UNIVERSITY OF LONDON

BSc EXAMINATION 2017

For Internal Students of
Royal Holloway

DO NOT TURN OVER UNTIL TOLD TO BEGIN

IY2760: Introduction to Information Security
IY2760R: Introduction to Information Security – PAPER FOR RESIT CANDIDATES

Time Allowed: **TWO hours**

Answer ALL questions
Calculators are not permitted

1. Introduction to Information Security Primitives and Concepts

   (a) Information security is often defined in terms of 'CIA'. Explain what these three letters stand for, and briefly define each term. [6 marks]

   (b) Describe the terms *'Plaintext'*, *'Ciphertext'* and *'Cipher'*. [3 marks]

   (c) An attacker can bypass a protection mechanism if he/she has access to a system layer below where a protection mechanism is located. For each of the following two examples discuss how an attacker with *'system privilege to the operating system'* and *'access to system hardware'* can bypass security mechanisms located at a higher layer. [6 marks]

   (d) Define what an *'Information Security Policy'* is. [2 marks]

   (e) Define the four fundamental threats, matching *'Confidentiality'*, *'Integrity'*, *'Availability'* and *'Legitimate use'*. [4 marks]

   (f) Security Protocols

      i. Introduce the two types of adversaries against a cryptographic protocol. [2 marks]

      ii. Which of the two types of adversaries you identified in 1(f)(i) can cause more harm during a communication protocol and why? [2 marks]

2. Cryptography

(a) Cryptographic algorithms can be divided into *symmetric* and *asymmetric* ones. Explain the main difference between these two types of algorithms. [3 marks]

(b) What is a block cipher mode of operation, and why are such modes necessary? [4 marks]

(c) Describe, with the aid of a diagram, a different mode of operation for a block cipher of your choice (e.g. DES). [6 marks]

(d) Describe, preferably with the aid of a block diagram, how a stream cipher encrypts and decrypts data. [6 marks]

(e) Message Authentication Codes (MACs)

i. What security services can a MAC provide for a transmitted message? [3 marks]

ii. How is a MAC used to protect a transmitted message? [3 marks]

3. Europay MasterCard Visa (EMV) and Multi-Application Smart Card Technology

   (a) Explain what is meant by Card-Not-Present (CNP) transactions and state what might go wrong with such a transaction. [2 marks]

   (b) Digital Cash

      i. Define a digital cash system. [1 marks]

      ii. For the digital cash system that you identified in question 3(b)(i) discuss two of its advantages and disadvantages. [4 marks]

   (c) Discuss the Dynamic Data Authentication (DDA) method that is defined in the EMV standards. Your description should also include a diagram of the participating entities and the relationships between their cryptographic keys. [5 marks]

   (d) What is the role of a payment scheme operator (e.g. Visa) in an EMV transaction? [1 marks]

   (e) With the aid of a diagram, describe the four main parties involved in a typical EMV transaction. [4 marks]

   (f) Discuss two of the main multi-application smart card platforms or operating systems. [5 marks]

   (g) Describe three main factors contributing towards the evolution of monolithic smart card platforms towards true multi-application smart card platforms. [3 marks]

4. (a) Describe two reasons why *Passwords* and *Personal Identification Numbers (PINs)* are considered weak authentication mechanisms and introduce two alternative methods for enhancing the above mechanisms. [4 marks]

   (b) Specify the five component modules of an architecture for a typical biometric system for personal authentication, and briefly describe the role of each module. [10 marks]

   (c) In authentication protocols, the following types of non-repeating value can be used to provide *'freshness checking'* for protocol messages: random numbers (unpredictable nonces) and time-stamps. Describe each of these two mechanisms and provide an advantage and a disadvantage for each one. [6 marks]

   (d) Introduce fingerprint recognition authentication and describe two potential advantages and two disadvantages. [5 marks]

END