

UNIVERSITY OF PORTSMOUTH

FACULTY OF TECHNOLOGY

Department of Electronic and Computer Engineering

M591 – Technology Exploration Project

U13127

Date: 5 February 2010

Time: 09:00 – 10:30

INSTRUCTIONS

Write your student ID number clearly on page 2.

Write your answers to all 5 questions within the spaces provided in this examination paper.

Handwritten notes are permitted with this examination.

Calculators permitted are:

Casio FX 85 series

Casio FX 83 series

Examiner:

Prof Jiangzhou Wang, Mr Chi Nguyen

Student ID Number

QUESTION 1

a) Place an "X" in the box next to **3 terms** that are **categories of knowledge based authentication**. **[6 Marks]**

- hidden phrase
- mixed phrase
- passphrase
- single hash
- double hash

- associative
- commutative
- word cues
- fact-based cues
- system generated cues

b) Provide **descriptive examples of authentication methods** for all of the terms selected in part (a). **[9 Marks]**

Use the terms selected in part (a) to **explain the difference between push and pull authentication**. **[5 Marks]**

QUESTION 2

a) Place an "X" in the box next to **3 terms** that are **categories of graphical authentication**.

[6 Marks]

<input type="checkbox"/>	locimetric
<input type="checkbox"/>	symmetric
<input type="checkbox"/>	asymmetric
<input type="checkbox"/>	drawmetric
<input type="checkbox"/>	cognometric

<input type="checkbox"/>	shuffle
<input type="checkbox"/>	random
<input type="checkbox"/>	arranged
<input type="checkbox"/>	ascending
<input type="checkbox"/>	descending

b) Match each of the terms selected in part (a) with a subject from the list below. Describe how that subject could be used as a graphical authentication method.

[14 Marks]

Images of common domestic animals.

Images of cityscapes with skyscrapers.

Images of outlines for common dining room furniture.

QUESTION 3

a) Place an "X" in the box next to **3 terms** that are **security properties of cryptographic hash functions**. [6 Marks]

<input type="checkbox"/>	key resistant	<input type="checkbox"/>	reversible
<input type="checkbox"/>	tamper resistant	<input type="checkbox"/>	preimage resistant
<input type="checkbox"/>	collision resistant	<input type="checkbox"/>	second preimage resistant
<input type="checkbox"/>	linked identification	<input type="checkbox"/>	postimage resistant
<input type="checkbox"/>	automatic identification	<input type="checkbox"/>	second postimage resistant

b) Consider a sample hash function that takes as input any positive whole number. The hash function adds all the digits in the whole number and produces as output the last digit of the sum. Examples are provided below:

Input values	Output values
2	2
437	4
1024	7

Use all of the terms selected in part (a) to **provide reasons and examples** that show the hash function does **not** possess the required security properties. [14 Marks]

QUESTION 4

a) Place an "X" in the box next to **3 terms** that are directly **used to generate RSA digital signatures**. [6 Marks]

<input type="checkbox"/>	public key
<input type="checkbox"/>	private key
<input type="checkbox"/>	weak key
<input type="checkbox"/>	strong key
<input type="checkbox"/>	shared key

<input type="checkbox"/>	salt
<input type="checkbox"/>	buffer
<input type="checkbox"/>	nonce
<input type="checkbox"/>	digest
<input type="checkbox"/>	sample

b) As an example, Alice wants to place an order with her bank to convert £500 in her current account into US dollars and deliver the foreign currency to her sister's house. The bank wants to verify that Alice actually issued the order. Use all of the terms selected in part (a) to **describe how the bank could use a digital signature to authenticate that the order was issued by Alice**. [14 Marks]

QUESTION 5

a) Place an "X" in the box next to **3 terms** that are **participants specifically identified in the Data Protection Act 1998**. **[6 Marks]**

- | | |
|--------------------------|-------------------|
| <input type="checkbox"/> | companies auditor |
| <input type="checkbox"/> | companies house |
| <input type="checkbox"/> | data controller |
| <input type="checkbox"/> | data subject |
| <input type="checkbox"/> | data source |

- | | |
|--------------------------|---------------------|
| <input type="checkbox"/> | companies registrar |
| <input type="checkbox"/> | companies minister |
| <input type="checkbox"/> | data processor |
| <input type="checkbox"/> | data provider |
| <input type="checkbox"/> | data buyer |

b) Describe **2 fair information principles or practices** that are relevant **for each of the terms selected in part (a)**. **[14 Marks]**