A22648 *No calculator permitted in this examination*

UNIVERSITY OF BIRMINGHAM

School of Computer Science

Final Year – Degree of MEng with Honours
Computer Science/Software Engineering

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

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

Intercalated Year
Computer Science
Undergraduate Occasional
Computer Science/Software Engineering

06 20008

Cryptography

Summer Examinations 2008
Time Allowed: 1 ½ hours

**[This paper contains THREE parts
Answer TWO Questions from EACH PART]**

Part I

1. Briefly explain the following concepts: $\boxed{4+4+4+4+4}$

   (a) Pseudo-random Generator

   (b) Substitution Cipher

   (c) Asymmetric Cipher

   (d) Feistel Cipher

   (e) Collision Free Function

2. Explain the basics of a Merkle-Damgård Construction. $\boxed{20}$

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.

   $\boxed{8+12}$

Part II

4. (a) Carry out the following muliplication on permutations: $\boxed{5+5+5}$
   $(1\ 2)(4\ 5\ 6) * (2\ 3)(5\ 6)$

   (b) Compute the inverse of the following permutation: $(1\ 2\ 7\ 4\ 3\ 8)$

   (c) Apply the permutation $(1\ 3\ 4)(2\ 5\ 6)$ to the list of numbers `1 2 3 4 5 6` .

5. (a) Carry out the following modulo operation in $\mathbb{F}_2[x]$: $\boxed{5+10}$
   $x^7 + x^6 + x^4 + x^2 + x + 1 (\mathrm{mod}\ x^3 + x + 1)$

   (b) Let $n! = n \cdot (n-1) \cdots 2 \cdot 1$ be the factorial function. Show that the following holds:

   If p is a prime number, then $(p-1)! \equiv -1 (\mathrm{mod}\, p)$.

6. Carry out the following calculations in $\mathbb{Z}_{17}$: $\boxed{1+2+2}$

   (a) $13 + 12$

   (b) $8 \cdot 5$

   (c) 5^3

   Show that the following holds: $\boxed{10}$

   (d) Let $a_1, a_2, b_1, b_2, n \in \mathbb{Z}$ with $a_1 \equiv b_1 (\mathrm{mod}\, n)$ and $a_2 \equiv b_2 (\mathrm{mod}\, n)$.

$$(a_1 + a_2) \equiv (b_1 + b_2)(\mathrm{mod}\, n)$$

Part III

7. We define a Feistel cipher that has the following parameters:

   - 8-bit plaintext input M,
   - 4-bit key K,
   - 2 rounds of encryption,
   - Key schedule: $K_0 = K, K_1 = K_0 \lll 1$,
   - Feistel function: $M \oplus K_i \oplus (K_i \lll 2)$.

   Encipher the 24 bit plaintext $10111001\ 11111000\ 01100011$ with key $K = 1101$ using the Cipher Block Chaining mode (CBC) with initial value $IV = 11100011$. $\boxed{15}$

8. Consider the following two player game with two regular six-sided dice: Each player rolls one die secretly, keeping it hidden under a cup, i.e. only this player will know the value rolled. Both players then secretly estimate the sum of both dice, writing their estimate on a piece of paper. Both papers and dice are then revealed and the player closest to the sum of the two dice wins.

   Design protocols and commitment schemes to play the game electronically assuming that the two players would not trust each other. Give sufficient explanations why your protocol works. $\boxed{15}$

9. Consider the Diffie-Hellman key exchange protocol. Give the single steps of the protocol using as values: prime number $p = 13$, generator $g = 5$, Alice's secret key $a = 18$, and Bob's secret key $b = 19$. Give all the intermediate steps of the protocol. $\boxed{15}$

   [Hint: compute the subgroup of $\mathbb{Z}_{13}$ generated by 5 first.]

End of Paper