COMP 38411

Two hours

UNIVERSITY OF MANCHESTER
SCHOOL OF COMPUTER SCIENCE

Cryptography and Network Security

Date:	Friday 27th January 2017
Time:	09:45 - 11:45

Please answer any THREE Questions from the FOUR Questions provided

This is a CLOSED book examination

The use of electronic calculators is NOT permitted

[PTO]

1. Data Encryption Standard (DES) and Advanced Encryption Standard (AES) are two symmetric block ciphers. Answer the following questions.

   a) Compare and contrast the two block ciphers with respect to the following (use diagrams if necessary): the number of rounds used in each cipher, transformations (i.e. basic operations) used in each round, block sizes and key sizes.

   (8 marks)

   b) Compare and contrast the Electronic Cook Book (ECB) and Ciphertext Block Chaining (CBC) modes of operation for block ciphers with respect to the following (use diagrams if necessary): encryption, decryption and error propagation.

   (8 marks)

   c) Use diagrams to show how a block cipher can be used to implement a stream cipher. The diagrams should indicate how encryption and decryption operations are carried out using the implemented stream cipher.

   (4 marks)

2. RSA is a well-known public-key cryptosystem. You are now given two large primes, p and q, and a cryptographic hash function $H(x)$. Answer the following questions.

   a) Explain how RSA public and private keys are generated. Give mathematical equations if necessary. You should also indicate any parameter values that should be keep secret in this process.

   (6 marks)

   b) Give the equation to encrypt a message M to achieve confidentiality using the RSA cryptosystem, and the equation to decrypt the ciphertext to recover the message.

   (4 marks)

   c) Design a protocol along with any necessary procedure so that you can follow the procedure and use this protocol and the keys generated in step 2a) above to send a large message M to a group of unknown recipients. The protocol should provide protections against *impersonation*, *replay*, and *unauthorised modification* attacks. In your answer, the respective operations performed by the sender and the recipients, including any mathematical equations, should be described as well.

   (10 marks)

[PTO]

3. Symmetric key distribution is a challenging task for the adoption of symmetric ciphers. Answer the following questions.

   a) When distributing a symmetric key to another entity over a communication network, there are security threats or issues one should consider. Name and explain four possible threats in a symmetric key distribution process.

   (4 marks)

   b) Design a protocol for symmetrical key distribution between two parties, *Alice* and *Bob*, over a communication network without any assistance of a public-key cryptosystem. You may make any necessary assumption, but it is assumed that *Alice* and *Bob* have never met before.

   (6 marks)

   c) Design a method using the Diffie-Hellman protocol so that three parties, *Alice*, *Bob* and *Carole*, could establish a shared secret (symmetrical) key (i.e. to establish a secure shared channel among the three parties).

   (6 marks)

   d) Name and explain the well-known vulnerability in the Diffie-Hellman protocol, and give a solution to address this vulnerability.

   (4 marks)

4. Alice is planning to travel around the world, and is considering to install a mobile app on her smart phone and to use it to book her travel. Installing such a mobile app will obviously make Alice's travel a lot more convenient, but it will also introduce many new security threats or attacks.

   Answer the following questions.

   a) Draw an attack tree, where the goal of the attack is to modify Alice's travel bookings made through the mobile app installed on her smart phone. The tree should at least have FIVE leaf nodes, each capturing a unique security attack, and the attacks may lead to unauthorised modifications of her travel bookings. The names of the attacks you identify and how the attacks are mounted should be clearly outlined.

   (10 marks)

   b) For each identified attack, explain a preventive countermeasure.

   (10 marks)

END OF EXAMINATION