Two hours

UNIVERSITY OF MANCHESTER
DEPARTMENT OF COMPUTER SCIENCE

Cryptography

Date: Friday 24th January 2020

Time: 14:00 - 16:00

Please answer all THREE Questions

Question 1 is worth 10 marks. Questions 2 and 3 are worth 20 marks each

---

This is a CLOSED book examination

The use of electronic calculators is NOT permitted

1. a) Give four examples of modern malware. (1 mark)

   b) What is a **product cipher**? Why were product ciphers important in the development of modern cryptography? (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) In breaking Enigma, what was the main idea that led to success? (1 mark)

   e) How can XTS-AES be exploited in ransomware? (1 mark)

   f) Write down three possible ways that cryptography could make use of a pseudo-random number generator. (1 mark)

   g) Briefly explain the terms **one-way function** and **trapdoor one-way function**. (1 mark)

   h) What is the hard problem used in **elliptic curve cryptography**? (1 mark)

   i) Why is it that in certain public key cryptographic tasks, discrete log problems in prime fields can be substituted by elliptic curve techniques? (1 mark)

   j) Why is **Weisner Quantum Money** secure? (1 mark)

2. a) Describe the structure of AES. (7 marks)

   b) Describe the RSA public key cryptography scheme. (6 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) Name two pseudo random number generators. (3 marks)

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

b) Describe the ElGamal public key encryption and decryption algorithms. (5 marks)

c) Briefly describe the principles behind digital signatures. (3 marks)

b) Describe the *Keywrap* algorithm. (6 marks)

END OF EXAMINATION