University of Oslo
INF3510 Information Security
Spring 2010
Workshop Questions

Lecture 2: Cryptography

Question 1

In which situations can cryptography be used to protect information? Justify your answer.

Question 2

a. What is the main difference between encoding and encryption?
b. What is required to perform the decoding and decryption processes?

Question 3

Alice wants to send a message to Bob, without Carol (or other eavesdroppers) 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 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

a. Suppose that a single ciphertext bit of a received ciphertext message has been modified. How many bits should be expected to be in error in the decrypted plaintext in the following cases:
    1. the cipher is a binary additive stream cipher;
    2. the cipher is a block cipher operating in electronic codebook (ECB) mode;
    3. the cipher is a block cipher operating in cipher block chaining (CBC) mode.
b. Suppose now that a single ciphertext bit of a received message has been deleted. What happens now in each case?

Question 6

Hash functions are commonly used for checking message integrity.

a. List four basic properties 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 7

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 6

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 each participant in the basic Diffie–Hellman protocol has no assurance which other party the protocol is run with.

Question 7

The Diffie-Hellman key exchange is to be used to establish a shared secret key between Alice and Bob. Alice and Bob have agreed to use the prime $p = 17$ and base value $g = 3$.

a. Enumerate all the values $g^1 \bmod 17$, $g^2 \bmod 17$, . . . , $g^{16} \bmod 17$, and show that this gives all the values {1, 2, . . . , 16}.
b. If Alice chooses the random value $a = 4$, what value does Alice send to Bob?
c. If Alice receives the value 11 from Bob, what is the value of the shared secret key?

Question 8

Perform encryption and decryption using the RSA algorithm for the following (where M is the plaintext message):

a. p = 3, q = 11, e = 7, d = 3,M = 5
b. p = 5, q = 17, e = 5, d = 13,M = 8