Jamia Millia Islamia

Dept. Of Computer Science

Cryptography Assignment-3

Submitted By:Wasit Shafi **Submitted To**:Dr.Rafat Parveen

Roll no: 18MCA054

Question 1: What types of attacks are addressed by message authentication ?

Solution:

The types of attacks are addressed by message authentication are:

1. **Brute force attack:** consists of an attacker submitting many passwords or passphrases with the hope of eventually guessing correctly. The attacker systematically checks all possible passwords and passphrases until the correct one is found

2. **Traffic analysis:** process of intercepting and examining messages in order to deduce information from patterns in communication, which can be performed even when the messages are encrypted.

3. **Masquerade:** Its a type of attack where the attacker pretends to be an authorized user of a system in order to gain access to it or to gain greater privileges than they are authorized for.

4. **Content modification :** **Changes to the contents of the message.**

5. **Sequence modification:** Any modification to a sequence of messages between parties, including insertion, deletion and recording.

6. **Timing modification:** Delay or replay of messages.

7. **Disclosure**

Question 2: What two levels of functionality comprise a message authentication or digital signature mechanism?

Solution:

Two levels of functionality comprise a message authentication or digital signature mechanisms are Low level authentication and High-level authentication. At the lower level there must be some sort of function that produces an authenticator: a value to be used to authenticate a message. This lower level function is then used as primitive in a higher-level authentication protocol that enables a receiver to verify the authenticity of message.

Question 3: What are some approaches to producing message authentication ?

Solution:

Message authentication is a means of ensuring integrity of the message by providing a mechanism of verifying the source of a message and determining if the message may have been modified during transmission.

It can be achieved by:

1.Use of ciphertext : An encryption algorithm E is applied to a message M using a key K to produce an authenticated ciphertext.

2.Use of Tags: A : Tag is attached to the message at source using a tag-generation algorithm .At the receiver ,a tag-verification algorithm is applied to the message to authenticate it.

3.Use of MAC(message authentication code) : This is the case where the tag generation algorithm is stateless and deterministic. A tag-verification algorithm is not needed here.The receiver simply computes T=MACk(M′) to authenticate

Question 4: When a combination of synthetic encryption and an error code is used for message authentication , in what order must the two functions be performed ?

Solution:

Error control code, then encryption.

Question 5: What is a message authentication code?

Solution:

A message authentication code (MAC), sometimes known as a tag, is a short piece of information used to authenticate a message—in other words, to confirm that the message came from the stated sender (its authenticity) and has not been changed. The MAC value protects both a message's data integrity as well as its authenticity, by allowing verifiers (who also possess the secret key) to detect any changes to the message content.

A message authentication code system consists of three algorithms:

- A key generation algorithm selects a key from the key space uniformly at random.
- A signing algorithm efficiently returns a tag given the key and the message.
- A verifying algorithm efficiently verifies the authenticity of the message given the key and the tag. That is, return accepted when the message and tag are not tampered with or forged, and otherwise return rejected.