

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

***** SOLUTIONS *****

QUESTION 1

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

	hidden phrase	2	associative
	mixed phrase		commutative
2	passphrase		word cues
	single hash	2	fact-based cues
	double hash		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]**

Similar to:

Passphrase is a form of password authentication that uses a long string of one or more words as a shared secret. For example, "let me in" could be a passphrase. [3]

Associative passwords use several pairs of questions and answers for authentication. Each answer is provided by the user and is associated with the cue word provided in the question. For example, the cue word question could be "color" and a possible answer might be "yellow". [3]

Fact-based cues are a specific format of associative passwords in which the questions are intended to solicit fact based answers. Answers are considered to be facts if the information can be independently verified by a third party. For example, the question could be "Name of cat" and the answer might be "Oscar" for a specific user. [3]

Push authentication refers to methods in which the authentication system has the primary responsibility for selecting the secret and the user typically must recall the secret. An example of push authentication is passphrases. **Pull** authentication refers to methods that pull personal data from the user during the authentication process. Associative passwords and fact-based cues are examples of pull authentication. [5]

QUESTION 2

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

[6 Marks]

2	locimetric		shuffle
	symmetric		random
	asymmetric		arranged
2	drawmetric		ascending
2	cognometric		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.

Similar to:

Cognometric refers to graphical authentication methods that depend on the ability to recognize one or more images during the authentication process. Images of common domestic animals would be convenient for people to recognize during a cognometric authentication process. [4]

Locimetric refers to graphical authentication methods that depend on the accurate identification of target points or areas within an image. Usability is improved if the images have well defined areas and/or linear shapes. Skyscrapers in cityscape photos would be convenient for people to use during a locimetric authentication process. [5]

Drawmetric refers to graphical authentication methods that require users to reproduce specific drawings. Usability is improved if users are required to draw outlines of commonly used objects instead of detailed images. Outlines of common dining room furniture would be convenient for people to create during a drawmetric authentication process. [5]

QUESTION 3

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

	key resistant		reversible
	tamper resistant	2	preimage resistant
2	collision resistant	2	second preimage resistant
	linked identification		postimage resistant
	automatic identification		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]

Similar to:

Preimage resistant requires that it is difficult to find an input when given a specific output. The sample hash function fails because when given 2 as a specific output, it is easy to find input values such as 2, 93 or 7771 that could produce the required output. [5]

Second preimage resistant requires that it is difficult to find a different input that could produce the same output as a specific pair of input and output values. The sample hash function fails because when given 437 and 4 as an input and output pair, it is easy to find input values such as 4, 978 or 755647 that could produce the required output. [5]

Collision resistant requires that it is difficult to find more than one distinct input value which could produce the same output value. The sample hash function fails because there are only 10 possible output values, which indicates that there will be many collisions. For example, input values 1, 29 and 92 all produce the same output value 1. [4]

QUESTION 4

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

2	public key		salt
2	private key		buffer
	weak key		nonce
	strong key	2	digest
	shared key		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]

Similar to:

There are 2 steps for Alice to create a digital signature to accompany her order.
 First, Alice would create a hash **digest** of the order. [2]
 Second, Alice would use her **private key** to encrypt the hash digest. The output ciphertext is the digital signature. [3]

Alice would send the digital signature with her order to the bank. [2]

There are 3 steps for the bank to authenticate that the order was actually issued by Alice.
 First, the bank would create a hash digest of the order. [2]
 Second, the bank would use Alice's **public key** to decrypt the digital signature. [3]
 Third, the bank would compare the output of step 1 and step 2. If the outputs are identical, then the authentication is successful and the bank can be confident that Alice issued the order. [2]

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
2	data controller
2	data subject
<input type="checkbox"/>	data source

<input type="checkbox"/>	companies registrar
<input type="checkbox"/>	companies minister
2	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]

Similar to:

The **data controller** responsible for collecting personal data must be accountable for compliance with fair information principles and practices. [3]

The **data controller** must collect the minimum amount of information that is necessary for the specific user transaction or activity. [2]

The **data processor** must use the data only for the purpose specified during data collection unless required by government authorities. [3]

The **data processor** must specify the intended usage for the data at the time of collection. [2]

The **data subject** must have knowledge of the existence and usage of the system which is collecting and processing data. [2]

The **data subject** must have access to personal data and a reasonable method for correcting any errors or problems. [2]