A22648 *No calculator permitted in this examination*

UNIVERSITY OF BIRMINGHAM

School of Computer Science

Third year – Degree of BEng with Honours
Computer Science/Software Engineering

Fourth year – Degree of MEng with Honours
Computer Science/Software Engineering

Fourth Year – Joint Degree of MSci with Honours
Mathematics and Computer Science

Undergraduate Occasional
Computer Science/Software Engineering

Degree of MSc
Advanced Computer Science
Computer Science
Internet Software Systems
Computer Security

06 20008

Cryptography

Summer Examinations 2011

Time allowed: 1 ½ hours

[The paper contains Three Parts
Answer TWO Questions from EACH Part]

No Calculator

[Answer only two questions from this part.]

Part I

1. Briefly explain the following concepts:

   (a) Avalanche Effect

   (b) Modes of Operation

   (c) Cryptanalysis

   (d) Key Schedule

   (e) Commitment Scheme

$\boxed{3+3+3+3+3}$

2. (a) Explain the purpose and general working of Cryptographic Hash Functions as well as their required properties.

   (b) Give at least two examples of hash functions used in practice.

   (c) Briefly describe a way how a hash function can be constructed from an ordinary block cipher.

$\boxed{8+2+5}$

3. (a) Discuss some of the security requirements for implementations of the Advanced Access Content System (AACS) to ensure digital rights management (DRM) requirements.

   (b) Discuss some of the legal and ethical issues surrounding AACS and DRM in general.

   Give at least two security requirements and three legal or ethical issues. $\boxed{6+9}$

[Answer only two questions from this part.]

Part II

4. (a) Perform the following operations in $\mathbb{Z}_{15}$

(1) $12 + 23$

(2) $8 \cdot 6$

(3) 3^4

(b) Let $a, b \in \mathbb{Z}$. We define $a \sim b$ if and only if $a \equiv b(\bmod n)$, where $\equiv$ is the usual modulo operation in $\mathbb{Z}$. Show that $a \sim b$ is an equivalence relation, i.e., it holds

(i) for every $a \in \mathbb{Z}$: $a \sim a$ (Reflexivity)

(ii) for every $a, b \in \mathbb{Z}$: if $a \sim b$ then $b \sim a$ (Symmetry)

(iii) for every $a, b, c \in \mathbb{Z}$: if $a \sim b$ and $b \sim c$ then $a \sim c$ (Transitivity)

$\boxed{5+10}$

5. (a) Compute the subgroup of $\mathbb{Z}_{13}$ generated by 4.

(b) Let G be a group and H, K be subgroups of G. Show that the following holds:

$H \cup K$ is a subgroup if and only if $H \subseteq K$ or $K \subseteq H$.

$\boxed{5+10}$

6. (a) Compute the bit operation

$$11000001 \otimes 00010111$$

in the finite field $\mathbb{F}_{2^8} = \mathbb{F}_2[x]/p(x)$ with $p(x) = x^8 + x^4 + x^3 + x + 1$.

(b) Let G be a finite set that is closed under a binary operation $\circ : G \to G$. Show that if G has the following two properties:

(i) For each $a, b, c \in G$ we have $(a \circ b) \circ c = a \circ (b \circ c)$.

(ii) For each $a, b \in G$ there exist $x, y \in G$, such that $(a \circ x) = b$ and $(y \circ a) = b$.

then G is a group.

$\boxed{5+10}$

[Answer both questions in this part.]

Part III

7. Consider the Diffie-Hellman key exchange algorithm. Discuss how one can stage a man-in-the-middle attack on it. How could this be done in practice? What possible prevention of this attack could you think of? $\boxed{20}$

8. "Old Maid" is a card game played with a deck of 31 cards consisting of 15 pairs and a single card called, the Old Maid. The objective is to discard pairs of cards with the loser being the player left with the Old Maid.

   At the start the dealer deals all of the cards to the players. (Some players may have more cards than others; this is acceptable.) Players look at their cards and discard any pairs they have. Then, beginning with the person left of the dealer, each player takes turns offering their hand face-down to the person on their left. This person selects a card, adds it to their hand, and if possible discards a pair openly. The player then offers their hand to the person to their left and so on. Players are allowed to shuffle their hand before offering it to the next player.

   Assume that the players do not trust each other and do not have access to a trusted third party. Design protocols and commitment schemes for the card game assuming three players: Alice, Bob, and Carol. You may use hash functions or a ciphersystem to design your protocol. Give sufficient explanations how your protocol ensures that none of the players is able to cheat. In particular, you have to make sure that no two players can collude against the third.

   You don't have to give a protocol for shuffling, but you need to explain how your deck of cards is represented and what the state is after dealing. $\boxed{20}$