This question paper consists of 3 printed pages, each of which is identified by the Code Number COMP3223.

This is a closed book examination. No material is permitted.

School of Computing

MAY 2018

COMP3223

Cryptography

Answer all THREE Questions

Time allowed: Two hours

The marks available for each question are given in brackets after the question.
Candidates should look at these marks and allocate the time they spend on each question accordingly.

Question 1

Consider the differences between symmetric and asymmetric cryptosystems.

(a) Assume that there are n participants, and each participant wants to communicate with everyone else.

(i) How many keys are needed in total when a *symmetric* cryptosystem is used? Please give reasons. (You can use the O-notation in your answer.) **[1 mark]**

(ii) How many keys are needed in total when an *asymmetric* cryptosystem is used? Please give reasons. (You can again use O-notation.) **[1 mark]**

(b) List advantages and disadvantages of asymmetric cryptosystems compared to symmetric cryptosystems, considering in particular arrangements for key exchange and running times of the systems. **[4 marks]**

(c) What is a hybrid system? **[2 marks]**

(d) Name two modern symmetric cryptosystems and two modern asymmetric cryptosystems. **[4 marks]**

(e) Is there a cryptosystem with perfect security? If yes, give details of the cryptosystem. **[4 marks]**

[question 1 total: 16 marks]

Question 2

Assume Alice and Bob are two participants who have not met before, but want to agree on a common key via the Diffie-Hellman key exchange. Choose the modulus $p = 11$ and the generator $g = 2$.

(a) Verify that $g = 2$ is indeed a generator. **[3 marks]**

(b) State the algorithm for efficient computation of exponentiation modulo p in pseudocode. **[4 marks]**

(c) Compute the joint key if Alice chooses $a = 6$ and Bob $b = 9$. State all steps of the computation. **[5 marks]**

[question 2 total: 12 marks]

CONTINUED ON FACING PAGE

Question 3

(a) Explain the RSA cryptosystem. Give full details of the keys and the encryption and decryption functions. **[6 marks]**

(b) Let $n = 91$, $e = 19$ be Bob's public key in the RSA cryptosystem. Use the extended Euclidean algorithm to compute Bob's private key. State all steps of the computation. **[6 marks]**

[question 3 total: 12 marks]

[grand total: 40 marks]

END