University of Oslo
INF3510 Information Security
Spring 2012
Workshop Questions

Lecture 5: Cryptography

Question 1

In which situations and for which purposes can cryptography be used to protect information?

Question 2

Alice wants to send a message to Bob, without Eve observing it. Alice and Bob have agreed to use a symmetric cipher. Key exchange has already occurred, and so they share a key K. Outline the steps that Alice and Bob must follow when they encrypt and decrypt, respectively.

Question 3

Alice wants to send a message *M* with a digital signature *Sig*(*M*) to Bob. Alice and Bob have an authentic copy of each other's public keys, and have agreed on using a specific hash function *h*. Outline the steps that Alice must follow when signing *M*, and the steps that recipient Bob must follow for validating the signature *Sig*(*M*).

Question 4

Suppose that a binary additive stream cipher (such as the one time pad) has been used to encrypt an electronic funds transfer. Assuming that no other cryptographic processing is used, show that an attacker can change the amount of the funds transfer without knowing anything about the key used. (You may assume that the attacker knows the format of the plaintext message used for the funds transfer.)

Question 5

Hash functions are commonly used for checking message integrity.

a. List four basic requirements of hash functions
b. Use the internet to locate an SHA-1 demonstration tool — there's an interactive one written by Eugene Styer that can be used at http://people.eku.edu/styere/Encrypt/JS-SHA1.html. Investigate the four properties by examining the SHA-1 hashes for the following messages:
(i) Take $100 from my account
(ii) Take $1000 from my account
(iii) Take $100 from your account
(iv) Investigate other hashes for both longer and shorter messages

Question 6

Alice wants to send a message to Bob. Alice wants Bob to be able to ensure that the message did not change in transit. Briefly outline the cryptographic steps that Alice and Bob must follow to ensure the integrity of the message by creating and verifying a *MAC*.

Question 7

a. What is a the meaning of the term MAC ?
b. What is the difference between a MAC and a hash function?
c. In what ways can a hash value be secured so as to provide message authentication?
d. Imagine that a specific hash function is used for HMAC, and that vulnerabilities have been found in the hash functions so that the HMAC is insecure. Which changes in the HMAC are required in order to make it secure again?

Question 8

a. Explain why message authentication alone is insufficient as proof of message origin in general, and to settle disputes about whether messages have been sent.
b. What security service is provided by digital signatures, and explain how this service relates to message authentication.
c. In what order should the signature function and the encryption function be applied? Also explain why that order makes sense.
d. How can a sender give a plausible reason for repudiating a signed message?

Question 9

The Diffie-Hellman key agreement algorithm achieves key agreement by allowing two hosts to create a shared secret.

a. Clearly explain the operation of the Diffie–Hellman key exchange protocol.
b. Clearly explain why the basic Diffie–Hellman protocol does not provide any assurance regarding which other party the protocol is run with.