A22648 *No Calculator permitted in this examination*

UNIVERSITY OF BIRMINGHAM

School of Computer Science

First Year – MSc Computer Science
First Year – UG Aff Computer Science/Software Engineering
Fourth Year – MSci – Mathematics and Computer Science
First Year – MSc Computer Security

06 20008

Cryptography

Summer Examinations 2013

Time Allowed: 1:30 hours

[Answer ALL Questions]

TURN OVER

1. (a) What are the required properties of a hash-function? [6%]

   (b) How can you generate a hash function from a block cipher? [7%]

   (c) Consider a website which provides downloads of out-of-copyright sheet music. Each piece of sheet music is provided as a pdf-file together with a hash of the pdf-file over an unencrypted http-connection. Is this enough to prevent attackers modifying the pdf-file in transit by inserting malware? Justify your answer. If not, provide a fix which prevents those attacks, explaining any assumptions that are required for your solution to work over an unencrypted http-connection. http-connection. [12%]

2. (a) Explain how you use public-key cryptography for generation of digital signatures. [6%]

   (b) Why is randomisation necessary with public-key encryption? [6%]

   (c) Consider the following protocol between Alice (A) and an online music store (MS), where we assume that both Alice and the online music store have a public/private key pair ($prK_A, pubK_A$) and ($prK_{MS}, pubK_{MS}$) respectively and L is Alice's login name, and P the password, and $\{\_\}_\_$ is randomised encryption:

$$A \rightarrow MS : L, \{L, P\}_{pubK_{MS}}$$
$$MS \rightarrow A : \{symK\}_{pubK_A}$$

   The music store sends a message only if login name and password are OK for Alice. $symK$ is a new symmetric key chosen by the music store. The intention is that after the execution of this protocol $symK$ is a shared secret key between Alice and the music store, and that Alice has been authenticated to the music store. This protocol is vulnerable to attacks. Describe two attacks and provide countermeasures. [13%]

3. (a) Perform the following operations in $\mathbb{Z}_{12}$:

      (i) $8 - 10$ [2%]

      (ii) $5 * 4$ [2%]

      (iii) 5^{18} [3%]

      (iv) Calculate the multiplicative inverse of 7 by using the extended Euclidean algorithm. [5%]

   (b) Let G be a group with group operation $\circ$. Show that for each $a, b \in G$ there exists exactly one $c \in G$ such that $a \circ c = b$. [13%]

4. (a) How can you interpret addition in $\mathbb{F}_2[x]/p(x)$ as an operation on bitstrings? [3%]

   (b) Is Z_{p^2} a field if p is a prime number? Justify your answer. [3%]

   (c) Calculate $(x^3 + x^2 + 1) * (x^2 + x + 1)$ in $\mathbb{F}_2[x]/(x^4 + x + 1)$. [5%]

5. (a) What are the security requirements for CSS (Content Scrambling System)? [5%]

   (b) Discuss at least three legal or ethical issues arising from CSS. [9%]