University of Glasgow

**Tuesday 8 May 2018**
**9.30 am – 11.00 am**
**(Duration: 1 hour 30 minutes)**

**DEGREES OF MSc, MSci, MEng, BEng, BSc,MA and MA (Social Sciences)**

# Crypto and Secure Development M

**(Answer All Questions)**

**This examination paper is worth a total of 60 marks**

**The use of a calculator is not permitted in this examination**

**INSTRUCTIONS TO INVIGILATORS**

**Please collect all exam question papers and exam answer scripts and retain for school to collect. Candidates must not remove exam question papers.**

**1.** Describe the main weakness of integer arithmetic when used to implement encryption algorithms and show with the aid of an example how this is overcome by using integers modulo n. How does the homomorphism theorem make it easier to implement encryption algorithms? Describe an algorithm for solving the equation $ax \equiv 1 \mod n$. Are there any situations when your algorithm will fail? Use your algorithm to solve the equation $3x \equiv 1 \mod 17$.

[10]

**2.** Define the term "The entropy of a set of messages" and show how it can be calculated. Now define the term "unicity distance." What information is needed to calculate it, and how useful is the concept of unicity distance?

[5]

**3.** Alice is in charge of security at the GameSoft software company. She has to devise the encryption scheme whereby the order for just the right form of brain enhancing pastries is delivered to the local shop so that the programmers can continue working to their tight deadlines without loss of energy. It is important that the rival SoftGame company does not get hold of the order and inspire their own programmers to equal endeavours. She also knows that operative Bob, who has to deliver the encrypted order, is not very brave, and will disclose the key after only the slightest pressure, such as an hour without coffee. Devise a scheme for Alice, based on letter substitutions, which will allow Bob to divulge a key safe in the knowledge that his torturers will not find out the secret GameSoft donut order. Instead they will find a different order for an inferior brand of pastry, guaranteed to send their programmers to sleep within half an hour. You should provide precise details of your algorithm.

[6]

**4.** (a) A bank has decided to use a digital key to operate the locks of its safes. To guard against fraud the key will be split between two employees, who both have to present their part of the key simultaneously. One approach would be to give each employee half of the digits in the key. Explain why this is not a good approach. Describe in detail a scheme where each employee is given a key with as many digits as the full key, but both keys are needed to open the safe.

[5]

(b) The above scheme operated well for a while, but then one of the employees lost his key and the bank was unable to operate until new keys were issued and installed in the safe. Describe in detail a scheme where three different keys are issued to three employees but only two are needed to open the safe.

[7]

**5.** (a) Describe the RSA algorithm for public key encryption and explain why it works. Show how it can be used to sign a document.

[6]

(b) What is a blind signature and what are the benefits of using one? Show how the RSA algorithm can be used to produce blind signatures. Give one way that the person performing the blind signature can ensure that he is not swindled.

[6]

**6.** (a) One of the challenges when implementing a digital currency is preventing double spending. Describe in detail how this is prevented in Bitcoin.

[5]

(b) Describe the structure of a Blockchain and explain why it is a useful data structure for digital currency.

[4]

(c) In Bitcoin, copies of the ledger are distributed over a number of nodes, each with equal status. Explain how Bitcoin makes sure that the nodes are all in agreement, even when some are dishonest. How does it prevent a Sybil attack?

[6]