

UNIVERSITY OF PORTSMOUTH

FACULTY OF TECHNOLOGY

Department of Electronic and Computer Engineering

M590 Technology Exploration

SAMPLE

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

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

<input checked="" type="checkbox"/>	symmetric ciphers	<input type="checkbox"/>	EIP
<input checked="" type="checkbox"/>	asymmetric ciphers	<input checked="" type="checkbox"/>	MAC
<input type="checkbox"/>	hybrid ciphers	<input type="checkbox"/>	NOP
<input type="checkbox"/>	codes	<input type="checkbox"/>	shared
<input checked="" type="checkbox"/>	hashes	<input checked="" type="checkbox"/>	centralised
<input type="checkbox"/>	blocks	<input type="checkbox"/>	independent

Question 1B. For each of the terms that you selected in question 1A, briefly describe how that term improves the authentication process. [10 marks]

Symmetric ciphers can protect passwords used for authentication.

Asymmetric ciphers can provide digital signatures to identify the sender of the data.

Hashes can be used to generate message authentication codes (**MAC**) in order to authenticate the origin and integrity of the data.

A **centralised** authentication infrastructure is usually better at authenticating a large number of users.

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

<input type="checkbox"/>	fingerprint	<input type="checkbox"/>	null cipher
X	substitution	<input type="checkbox"/>	grille mask
<input type="checkbox"/>	transposition	X	spread spectrum
X	transform domain	X	distortion
X	cover generation	<input type="checkbox"/>	reversible
<input type="checkbox"/>	semagram cue	<input type="checkbox"/>	mutual

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

Substitution techniques may unintentionally alter the cover in a distinctive way to indicate that the cover has been modified.

Transform domain techniques are limited the small amount of change within the typical or standard range of activities of a cover object.

Cover generation techniques require the creation of a completely new cover object for each message. This creation process may be expensive, time consuming or difficult.

Spread spectrum techniques require more power and processing in order to utilise a wider range of frequencies and redundant data.

Distortion techniques require the use of a cover object which is not widely accessible since the existence of a message is easily revealed by comparison to the original object.