# CS808: Computer Security Fundamentals

## 2.12: Cryptography Questions

Crypto Questions

# Cryptography Comprehension Questions

## Question 1

Block ciphers can operate in either ECB mode or CBC mode.

a) Explain the difference between these two modes of operation. What extra information is required for CBC which isn't required for ECB?

b) Construct a scenario which demonstrates the weakness of ECB mode.

## Question 2

What are the three properties which make a hash function a cryptographic hash function, and why are they important?

## Question 3

a) What form of attack can a MAC help mitigate? b) How does a MAC mitigate this? c) Why can't we simply append a hash value to the end of the encrypted data to mitigate the attack?

## Question 4

a) Compare and contrast p-boxes and s-boxes b) How does AES use p-boxes and s-boxes?

## Question 5

In your own words, explain how a digital signature mitigates an attack in which the attacker intercepts the communication from sender to recipient and replaces the document with their own document.

## Question 6

You and a friend have public and private key pairs. a) How can you send secret messages to each other? b) What could information security property could you achieve if you encrypted a message with your private key and released the cipher text? c) How could you combine encryption using different keys to provide confidentiality and authenticity?

# Cryptography Scenario-based Questions

## Question 1

Alain Thénardiers often uses his company's secure email server. He has lost his private key, but still has the corresponding public key. a) Is he still able to send encrypted emails? What about receiving? b) Is he still able to sign the email he sends? What about verifying the signatures of emails he received? c) What must he do to be capable of carrying out all of the operations above?

## Question 2

A group of n people would like to use a public key encryption system to exchange confidential information pairwise. That is each person should be able to communicate privately with each other person in the group, without anyone else being able to read the message.

### a)

Bob would like to send Alice encrypted and signed information. They are both members of the group. What keys must Bob use to achieve this?

### b)

Name a well-known asymmetric encryption system, explain how it works The group has decided to use a hybrid system – using a combination of asymmetric and symmetric encryption.

### c)

Why might the group have decided to do this?

## Question 3

Demonstrate how RSA generates keys using p=2, q=7.

## Question 4

Your friend Miriam (who lives next door) has decided she'd like to share a file with you, but only with you. She's decided to encrypt the file before sending it to you.

a) What type of encryption (symmetric or asymmetric) should she use? Given your choice, propose a specific algorithm and explain to her on a high level how it works. b) Miriam doesn't know how Diffie-Hellman relates to public key encryption, explain how they are related.

## Question 5

Design a cipher which uses a Fiestel structure. Note it need not meet the formal requirements of a secure cipher.

Last modified: Tuesday, 24 September 2024, 5:01 PM

◄ 2.11: Lab: OpenSSL for AES

Jump to...

2.13: Discussion: Pre lecture session question forum ►