

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

**** SOLUTIONS ****

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	X	CBC
X	private key	X	ciphertext
X	block cipher	<input type="checkbox"/>	authenticity
X	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]

DES is a 64-bit **block cipher** that also uses a 64-bit **private key**. The key is composed of seven 8-bit keys and 8 parity check bits. As such, the effective key length is only 56-bit. (+3)

DES is a reversible transformation that protects data **confidentiality**. It operates by applying an initial permutation to the plaintext. 16 sub-keys are generated from the 64-bit key. Each sub-key is applied to the data sequentially through a series of operations that constitute a round. After 16 rounds are complete, the **ciphertext** is created by applying the inverse permutation. Deciphering is done by the reverse process using the same 64-bit key. (+5)

Cipher block chaining (**CBC**) is a common mode of operation for using DES with large amounts of ciphertext in a streaming format. (+2)

DES is more practical for everyday use because it's faster than asymmetric ciphers. DES can be implemented on a wider range of software and hardware because it doesn't require the use of extremely large integer values (unlike, for example, RSA). (+5)

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

	random
X	verify
	substitution
	transform
X	identifier
X	accountable

	diffusion
	cover
X	identify
X	authorise
	transposition
	integrity

Question 2B. Use all of the terms you selected in question 2A to describe a specific centralised authentication system and a specific federated authentication system. Compare the systems by providing two advantages of using one of the systems you described. [15 marks]

The University computer network is a centralised authentication system using something you know (password). **Identifiers** are issued by the University and they fully **identify** students in order to enforce **accountable** computer use. (+5)

The Ebrary online book service uses Athens authentication, which is a federated system. Identifiers are issued by the participating academic institutions and the Athens system only **verify** identifiers sufficiently to **authorise** access to Ebrary. (+5)

Centralised authentication systems such as the University computer network is easier for managing large numbers of users. It has less potential for data privacy problems because authentication data is not transferred as often or as widely. (+5)

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]

X	algorithm		token
X	fixed length	X	private key
	reversible transformation		independent
	asymmetric	X	one way transformation
	public key	X	variable length
	analog		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]

Hash functions and semagrams both practically behave as **one way transformations**. In typical usage, both methods accept **variable length** input and produce **fixed length** output. (+7)

Hash functions are **algorithms** that could be based on symmetric block ciphers. In contrast, semagrams are not based on algorithms such as symmetric ciphers. (+4)

Hash functions may be used with or without a **private key**. In contrast, semagrams require a private stego-key which is typically effective for one use and discarded afterwards. (+4)

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]

X	firewall		blackbox
	grille mask		patchwork
X	traffic analysis	X	sandbox
	transform domain	X	pattern
	intelligent network		whitebox
	payload mimic	X	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]

The **honeypot** method would be most effective to detect worms that delete files because changes to the file system are easy to observe and record. The **sandbox** method be most effective to defend against worms that delete files because it would restrict access to a limited part of the file system. (+6)

The **traffic analysis** method would be most effective to detect worms that send files because the outbound email may cause noticeable changes to the **pattern** of network traffic. The **firewall** method would be most effective to defend against worms that send files because outbound email could be restricted to only authenticated senders. (+6)

Worms that send files via email would cause more commercial damage because disclosed files may create legal liabilities due to data privacy legislation and damage the reputation and brand of a company. This is likely to be higher than the loss of deleted files, which is mitigated by the possibility of backup data. (+3)