THE UNIVERSITY OF WARWICK
First Year Examinations: Summer 2015
CS1400 Computer Security

Time allowed: 2 hours
Calculators may be used.
Attempt **ALL** questions from Section A and **THREE** questions from Section B.
Read carefully the instructions on the answer book and make sure that the particulars required are entered on each answer book.

Section A Each question in Section A is worth 4 marks

1. Explain what privacy, integrity, authentication and non-repudiation mean in security. [4]

2. (a) State a common feature of viruses and worms and a difference between viruses and worms [2]

(b) Explain what is a buffer overflow attack and describe a measure to prevent a buffer overflow attack. [2]

3. What is hashing and what is encryption in security? Explain the differences between hashing and encryption [4]

4. What is an entropy value for passwords? Explain the general principles which are used for increasing password entropy. [4]

5. What is Discretionary Access Control (DAC)? There are two ways to represent the permissions in DAC, namely, Access Control Lists and Capabilities. Explain how Access Control Lists and Capabilities store permissions. [4]

6. Permutation and substitution are two common methods to help generate cipher texts. What are the permutation and the substitution methods? Explain how frequency analysis can be used to crack long cipher texts. [4]

7. What is a one way function in security? Give two one way functions that are used in encryption. [4]

8. Assume Alice and Bob use the Diffie-Hellman-Merkle (DHM) key exchange protocol to establish a secret key. Assume Alice and Bob choose 8 and 11 as the secret numbers, respectively. What is the secret key exchanged between them? You should show the main steps used in the DHM protocol to establish the secret key. [4]

9. Discuss why public key encryption algorithms, such as RSA, are generally much slower than secret key encryption algorithms, such as AES. [4]

10. Explain how digital signatures protect data integrity. [4]

Section B Each question in Section B is worth 20 marks; Attempt **THREE** questions

11. (a) Assume that Alice sends a message to Bob and the public key encryption algorithm is used to encrypt the message. Explain which key Alice uses to encrypt the message and how Alice authenticates Bob. [6]

(b) There are two general mechanisms to achieve authentication: Certificate Authority (CA) and Web of Trust. Discuss the differences between these two mechanisms. [8]

(c) What is a replay attack? Give two solutions to prevent replay attacks and explain how these two solutions work. [6]

12. Alice creates an RSA public key pair. She chooses 17 and 11 as the two prime numbers to generate the public key and 7 as the other publicly-known value *e*.

i. How is the public key generated? [4]

ii. Explain the principle used to generate the publicly-known value *e* [2]

iii. What is the formula to generate the private key? [6]

iv. Alice wants to send the letter “M” (the numeric representation of M is 88) to Bob. What is the formula that Alice should use to generate the cipher message? [4]

v. What is the formula that Bob should use to decrypt the cipher message? [4]

13. (a) Discuss the challenges of protecting the security of virtual machines. You should develop your discussions by comparing the features of virtual machines and physical machines. [10]

(b) What is a firewall? Explain three main methods used in a firewall to control network traffic. Explain the features of these three methods and compare their advantages and disadvantages. [10]

14. (a) ActiveX is a technology that enables different software applications to share functionality and information. Explain why ActiveX poses a security threat. [5]

(b) A Cookie is a piece of data sent from a web server and stored in a user's web browser. Can Cookies carry viruses? Discuss three security issues cookies may cause. [10]

(c) Explain how the HTTPS protocol works. [5]