

Two hours

**UNIVERSITY OF MANCHESTER  
SCHOOL OF COMPUTER SCIENCE**

Cryptography

Date: Friday 26th January 2018

Time: 14:00 - 16:00

---

**Please answer all THREE Questions.**

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

---

This is a CLOSED book examination

The use of electronic calculators is NOT permitted

**[PTO]**

1.

- a) Give four examples of modern malware. (1 mark)
- b) What is a product cypher? Why were product cyphers important in the development of modern cryptography? (1 mark)
- c) Write down three important design considerations for a Feistel cipher. (1 mark)
- d) Briefly explain the term **triple DES**. Why are multiple DES encryptions genuinely stronger than a single DES encryption? (1 mark)
- e) Which algorithm is used to find the inverse of an element in a finite field? (1 mark)
- f) Describe briefly the **Blum-Blum-Shub pseudo-random number generator**. (1 mark)
- g) What property is possessed by counter mode, that is not possessed by any other standard block cipher mode? (1 mark)
- h) What is the most important property of digital signatures? (1 mark)
- i) Why does quantum factoring not constitute a threat to RSA? (1 mark)
- j) What is keywrapping good for? (1 mark)

2.
  - a) Describe the structure of a round of a Feistel cypher. (3 marks)
  - b) Describe the *Extended Euclid Algorithm* for finding not only the GCD of two numbers  $x$  and  $y$ , but also the coefficients  $a$  and  $b$  such that  $\text{GCD}(x, y) = ax + by$ . (4 marks)
  - c) Describe the RSA public key cryptography scheme. (6 marks)
  - d) What defence does Optimal Asymmetric Encryption Padding provide against malevolent manipulation of the final cyphertext produced? (4 marks)
  - e) Describe the Diffie-Hellman key agreement protocol. (3 marks)

3.
  - a) Describe the structure of AES. (6 marks)
  - b) Explain the RSA-PSS digital signature scheme. (5 marks)
  - c) What useful property does the RSA-PSS digital signature scheme have? (2 marks)
  - d) Describe the ElGamal encryption scheme using elliptic curves. (7 marks)

**END OF EXAMINATION**