University of Oslo
IN2120 Information Security
Autumn 2018
Workshop Questions

Lecture 2: Cryptography

Question 1

For which information states (storage, transmission, processing) and for which security services can cryptography be used to protect information?

Question 2

Alice wants to send message *M* to Bob, without Eve observing it. Alice and Bob have agreed to use a symmetric cipher. Key exchange has already been done, and so they share a key *K* for a specific encryption algorithm E.

a. Outline the steps that Alice must follow for encrypting *M* and sending it to Bob.
b. Outline the steps that Bob must follow for decrypting the received ciphertext *C*.

Question 3

Alice wants to send a message *M* with a message authentication code MAC(*M*) to Bob. Alice and Bob share a secret key *k*, and have agreed on using a specific algorithm MACfunc which takes input parameters *M* and *k* to produce MAC(*M*).

a. Outline the steps that Alice must follow for sending *M* .
b. Outline the steps that recipient Bob must follow for verifying the authenticity of *M*.
c. Explain why the MAC proves to Bob that a received message is authentic, and why Bob is **unable** to prove to a third party that the message is authentic.

Question 4

Alice wants to send message *M* with digital signature Sig(*M*) to Bob. They have each other's public keys, and have agreed on a specific hash function h and a signature algorithm that operates in signature mode S (equivalent to Decryption mode D) or in verification mode V (equivalent to Encryption mode E).

a. Outline the steps that Alice must follow for sending *M*.
b. Outline the steps that recipient Bob must follow for verifying the authenticity of *M*.
c. Explain why the digital signature proves to Bob that a received message is authentic, and why Bob is **able** to prove to a third party that the message is authentic.
d. How can a sender give a plausible reason for repudiating a signed message?
e. Discuss the semantic interpretation of 'digitally signed', i.e. does it mean that i) Alice agrees with the content of the message, or ii) Alice sent the message without necessarily agreeing to its content ?

Question 5

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 6

Hash functions are commonly used for checking message integrity.

a. List the four basic requirements of cryptographic hash functions

b. What's the difference between the two variants of collision resistance ?

c. Use the internet to locate a SHA-2 demonstration tool — there's an interactive one written by Geraint Luff that can be found at: http://geraintluff.github.io/sha256/
Investigate hash function properties by computing SHA-2 hashes for the following:
(i) Take $100 from my account
(ii) Take $1000 from my account
(iii) Take $100 from your account
(iv) (You can try other hashes for both longer and shorter messages)

Question 7

In case a message needs confidentiality **and** integrity/authenticity/non-repudiation: in what order should the signature function and the encryption function be applied? Also explain why that order makes sense.

Question 8

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.

Question 9

Quantum computing has the potential of making obsolete and insecure most of the standardized asymmetric cryptographic algorithms. Assume the following time periods:

- t_1: the time it takes to standardize quantum-resistant crypto (QRC) algorithms.
- t_2: the time it takes to update crypto applications with standardized QRC algorithms.
- t_3: the time that legacy non-QRC applications must remain operational and secure
- t_4: the time it takes to make large-scale quantum computers practical

a. Express in terms of inequality equations with the terms t_1, t_2, t_3 and t_4 two scenarios:
Scenario 1 where crypto applications will remain secure
Scenario 2 where crypto applications will become insecure

b. What is the expected time frame for standardizing quantum-resistant algorithms? See http://csrc.nist.gov/groups/ST/post-quantum-crypto/documents/pqcrypto-2016-presentation.pdf