**German University in Cairo**
**Faculty of Media Engineering and Technology**
**Mervat Abu-Elkheir**
**Ahmad Helmy**
**Mohamed Abdelrazik**

# CSEN1001: Computer and Network Security

Spring Term 2019

# Tutorial 9

## Problem 1 - MAC warm-up

What is a MAC? What are the requirements that a MAC must satisfy to be legitimate?

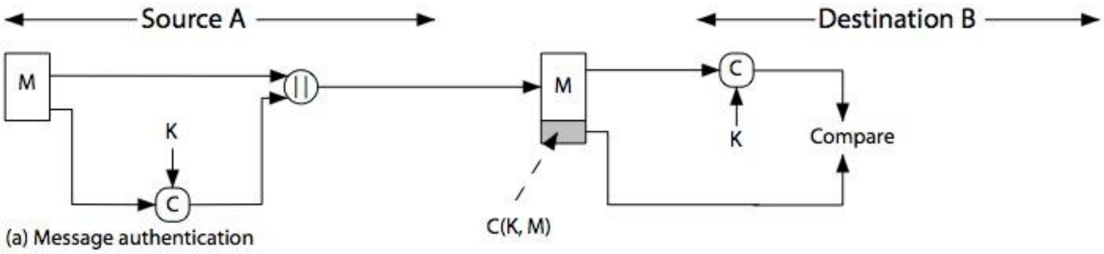
## Answer

MAC stands for Message Authentication Code.

It is generated by an algorithm that creates a small fixed-sized block depending on both the message intended to be sent and some key. Upon sending the message, this block is appended to the message as a signature.

At the receiver's end, the receiver performs the same computation on the received message and checks if it matches the MAC attached.

This process provides assurance that message is unaltered and comes from the claiming sender.



(a) Message authentication

The requirements are:

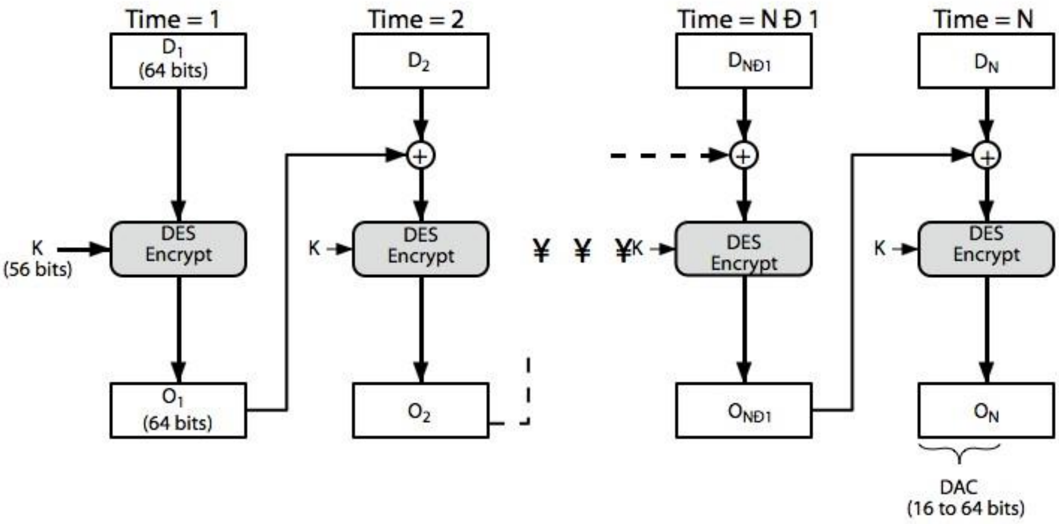
1. Knowing a message and its MAC, it is infeasible to find another message with same MAC
2. MACs should be uniformly distributed
3. MAC should depend equally on all bits of the message

## Problem 2 - MAC

It is noted that given the CBC MAC of a one block message, say T = MAC (K, X), the adversary immediately knows the CBC MAC for the two-block message $X \| (X \oplus T)$ since this is once again T. Justify this statement.

## Answer

For a one-block message, the MAC using CBC-MAC is T = E(K, X), where K is the key and X is the message block.



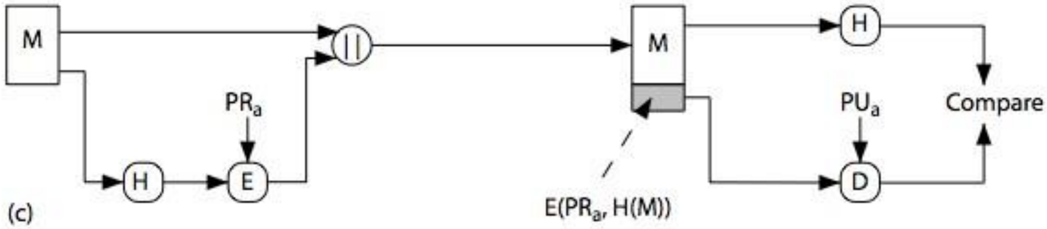
As for the two-block message in which the first block is X and the second block is $X\oplus T$. Then, the MAC is $E(K, [T \oplus (X \oplus T)]) = E(K, X) = T$.

## Problem 3 - Hash

What is a Hash function? What are the requirements that a Hash function must satisfy to be legitimate?

## Answer

A hash function is special function designed to condense an arbitrary message to a fixed size block. It is also attached to the message. The receiver would perform the same function on the sent message and match it with the attachment. This makes sure that integrity holds as a Hash is used to detect changes to a message.



Requirements for Hash Functions:

1. Can be applied to any sized message M
2. Produces fixed-length output h
3. Is easy to compute h=H(M) for any messa
4. Given h, it is infeasible to find x (One-way or Irreversible)
5. Given x is infeasible to find y such that H(y)=H(x) **weak collision resistance**

## Problem 4 - MAC and Hash

What is the difference between a message authentication code and a one-way hash function?

## Answer

A hash function alone does not provide message authentication. A hash function only detects if the message was changed or modified. This ensures integrity, but does not provide a check for authenticity and non-repudiation. A secret key must be used in some fashion with the hash function to produce authentication.
On the other hand, a MAC by definition uses a secret key to calculate a code used for authentication.

## Problem 5 - Message Authentication

Given is a protocol in which the sender performs the following
operation: y = e [(M||H (k2||M)), k1]

M is the message, H is a hash function, e is an encryption algorithm, || denotes simple concatenation, and k1 and k2 are secret keys which are only known to the sender and the receiver. Assume that both the sender and the receiver know the concatenation and de-concatenation structure.

a) Provide a step-by-step description (e.g., with an itemized list) of what the receiver does upon receiving y.

For the following statements, show whether the statement is correct or not:

b) An attacker can alter the Message M.
c) Given protocol does not provide authentication, but non-repudiation will hold.

## Answer

1. Receiver decrypts the message using k1 : d(y, k1) = M||H(k2||M)

2. Receiver de-concatenates the result from the previous operation to get M
3. Receiver prepends the message with k2 then computes the Hash of M resulting in H' (k2||M)
4. Receiver verifies the message signature by checking whether: H' (k2||M)? = H (k2||M)

b) Incorrect.

- In the normal scenario, according to the given k1 and k2 are only known by the sender and receiver, so an adversary would not be able to decrypt the message.
- Even if k1 was leaked/cracked and the attacker was able to obtain M||H(k2||M) after decryption. The adversary still would not know the hash function or k2 to compute the proper hash signature for the altered message. Thus he would be able to see the message, and may be alter it but he would not be able to create a correct signature for the altered message; i.e. the receiver will detect if there were changes.

c) Correct. Although, k1 and k2 are only known by the two communicating parties. Supposedly, they can verify each other's identities.

However, a man in the middle can simply replay the entire message together to the receiver. Hence, the receiver has no way of authenticating the true sender of the message.