

UNIVERSITY OF PORTSMOUTH

FACULTY OF TECHNOLOGY

Department of Electronic and Computer Engineering

M590 Technology Exploration

Date : 2 February 2006

Time : 11.15 – 13.15

INSTRUCTIONS

Write your student ID number clearly on page 2.

Write your answers to all 5 questions in this examination paper.

For each question, indicate your answer to **part A** by placing an “X” in the box next to the appropriate boxes on the answer sheet. For each question, write your answer to **part B** by writing in the appropriate space in this examination paper.

Handwritten notes are permitted with this examination.

Calculators permitted to be used:

Casio FX 85WA

Casio FX 83WA

Casio FX 85MS

Examiners:

Mr Chi Nguyen, Dr Zhili Sun

Student ID Number

*** SOLUTIONS ***

Question 1A. Place an "X" in the box next to 5 terms that are most directly related to the benefits of using cryptography. [10 marks]

<input type="checkbox"/>	authorisation	<input checked="" type="checkbox"/>	confidentiality
<input checked="" type="checkbox"/>	authenticity	<input checked="" type="checkbox"/>	integrity
<input type="checkbox"/>	approval	<input type="checkbox"/>	accuracy
<input checked="" type="checkbox"/>	privacy	<input type="checkbox"/>	evidence of transfer
<input type="checkbox"/>	performance	<input type="checkbox"/>	evidence of size
<input type="checkbox"/>	predictability	<input checked="" type="checkbox"/>	evidence of origin

Question 1B. For each of the terms that you selected in question 1A, briefly describe a cryptographic method which provides that benefit. [10 marks]

Symmetric ciphers can protect **confidentiality** of data.

Hash functions can be compared to assure **integrity** of data.

Message authentication codes (MAC) can be compared to assure **evidence of origin**.

Digital certificates can be used to assure the **authenticity** of data.

Secure shell software can protect the **privacy** of a TCP/IP connection.

Question 2A. Place an “X” in the box next to 5 terms that are most directly related to the use of authentication mechanisms. [10 marks]

<input type="checkbox"/>	ECB
<input checked="" type="checkbox"/>	MAC
<input type="checkbox"/>	CBC
<input checked="" type="checkbox"/>	tokens
<input type="checkbox"/>	locks
<input type="checkbox"/>	rings

<input type="checkbox"/>	something you create
<input checked="" type="checkbox"/>	something you know
<input checked="" type="checkbox"/>	something you are
<input type="checkbox"/>	something you hear
<input type="checkbox"/>	something you read
<input checked="" type="checkbox"/>	something you have

Question 2B. For each of the terms that you selected in question 2A, briefly describe a weakness associated with using that authentication mechanism. [10 marks]

Message authentication codes (**MAC**) require a secret key. This creates a weakness with the need for a secure key exchange method.

Authentication credentials based on **something you know** suffers from the weakness of being difficult to remember.

Authentication credentials based on **something you are** suffers from the weakness of being difficult to revoke because the credentials can't easily be taken away.

Authentication credentials based on **something you have** suffers from the weakness of being easy to share between multiple users.

Tokens are a form of authentication based on something you have. Thus, it suffers from the same weakness.

Question 3A. Place an “X” in the box next to 5 terms that are most directly related to authentication processes and infrastructure. [10 marks]

<input type="checkbox"/>	grille	<input type="checkbox"/>	dispersed
X	issuer	X	federated
<input type="checkbox"/>	substitution	<input type="checkbox"/>	source
X	centralised	X	accountable
<input type="checkbox"/>	sample	<input type="checkbox"/>	watermark
X	authorise	<input type="checkbox"/>	transform

Question 3B. Briefly describe two authentication methods using all the terms that you selected in question 3A. [10 marks]

A common challenge response authentication method is the use of passwords. For example, the university Novell network is a **centralised** system which uses password authentication. The University acts as the **issuer** of the Novell account and mostly use the authentication as a way to **authorise** students to have access to the network.

The government issued passport is an example of a token based authentication method. This is a **federated** system because passports are issued independently by national governments and accepted by governments of other nations. Passports provide a way for governments to hold travellers and visitors **accountable** to legal requirements.

Question 4A. Place an “X” in the box next to 5 terms that are most directly related to the use of spam mimic as a stenographic method. [10 marks]

<input type="checkbox"/>	audio	<input checked="" type="checkbox"/>	stego-object
<input type="checkbox"/>	statistical	<input checked="" type="checkbox"/>	cover object
<input checked="" type="checkbox"/>	linguistic	<input checked="" type="checkbox"/>	cover generation
<input type="checkbox"/>	distortion	<input type="checkbox"/>	transform domain
<input type="checkbox"/>	transposition	<input checked="" type="checkbox"/>	stego-key
<input type="checkbox"/>	injection	<input type="checkbox"/>	spread spectrum

Question 4B. Briefly compare the differences and similarities between spam mimic and symmetric ciphers using all the terms that you selected in question 4A. [10 marks]

Spam mimic is a **linguistic cover generation** technique which generates **cover objects** in the form of spam. The message is hidden in the spam according to an algorithm which acts as the **stego-key**. The output for a specific message and stego-key combination is a **stego-object** which appears to be nothing more than spam text.

Symmetric ciphers is similar because it can be applied to **linguistic** data. The cipher key is used in a similar role to the **stego-key** and the cipher text protects the data in a similar role to the **stego-object**. The process of generating the cipher text is similar to the process of **cover generation** for spam mimic.

Symmetric ciphers are different because cipher text indicates the existence of hidden data whereas spam mimic text doesn't indicate the existence of hidden data.

Question 5A. Place an "X" in the box next to 5 terms that are most directly related to the detection of software worms. [10 marks]

<input type="checkbox"/>	firewalls	<input type="checkbox"/>	automated patching
<input type="checkbox"/>	sandboxes	<input type="checkbox"/>	software jails
<input checked="" type="checkbox"/>	black holes	<input type="checkbox"/>	weak hosts
<input checked="" type="checkbox"/>	honeypots	<input type="checkbox"/>	disabled services
<input type="checkbox"/>	proxy signatures	<input checked="" type="checkbox"/>	traffic volume
<input checked="" type="checkbox"/>	log signatures	<input checked="" type="checkbox"/>	network scans

Question 5B. For each of the terms that you selected in question 5A, briefly describe how software worms can evade that method of detection. [10 marks]

Software worms can evade **black holes** by using an enumerated target list.

Software worms can evade **honeypots** by detecting and avoiding hosts with default configurations.

Software worms can evade **log signature** analysis minimising the use of non-standard probes of server software.

Software worms can evade **traffic volume** analysis by using passive target identification techniques.

Software worms can evade **network scan** analysis by using intermittent or random scheduling of target identification.