Two hours

UNIVERSITY OF MANCHESTER
SCHOOL OF COMPUTER SCIENCE

Cryptography

Date: Tuesday 24th January 2012
Time: 09:45 - 11:45

Please answer question ONE and TWO other questions

Question 1 is worth 10 marks. Questions 2-4 are worth 20 marks each.

This is a CLOSED book examination
The use of electronic calculators is NOT permitted
1. **COMPULSORY**

   a) What is the main difference between a **passive attack** and an **active attack**?  
      (1 mark)

   b) Write down the main difference between a **chosen plaintext attack** and a **chosen cyphertext attack**.  
      (1 mark)

   c) In breaking Enigma, what was the main idea that led to success?  
      (1 mark)

   d) Write down the main difference between a **block cypher** and a **stream cypher**.  
      (1 mark)

   e) What are the permitted sizes for a finite field?  
      (1 mark)

   f) Write down the four stages of an AES encryption round.  
      (1 mark)

   g) What is a **pseudo-random number generator**?  
      (1 mark)

   h) Write down the main difference between **private key cryptography** and **public key cryptography**.  
      (1 mark)

   i) What is an elliptic curve over a finite field?  
      (1 mark)

   j) Write down the hard problem whose difficulty the Diffie-Hellman key agreement protocol relies on.  
      (1 mark)
2. a) Describe the structure of a round of a Feistel cipher. (5 marks)

b) Describe the structure of a round of the AES cipher. (5 marks)

c) Describe the difference between a pseudo random number generator and a true random number generator. How do you guard against bias in a true random number generator? (4 marks)

d) Describe the Diffie-Hellman key agreement protocol. (6 marks)

3. a) Explain the following terms in relation to the practical use of a block cipher in block mode: electronic codebook, cypher block chaining. (10 marks)

b) In the practical use of a block cipher in stream mode, which of the following modes allow the precomputation of the encryption stream: cypher feedback, output feedback, counter? (2 marks)

c) Give an explanation of the working of one of the stream mode methods in part (b). (5 marks)

d) In the counter stream mode method of operation, why would it be insecure to reuse the key and starting counter value for two different messages? (3 marks)

4. a) Describe DSA signature generation and verification. Explain how signature verification works. (10 marks)

b) Describe the Eckert E91 quantum key distribution algorithm. (10 marks)

END OF EXAMINATION