THE UNIVERSITY
of LIVERPOOL

JANUARY 2006 EXAMINATIONS

MOCK EXAM PAPER

PRIVACY AND SECURITY

TIME ALLOWED : Two Hours and a Half

INSTRUCTIONS TO CANDIDATES

Answer THREE out of four questions listed

If you attempt to answer more questions than the required number of questions (in any section), the marks awarded for the excess questions will be discarded (starting with your lowest mark).

Answer **THREE** out of four questions listed **(here, in the Mock Paper, only two out of four questions are presented.)**

1. (a) Describe the technique of pseudonymous audit. For what purpose can it be used for? Why is fully anonymous audit not suitable here?

(3 marks)

(b) List three main categories of authentication techniques. Discuss advantages and disadvantages of password based techniques.

(4 marks)

(c) Describe the mechanism of mix-networks for anonymity protection. How it can be compared with anonymizers and crowds ?

(4 marks)

(d) What are the potential problems with the security protection based on the *secrecy* of an encryption algorithm?

(2 marks)

(e) For a block cipher, what is the Electronic Codebook Mode (ECB) What are advantages and disadvantages of using this mode?

(4 marks)

(f) Using operators `believes`, `sees`, `possesses`, `said` of BAN logic, write the rule in BAN logic formalizing the following principle:

> if an agent P believes that it shares the symmetric key K with an agent Q, and agent P receives a message encrypted under K, then agent P believs that agent Q once said message X.

(4 marks)

2. (a) What is aggregated information? What is the difference between aggregated and anonymized information?

(3 marks)

(b) Compare linkable and unlinkable anonymity and pseudonymity. Which of these is needed to build digital reputation?

(4 marks)

(c) Compare symmetric encryption (SE) and public-key encryption (PKE)? What are advantages and disadvantages of each technique?

(5 marks)

(d) What is the statistical analysis based method in intrusion detection? Describe advantages and disadvantages of the method.

(4 marks)
(5 marks)

(e) Describe Use Limitation Principle in privacy protection (as it is defined in OECD Guidelines).

(4 marks)

(f) In Diffie-Hellman Key Exchange algorithm, what would be the common secret key, if 71 is used as a prime number, 7 as its primitive root and the parties have selected 5 and 9 as their random numbers?

(6 marks)