

THE UNIVERSITY OF SYDNEY

FACULTIES OF SCIENCE AND ENGINEERING

SAMPLE EXAMINATION

Computer Security

JUNE 200

Time Allowed: Two (2) Hours.

Value of Examination: 60%

OPEN BOOK EXAMINATION

Lecturer/s: M. Hitchens

Instructions to Candidates

PLEASE READ THE FOLLOWING INSTRUCTIONS CAREFULLY

You should attempt to answer **ALL** questions. Each of the six questions has equal value.

You **MAY NOT** retain this examination paper.

Computer Security

Question 1

10 marks

- a) What is the difference between a threat and an attack?
- b)
- c)

Question 2

10 marks

- a) Is DES an onto function? That is, is every possible 64-bit string the result of encrypting some other 64-bit string? Why?
- b)

Question 3

10 marks

- a) For Kerberos version 4, why is the authenticator field not of security benefit when asking the KDC for a ticket for Bob, but useful when logging into Bob?
- b) Design a modification to MD2 to handle messages which are not an integral number of bytes. Design it so that messages that are an integral number of bytes have the same digest value as with the existing MD2.
- c)

Question 4

10 marks

- a)
- b) Consider a system which an intrusion detection system which is based on Statistical Profiles. The learning process for the system consisted of example log session by system administrators over a weekend. Not surprisingly the system seems unable to detect intrusions. Which of the following would you recommend:
 - Replacing the system
 - Adding additional detection functions
 - Redoing the basic learning process
 - Some combination of the aboveProvide justifications for your answer

Question 5

10 marks

- a)
- b) The following algorithm is designed for mutual authentication. However, it has flaws. Identify those flaws and give a corrected version of the protocol.

$$A \rightarrow B : ID_A, R_1$$

$$B \rightarrow A : K_{AB}\{R_1\}$$

Question 6

10 marks

- a)
- b) The following protocol uses nonces. Which of the nonces must be unpredictable and why?

$$A \rightarrow KDC : N_{A1}, ID_A, ID_B$$

$$KDC \rightarrow A : K_A\{N_{A1}, ID_B, K_{AB}, K_B\{ID_A, K_{AB}\}\}$$

$$A \rightarrow B : K_B\{ID_A, K_{AB}\}, K_{AB}\{N_{A2}\}$$

$$B \rightarrow A : K_{AB}\{N_{A2}-1, N_{B1}\}$$

$$A \rightarrow B : K_{AB}\{N_{B1}-1\}$$