Jamia Millia Islamia

Dept. Of Computer Science

Cryptography Assignment-4

Submitted By:Wasit Shafi

Roll no:18MCA054

Submitted To:Dr.Rafat Parveen

Question 1: List two disputes that can arise in the context of message authentication.

Solution:

Suppose that John sends an authenticated message to Marry, Consider the following disputes that could arise.

1. Mary may forge a different message and claim that it came from John. Mary would simply have to create a message and append an authentication code using the key that John and Mary share.

2. John can deny sending the message. Because it is possible for Mary to forge a message, there is no way to prove that John did in fact send the message.

Question 2: What are the properties a digital signature should have? Explain.

Solution :

1. **Authenticity :** The authenticity of a signature generated from a fixed message and fixed private key can be verified by using the corresponding public key. A valid signature implies that the signer deliberately signed the associated message.

2. **Unforgeability :** Only the signer can give a valid signature for the associated Message.

3. **Non-re-usability :** The signature of a document can't be used on another document.

4. **Non-repudiation :** The signer can't deny having signed a document that has valid Signature.

5. **Integrity :** Ensure the contents have not been modified.

6. Digital Signature should be computationally infeasible to generate a valid signature for a party without knowing that party's private key.

Question 3: What requirements should a digital signature scheme satisfy?

Solution :

- The signature must be a bit pattern that depends on the message being signed.
- The signature must use some information unique to the sender to prevent both forgery and denial.
- It must be relatively easy to produce the digital signature.
- It must be relatively easy to recognize and verify the digital signature.
- It must be computationally infeasible to forge a digital signature, either by constructing a new message for an existing digital signature or by constructing a fraudulent digital signature for a given message.
- It must be practical to retain a copy of the digital signature in storage.

Question 4 : What is the difference between direct and arbitrated digital signature?

Solution :

S.NO	DIRECT DIGITAL SIGNATURE	ARBITRATED DIGITAL SIGNATURE
1.	It only requires the communicating parties.	It requires arbiter along with communicating parties to send or receive messages.
2.	In this the digital signature encrypts the whole plain text with the sending party's private key.	The encrypted message is sent by X to arbiter Z with Y's id, timestamp and some random number PQ.

3.	The message is directly transmitted between both parties without any help of a intermediate.	Arbiter is needed to transmit the message.
4.	Timestamp is not maintained by both side.	Timestamp is maintained by all three members by default.
5.	In case the confidentiality is needed the message will be encrypt with receiver's public key or a shared key.	The arbiter provides confidentiality of the message.
6.	Vulnerable to any kind of replay attack.	The timestamp is used to protect the message from any kind of replay attack.
7.	It clocks a processing speed of 16 MHz.	While Raspberry Pi clocks a processing speed of 1.4 GHz.
8.	It is implemented using public key.	It is implemented using private key.

Question 5 : In what order should the signature function and the confidently function be applied to a message, and why?

Solution :

It is important to perform the signature function first and then an outer confidentiality function. In case of dispute, some third party must view the message and its signature. If the signature is calculated on an encrypted message, then the third party also needs access to the decryption key to read the original message. However, if the signature is the inner operation, then the recipient can store the plaintext message and its signature for later use in dispute resolution.