Two hours

Question ONE is COMPULSORY

UNIVERSITY OF MANCHESTER
SCHOOL OF COMPUTER SCIENCE

Cryptography

Date: Monday 20th January 2014
Time: 14:00 - 16:00

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

[PTO]
1. **COMPULSORY**

   a) Write down three of the six security services that are considered in the X.800 international standard. (1 mark)

   b) Why do the 26! different possible keys in a monoalphabetic substitution cipher not provide any real security against cryptanalysis? (1 mark)

   c) Consider a block cipher working on 64 bit blocks. How many possible block ciphers are there in the ideal case? How many are there if a key of 64 bits is used? (1 mark)

   d) Write down three important design considerations for a Feistel cipher. (1 mark)

   e) What is a group? What can you do in a ring that you cannot do in a group? What can you do in a field that you cannot do in a ring? (1 mark)

   f) What is the main difference between DES and AES? (1 mark)

   g) What is the difference between the CBC and CFB modes when data blocks are changed during encryption? (1 mark)

   h) What is the Birthday Paradox? (1 mark)

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

   j) What is the main difference between the E91 quantum key distribution protocol and the BB84 and B92 quantum key distribution protocols? (1 mark)

2. a) Describe the working of the Enigma machine. Why was it possible to use the same process for encryption as for decryption? (10 marks)

   b) In the context of block ciphers, what is an S-box? (3 marks)

   c) Explain how S-boxes are applied in DES. (3 marks)

   d) Explain why the Galois field GF(7) can be implemented using numbers, but the Galois field GF(8) cannot. (4 marks)
3. a) Describe the RSA public key cryptography scheme. (6 marks)
    b) Why, when looking for candidate primes to use in practical applications of RSA, is the Miller-Rabin algorithm run many times? (3 marks)
    c) Describe the Diffie-Hellman key agreement protocol. (3 marks)
    d) Describe two ways in which a block cipher can be used to implement a pseudorandom number generator. (4 marks)
    e) Give a description of the ANSI X9.17 pseudorandom number generation algorithm, including a suitable diagram. (4 marks)

4. a) Suppose that a straight line intersects a real elliptic curve in one point. What can you deduce? (1 mark)
    b) Suppose that a straight line intersects a real elliptic curve in two points. What can you deduce? (1 mark)
    c) Describe the ElGamal encryption scheme using elliptic curves. (8 marks)
    d) Describe DSA signature generation and verification. Explain how signature verification works. (10 marks)

END OF EXAMINATION