A22648 No calculator permitted in this examination

UNIVERSITY OF BIRMINGHAM

School of Computer Science

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

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

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

Undergraduate Occasional
Computer Science/Software Engineering

06 20008

Cryptography

Summer Examinations 2010

Time allowed: 1 ½ hours

[Answer TWO Questions from EACH Part]

Part I

1. Briefly explain the following concepts:

   (a) Cryptanalysis

   (b) Stream Cipher

   (c) Birthday Paradox

   (d) Masquerading Attack

   (e) Merkle-Damgård Construction

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

2. (a) Explain the operation of Linear Feedback Shift Registers (LFSR).

   (b) How can LFSRs be used to build secure stream ciphers?

$\boxed{7+8}$

3. The content scrambling system (CSS) is used to encrypt multimedia DVDs.

   (a) Briefly sketch how the cipher of CSS works.

   (b) DeCSS is an open source library that allows to decrypt content encrypted with CSS. DeCSS has been outlawed in some countries as it is not officially licensed by the CSS License Agency.

   Discuss some of the legal and ethical issues related to this.

   (c) In this context, what are *illegal prime numbers* and their implications?

$\boxed{2+8+5}$

Part II

4. (a) Compute the bit operation

$$01010101 \otimes 10010001$$

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) Consider the following algebraic structure $(A, \circ)$, given by its multiplication table.

$\circ$	a	b	c	d	e	f
a	a	b	c	d	e	f
b	b	a	e	f	d	c
c	c	d	a	e	f	b
d	d	f	b	a	c	e
e	e	c	f	b	a	d
f	f	e	d	c	b	a

Determine which of the group properties hold for $(A, \circ)$.

$\boxed{8+7}$

5. (a) Compute 8^{38} in $\mathbb{Z}_{35}$.

(b) Show that the following holds:
Let G be a group and H, K be subgroups of G. Then $H \cap K$ is a subgroup of G.

$\boxed{5+10}$

6. (a) Compute the Greatest Common Divisor of 78 and 14 using the Euclidean algorithm.

(b) Show that the following holds:

$$(((a + b) \bmod n) + c) \bmod n \equiv (a + b + c) \bmod n$$

$\boxed{5+10}$

Part III

7. Consider the Diffie-Hellman key exchange protocol. Give all single steps of the protocol using as values: prime number $p = 17$, generator $g = 8$, Alice's secret key $a = 14$, and Bob's secret key $b = 23$. $\boxed{20}$

   [Hint: compute the subgroup of $\mathbb{Z}_{17}$ generated by 8 first.]

8. Card-Jitsu™ is a martial arts card game in which two penguins fight each other using cards that depict different elements (Snow, Water, Fire) and a numerical value. A card beats another either by precedence of element (Fire beats Snow, Snow beats Water, and Water beats Fire) or, in case two cards show the same element, by order of the numerical value. While cards are chosen from a deck of 32 different cards, each card can occur multiple times in the same game.

   At the start each penguin has four cards, only visible to themselves. In each turn each penguin chooses one of its four cards. The two choosen cards are uncovered and the winner is determined. Then both penguins draw a new card.

   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 preparation phase and for a player's turn. 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. $\boxed{20}$

9. Consider the following public key cipher with key generator algorithm G and encryption algorithm E:

   Key generator G: Alice generates a key as follows

   - Generate primes p, q and $g \in \mathbb{Z}_p^*$ that generates the subgroup G_q.
   - Choose random x, y from $\{0, \ldots, q-1\}$.
   - Compute $h_1 = g^x$ and $h_2 = g^y$.
   - Publish the public key $\widehat{K} = (G_q, q, g, h_1, h_2)$.
   - Retain the private key pair $K = (x, y)$.

   Encryption algorithm E: To encrypt a message M to Alice using her public key $\widehat{K} = (G_q, q, g, h)$, Bob computes the following steps

   - M is considered to be an element of G
   - Choose random $z \in \{0, \ldots, q-1\}$, calculate $c_1 = g^z$ and $c_2 = M \cdot h_1^{-z} \cdot h_2^z$.
   - The ciphertext is then $C = (c_1, c_2)$.

   Note that all multiplications are modulo p.

   (a) Design an appropriate decryption algorithm D for the cipher and demonstrate its correctness.

   (b) Assume that we run the algorithm with the parameters $p = 23$, $q = 11$, $G_{11} = \langle 6 \rangle$, $x = 9$, $y = 8$, $z = 7$. Use D in order to decrypt the ciphertext $C = (3, 10)$. $\boxed{12+8}$

End of Paper