

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

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]

- authorisation
- authenticity
- approval
- privacy
- performance
- predictability

- confidentiality
- integrity
- accuracy
- evidence of transfer
- evidence of size
- 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]

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]

- ECB
- MAC
- CBC
- tokens
- locks
- rings

- something you create
- something you know
- something you are
- something you hear
- something you read
- 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]

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"/>
<input type="checkbox"/>
<input type="checkbox"/>
<input type="checkbox"/>
<input type="checkbox"/>
<input type="checkbox"/>

grille
issuer
substitution
centralised
sample
authorise

<input type="checkbox"/>
<input type="checkbox"/>
<input type="checkbox"/>
<input type="checkbox"/>
<input type="checkbox"/>
<input type="checkbox"/>

dispersed
federated
source
accountable
watermark
transform

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

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]

firewalls

sandboxes

black holes

honeypots

proxy signatures

log signatures

automated patching

software jails

weak hosts

disabled services

traffic volume

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]