COMP 38411

Two hours

UNIVERSITY OF MANCHESTER
SCHOOL OF COMPUTER SCIENCE

Cryptography and Network Security

Date: Wednesday 24th January 2018

Time: 14:00 - 16:00

Please answer all THREE Questions.

This is a CLOSED book examination

The use of electronic calculators is NOT permitted

[PTO]

1. A hash function, message encryption and Message Authentication Code (MAC) are three types of functions that may be used to produce a message authenticator (that is sometimes also called MAC). Answer the following questions.

   a) What are the fundamental differences among these three types of functions?

   (6 marks)

   b) Name and explain 4 properties a hash function should have for it to be cryptographically secure and of practical application.

   (4 marks)

   c) Describe how an authenticator can be constructed from a hash function, and how an authenticator can be constructed from a block cipher.

   (4 marks)

   d) Name and explain *three* security properties that can be provided by using a message authenticator.

   (6 marks)

2. Ciphers can be classified into two main types, block ciphers and stream ciphers. Answer the following questions.

   a) Block ciphers are usually designed to provide confusion and diffusion. Explain what is meant by each of these properties, and give examples of the features of block ciphers, which are used to provide them.

   (4 marks)

   b) Describe the Advanced Encryption Standard (AES) with reference to (use diagrams if necessary): encryption, block size, key size, number of rounds. Describe how AES provides confusion and diffusion.

   (10 marks)

   c) Use diagrams to show how a stream cipher is built from the AES cipher. The diagrams should indicate how encryption and decryption operations are carried out using the implemented stream cipher. Compare and contrast stream ciphers with block ciphers.

   (6 marks)

[PTO]

3. A company has been given a job of designing an Air Space Control system. The system should be able to tell (within a few seconds) if an aircraft appearing on their radar is authorised. If the aircraft is authorised to use the air space, then the system will not take any further action. Otherwise, the system will issue an instruction for a military action to be taken to bring down the aircraft. After some research, the company has come up with a solution. In this solution, authorised aircrafts and the air traffic controller (AirTrafficController) are each issued with a pre-shared secret key, *K*. At run time, AirTrafficController uses a challenge-response protocol to verify any incoming aircraft. This protocol consists of two messages, a challenge and a response, as shown below:

   I. $A \rightarrow B: n;$
   II. $B \rightarrow A: \mathrm{E}(K, n);$

   Where message I is the challenge that is sent by *A* (AirTrafficController) to *B* (any incoming aircraft), message II is *B*'s response to the challenge, *n* is a unique random nonce, *K* is the pre-shared secret that is known to all the authorised aircrafts and AirTrafficController, and *E* is an encryption function (or a secure one-way cryptographic function).

   Answer the following questions.

   a) Can this protocol be used to identify any unauthorised aircraft? You should justify your answer. Also explain the purpose for the use of the nonce in this protocol.

   (4 marks)

   b) Analyse the security of this protocol, identifying at least *three* threats or attacks that may compromise the security of this protocol (i.e. the threats or attacks by which an enemy aircraft, or an unauthorized aircraft, can successfully invade the air space). For any threats or attacks you have identified, describe how they are mounted.

   (10 marks)

   c) For each of the threats or attacks you have identified in b), describe a countermeasure.

   (6 marks)

END OF EXAMINATION