus

At the end of this unit, you should be able to understand and comprehend the following syllabus topics:

- Digital signature and authentication protocols
- Needham Schroeder Authentication protocol
- Digital Signature Schemes
  - RSA
  - ElGamal
  - Schnorr
  - DSS

4.1 Digital Signature

✍ ***Definition :*** *A digital signature is a hash value that has been encrypted with the sender's private key. The act of signing means encrypting the message's hash value with a private key (since no one else knows the sender's private key).*

4.1.1 How does this Work?

So, as shown in Fig. 4.1.1 the sender computes and encrypts the hash value with her private key. As shown in Fig. 4.1.2, at the receiving end, you decrypt the hash value with the sender's public key. Now, because no one else knows the private key of the sender, altering hash value and re-signing with the private key of the sender is not possible.

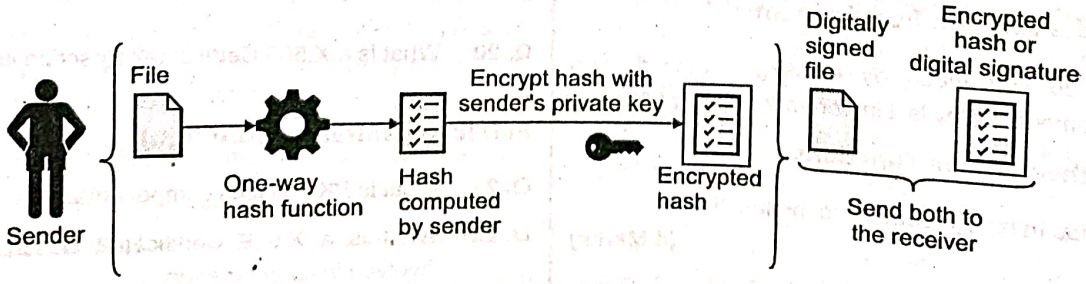

Fig. 4.1.1 : Computation of Digital Signature at the Sender's side

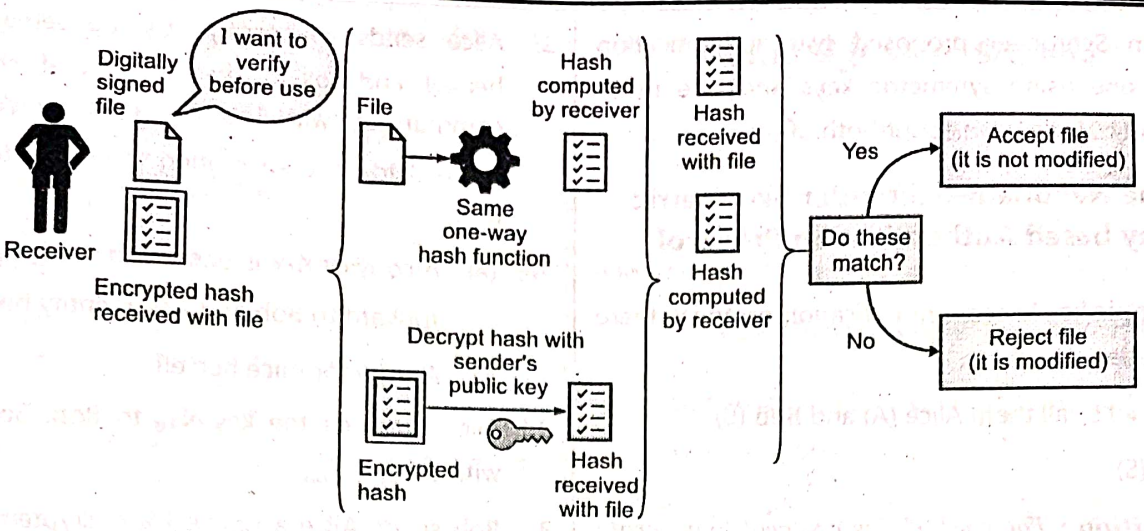

Fig. 4.1.2 : Verification of Digital Signature at the Receiver's side

Table 4.1.1

Sr. No.	Processing applied on a message	Security Property achieved
1.	Encryption	Confidentiality
2.	Hashing	Integrity
3.	Digitally Signing	Integrity, authentication, non-repudiation
4.	Encryption and digitally signing	Confidentiality, Integrity, authentication, non-repudiation

4.1.2 Application and Use of Digital Signature

1. Sending and receiving secure emails
2. Signing documents. For example, you can sign income tax returns using digital signature
3. Sending and receiving important files. For example, insurance policy documents, Aadhar card e-letter, etc.

4.1.3 Properties of Digital Signature

Q. What is the significance of a digital signature on a certificate? Justify. **MU - May 19, 5 Marks**

Digital signature provides three security properties as shown in Fig. 4.1.3.

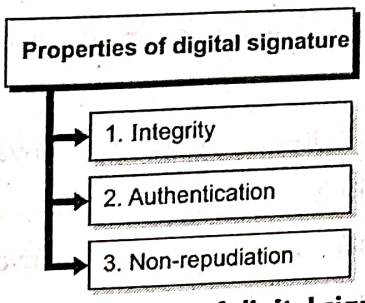

Fig. 4.1.3 : Properties of digital signature

1. **Integrity :** Via hash value calculation
2. **Authentication :** Via the ability to prove sender's identity by decrypting hash with the sender's known public key
3. **Non-repudiation :** Sender cannot deny sending the message because she used her private key to encrypt the hash

4.1.4 Comparison between Hash, MAC and Digital Signature

The Table 4.1.2 summarizes the difference between Hash, MAC and Digital Signatures. Your understanding of these differences is crucial.

Table 4.1.2

Comparison Attribute	Hash	MAC	Digital Signature
Integrity	Yes	Yes	Yes
Authentication	No	Yes	Yes
Non-repudiation	No	No	Yes
Keys Used	None	Symmetric Keys	Asymmetric Keys

4.2 Needham Schroeder Authentication Protocol

Q. What is Authentication? Explain Needham Schroeder Authentication protocol. **MU - Dec. 18, 5 Marks**

Needham Schroeder proposed two authentication protocols – one using symmetric keys and one using asymmetric keys. Let's learn about both of them.

4.2.1 The Needham–Schroeder Symmetric Key based Authentication Protocol

- In symmetric key based authentication protocol, there are 3 entities
- 2 users – let's call them Alice (A) and Bob (B)
- 1 Server (S)

✍ ***Definition :*** *The goal of this protocol to generate and share a key that can be used for securing communication between the two users - A and B.*

Note here that the Needham–Schroeder Symmetric Key Based Authentication Protocol forms a basis for Kerberos based authentication. It solves the key distribution problem.

Assume the following primitives :

- A and B are identities of Alice and Bob respectively
- K_{AS} is a symmetric key known only to A and S
- K_{BS} is a symmetric key known only to B and S
- N_A and N_B are nonce (random number used once) generated by A and B respectively
- K_{AB} is the symmetric key that needs to be generated and shared between A and B for secure communication

4.2.1(A) Protocol Operation

Following is the sequence of activities that the protocol follows :

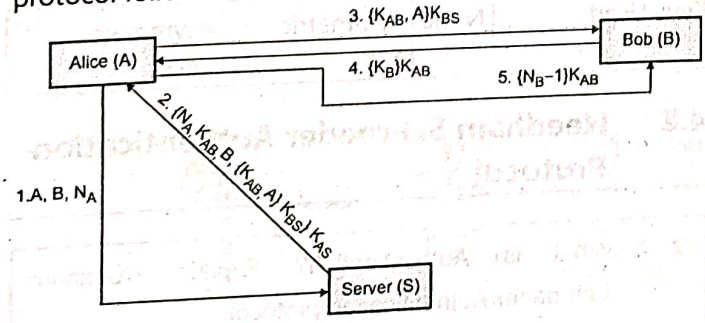

Fig. 4.2.1

1. Alice sends a message to the server identifying herself and telling the server that she wants to communicate with Bob. The server generates K_{AB} and sends it to Alice encrypting the entire response with K_{AS}.
   (a) A copy of K_{AB} is encrypted using K_{BS} for Alice to forward to Bob and also identify herself and
   (b) A copy for Alice herself.
2. Alice forwards the key K_{AB} to Bob. Bob decrypts it with the key K_{BS}.
3. Bob sends Alice a nonce N_B encrypted using K_{AB} to show that he has the key.
4. Alice performs a simple operation on the nonce N_B, re-encrypts it and sends it back verifying that she is still alive and that she holds the key as well.

4.2.1(B) Attack on the protocol

This protocol is vulnerable to replay attack. The attacker can grab the older and compromised value for K_{AB}. He can then replay the message $\{K_{AB}, A\}$ K_{BS} to Bob, who will accept it. Kerberos solves this problem by adding timestamp to avoid replaying older communication.

4.2.2 The Needham–Schroeder Asymmetric Key based Authentication Protocol

In asymmetric key based authentication protocol, there are 3 entities as well

- 2 users – let's call them Alice (A) and Bob (B)
- 1 Server (S)

✍ ***Definition :*** *The goal of this protocol is to share the respective public keys between the two users - A and B.*

Assume the following primitives

- **3 key pairs :** P stands for Public Key, Q stands for Private Key
  - **K_{PA} and K_{QA} :** Public and Private Keys of A respectively
  - **K_{PB} and K_{QB} :** Public and Private Keys of B respectively

- K_{PS} and K_{QS} : Public and Private Keys of S respectively
- K_{PS} is known to both A and B and is trusted

4.2.2(A) Protocol Operation

Following is the sequence of activities that the protocol follows :

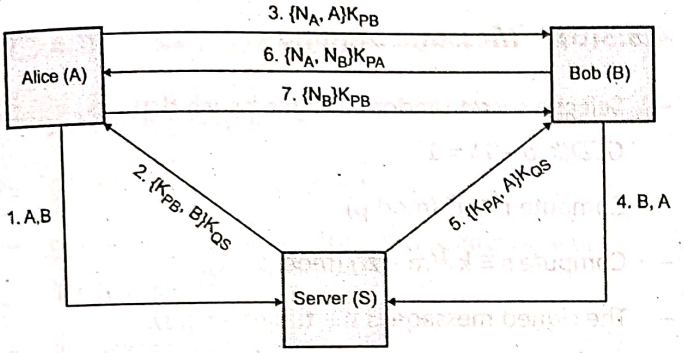

Fig. 4.2.2

1. A requests B's public keys from S
2. S responds with B's public key K_{PB} alongside B's identity, encrypted by the server's private key K_{QS}
3. A chooses a random nonce N_A and sends it to B by encrypting it using B's public Key K_{PB} received in step 2
4. B now knows that A wants to communicate. So, B requests A's public keys from S
5. S responds with A's public key K_{PA} alongside A's identity, encrypted by the server's private key K_{QS}
6. B chooses a random nonce N_B and sends it to A along with N_A to prove his ability to decrypt with K_{QB}
7. A confirms N_B to B, to prove her ability to decrypt with K_{QA}

4.2.2(B) Attack on the Protocol

This protocol is vulnerable to Man-in-the-Middle attack. The attacker can make A and B believe that they are communicating. This could be fixed by updating the step 6 by passing along the identity - $\{N_A, N_B, B\}K_{PA}$. So, A would know who she is actually communicating with instead of being attacked by the middle-man.

4.3 Digital Signature Schemes

There are various schemes to create and verify digital signatures. These schemes are developed and implemented using various encryption and hashing algorithms. Let's learn about a few of them.

4.3.1 RSA Digital Signature Scheme

✍ ***Definition :*** *RSA signatures are based on public key cryptography.*

RSA uses public key cryptography for creating and verifying digital signatures.

4.3.1(A) Key Generation

RSA digital signatures work on public and private key pairs. They can be generated by the regular key pair generating method by a Certificate Authority (CA) or on the user's system by herself. Recall from your reading on RSA algorithm that the keys are as following:

- The public key = *(n, e)*
- The private key = *(n, d)*

4.3.1(B) Message Signing

To sign a message, M

- Calculate the hash value of the message M at sender's end
- h = hash(M)
- Encrypt *h* using RSA private key
- Signature S = $(h)^d \bmod n$

4.3.1(C) Signature Verification

- Decrypt Signature *S* using public key
- h' = $(S)^e \bmod n$
- Calculate the hash value of the message M at receiver's end
- h = hash(M)
- If h = h', the signature is valid else the signature is invalid

4.3.2 Schnorr Digital Signature Scheme

✍ ***Definition :*** *Schnorr signatures are based on discrete logarithm problems.*

Schnorr signatures were developed by Claus P Schnorr and subsequently protected by U.S. Patent until late 2008. As a result of the patent, Schnorr signatures have not been standardized or widely used in crypto libraries today. It is believed to be a more elegant signature solution with a simple mathematical proof.

4.3.2(A) Key Generation

- Choose a private signing key, x
- The public verification key is $y = g^x$ where g is a generator point.

4.3.2(B) Message Signing

To sign a message, M

- Choose a random value k
- Let $r = g^k$
- Let e = Hash (r || M) e
- Let S = k – xe

The signature is the pair(s, e).

4.3.2(C) Signature Verification

- Let $r_v = g^s y^e$
- Let e_v = Hash(r_v|| M)

If $e_v = e$, then the signature is verified.

4.3.3 ElGamal Digital Signature Scheme

✍ ***Definition :*** *The ElGamal digital signature scheme is based on the difficulty of computing discrete logarithms.*

It was conceived by Taher ElGamal in 1984. It is not used widely in the industry today.

Suppose a message m needs to be signed. Following are the set of steps in the scheme.

4.3.3(A) Key Generation

- Choose a large prime p and a primitive root α.
- Choose a secret integer z and calculate $\beta \equiv \alpha z \pmod p$.
- The values of p, α and β are made public and z is kept private.

4.3.3(B) Message Signing

- Select a secret random integer k such that $GCD(k, p-1) = 1$.
- Compute $r \equiv \alpha^k \pmod p$.
- Compute $s \equiv k^{-1}(m - zr) \pmod{p-1}$.
- The signed message is the triplet (m, r, s).

4.3.3(C) Signature Verification

- Compute $v_1 \equiv \beta^r r^s \pmod p$ and $v_2 \equiv \alpha^m \pmod p$.
- The signature is declared valid if $v_1 \equiv v_2 \pmod p$.

4.3.4 Digital Signature Standard (DSS)

✍ ***Definition :*** *National Institute of Standards and Technology (NIST) defined the Digital Signature Standard to provide approved techniques for generating and validating digital signatures for authenticating messages (or any binary data in general).*

It approved three techniques as part of the standard.

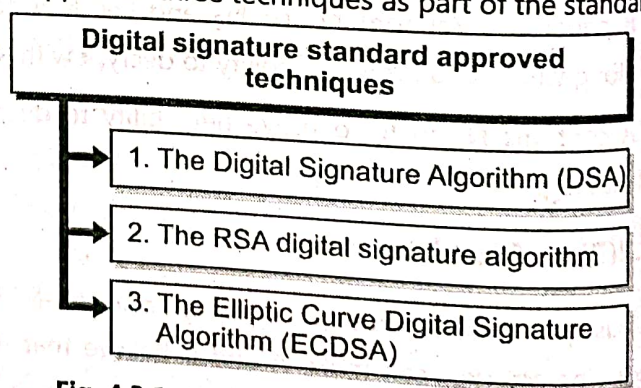

Fig. 4.3.1 : Techniques of digital signature

Out of the three currently listed techniques, DSA was the primary and the original proposal in the standard. Let's learn about it in brief.

4.3.4(A) Digital Signature Algorithm (DSA)

✍ ***Definition** : The Digital Signature Algorithm (DSA) is based on the difficulty of computing discrete logarithms.*

It is based on ElGamal and Schnorr digital signature schemes.

4.3.4(B) Key Generation

- p is a prime number
- q is a prime divisor of $(p - 1)$
- $g = h^{(p-1)/q} \bmod p$ where h is any integer with $1 < h < (p - 1)$
- x is user's private key
- y is user's public key

4.3.4(C) Message Signing

- M is message to be signed
- H(M) = SHA1(M)
- $r = (g^k \bmod p) \bmod q$
- $s = [k^{-1} (H(M) + xr)] \bmod q$
- Signature = (r, s)

4.3.4(D) Signature Verification

- *Assume* M', r', s' are as received at the receiver's end
- $w = (s')^{-1} \bmod q$
- $u_1 = [H(M')w] \bmod q$
- $u_2 = (r')w \bmod q$
- $v = [(g^{u1} y^{u2}) \bmod p] \bmod q$
- v should match r'

Review Questions

Here are a few review questions to help you gauge your understanding of this chapter. Try to attempt these questions and ensure that you can recall the points mentioned in the chapter.

Digital Signature

Q. 1 Write a short note on digital signature and also list its usage. **(4 Marks)**

Q. 2 With suitable diagrams, explain how digital signature works. **(8 Marks)**

Q. 3 List the properties of digital signature. **(4 Marks)**

Q. 4 Compare Hash, MAC, and Digital Signature. **(4 Marks)**

Needham Schroeder Authentication Protocol

Q. 5 With a block diagram, describe the Needham–Schroeder Symmetric Key Based Authentication Protocol. **(8 Marks)**

Q. 6 With a block diagram, describe the Needham–Schroeder Asymmetric Key Based Authentication Protocol. **(8 Marks)**

Digital Signature Schemes

Q. 7 List the steps for key generation, message signing and signature verification in RSA Digital Signature Scheme. **(8 Marks)**

Q. 8 List the steps for key generation, message signing and signature verification in Schnorr Digital Signature Scheme. **(8 Marks)**

Q. 9 List the steps for key generation, message signing and signature verification in ElGamal Digital Signature Scheme. **(8 Marks)**

Q. 10 List the steps for key generation, message signing and signature verification in Digital Signature Algorithm (DSA). **(8 Marks)**

❑❑❑