

UNIVERSITY OF PORTSMOUTH

FACULTY OF TECHNOLOGY

Department of Electronic and Computer Engineering

M591 – Technology Exploration

U13127

Date: 8 February 2007

Time: 2 hours

INSTRUCTIONS

Write your student ID number clearly on page 2.

Write your answers to all 4 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 are:

Casio FX 85WA

Casio FX 83WA

Casio FX 85MS

Examiner:

Mr Chi Nguyen

Student ID Number

Question 1A. Place an “X” in the box next to 5 terms that are most directly related to the use of symmetric ciphers. [10 marks]

| | | | |
|--------------------------|-----------------|--------------------------|---------------|
| <input type="checkbox"/> | RSA | <input type="checkbox"/> | MAC |
| <input type="checkbox"/> | SHA | <input type="checkbox"/> | CBC |
| <input type="checkbox"/> | private key | <input type="checkbox"/> | ciphertext |
| <input type="checkbox"/> | block cipher | <input type="checkbox"/> | authenticity |
| <input type="checkbox"/> | confidentiality | <input type="checkbox"/> | hybrid cipher |
| <input type="checkbox"/> | null cipher | <input type="checkbox"/> | public key |

Question 1B. Use all of the terms you selected in question 1A to describe a specific symmetric cipher. Provide two advantages of using the cipher you described when compared to asymmetric ciphers. [15 marks]

Question 3A. Place an “X” in the box next to 5 terms that are most directly related to the use of hash functions. [10 marks]

| | | | |
|--------------------------|---------------------------|--------------------------|------------------------|
| <input type="checkbox"/> | algorithm | <input type="checkbox"/> | token |
| <input type="checkbox"/> | fixed length | <input type="checkbox"/> | private key |
| <input type="checkbox"/> | reversible transformation | <input type="checkbox"/> | independent |
| <input type="checkbox"/> | asymmetric | <input type="checkbox"/> | one way transformation |
| <input type="checkbox"/> | public key | <input type="checkbox"/> | variable length |
| <input type="checkbox"/> | analog | <input type="checkbox"/> | key exchange |

Question 3B. Use all of the terms you selected in question 3A to specify two similarities and two differences between the use of hash functions and the steganographic use of semagrams. [15 marks]

Question 4A. Place an “X” in the box next to 5 terms that are most directly related to methods of detecting and defending against software worms and viruses. [10 marks]

| | | | |
|--------------------------|---------------------|--------------------------|-----------|
| <input type="checkbox"/> | firewall | <input type="checkbox"/> | blackbox |
| <input type="checkbox"/> | grille mask | <input type="checkbox"/> | patchwork |
| <input type="checkbox"/> | traffic analysis | <input type="checkbox"/> | sandbox |
| <input type="checkbox"/> | transform domain | <input type="checkbox"/> | pattern |
| <input type="checkbox"/> | intelligent network | <input type="checkbox"/> | whitebox |
| <input type="checkbox"/> | payload mimic | <input type="checkbox"/> | honeypot |

Question 4B. Use all of the terms you selected in question 4A to compare a software worm that deletes files on affected computers and a software worm that sends files on affected computers to random email addresses. Specify the most effective detection method and defensive method for each worm. Indicate which worm would cause more commercial damage and the primary reason for your assessment. [15 marks]