## 

## [3413ICT Network Security](file:///C:\Documents%20and%20Settings\s995689\My%20Documents\Teaching\Courses_2013\Courses_2003\6216INT_03\6216inthome.html)

### **Workshop 4B**

**Review the lecture, answer the following questions:**

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

MAC (Message Authentication Code): Guarantees both authentication and integrity. MAC requires a private key while a hash function doesn’t. Has functions guarantee integrity of the message but do not provide authentication.

1. What are the main differences between HMAC and CMAC?

HMAC: Hash Message Authentication Code. Replacing an existing MAC token with a hash function. There are a few benefits to doing this such as having access to more code libraries and being able to swap out the hash function with a different one and still having everything work.  
  
CMAC: Cipher Message Authentication Code: Block cipher that provides authentication and message integrity.

1. What characteristics are needed in a secure hash function?

• disclosure   
•  traffic analysis   
•  masquerade   
•  content modification   
•  sequence modification   
•  timing modification   
•  source repudiation   
•  destination repudiation

1. Compare the three Hash algorithms: MD5, SHA-1, Whirlpool.

MD5: produces 128-bit hash value. The encryption goes through 4 different rounds.  
SHA-1: 160 bit hash values with 3 additional algorithms. SHA-256/384/512. Designed with comparability provided by the AES cipher.  
Whirlpool: Based on AES-like block algorithm that uses an 8x8 state matrix and produces a 512bit digest. The state goes through 4 different functions (SubByte, ShiftColumn, MixRows, AddRoundKey) over 10 rounds.

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

- Private key could be compromised so the sender’s identity could be stolen buy would show up as valid  
- Brute force attach  
- Birthday attack

1. What are the properties a digital signature should have?

* Signatures depend on the message signed
* It uses information unique to sender, to prevent both forgery and denial
* Signature creation/verification are efficient
* It is computationally infeasible to forge
  + with new message for existing digital signature
  + with fraudulent digital signature for given message

1. What problem was Kerberos designed to address?  
   Centralized 3rd party private key authenticator. This allows users in a network to access the services available without having to trust the all the workstations. Instead, only one server needs to be trusted, Kerberos.
2. What four requirements were defined for Kerberos?  
   Security  
   Reliability  
   Transparency  
   Scalability
3. What is the purpose of the X.509 standard?

Defines a framework for authentication services. Directory may store public key certificates & digital signatures. Also defines authentication protocols.

1. How is an X.509 certificate revoked?

Expires after a period of time  
Private Key is compromised  
User is no longer certified by CA  
C.A certificate is compromised