4790

The University of Sydney
Department of Electrical and Information Engineering

ELEC5616 ::
COMPUTER AND NETWORK SECURITY

Semester 1, 2011

Time Allowed: 2 hours

The exam is marked out of 100.

Candidates must answer all four (4) questions.

All Questions are of equal value (25 marks per question).

Do not answer more than four questions.

Each question must be answered in a seperate book. Question 4 is to be answered on the multiple choice answer sheet provided.

This is a closed book exam.

Non-programmable calculators are allowed.

Question 1: Symmetric Cyphers (25 marks)

A. **Feistel Networks (5 marks)**
What is a Feistel Network? What specific advantages does it bring?

B. **DES (5 marks)**
Show with a diagram DES encryption and decryption, with specific reference to how this is achieved using a Feistel network. Show all input and output block / key sizes. How would you modify DES to increase the key size to when it was Lucifer?

C. **IV, IP, IIP (5 marks)**
Explain the role of an IV, IP and IIP in DES.

D. **Avalanche Effect (10 marks)**
Draw the DES round function. Now explain in detail the avalanche effect, with reference to the importance of rounds, cypher inputs and importance of two fundamental cryptographic primitives.

Question 2: Asymmetric Cryptosystems (25 marks)

A. **Security (5 marks)**
Is a well designed 1024 bit symmetric cypher likely to be stronger or weaker than a well designed 1024 bit asymmetric cypher? Why? Which is likely to run faster? Why?

B. **PGPlite (10 marks)**
Design a quick and dirty secure messaging system showing key setup, authentication and sending of messages between two parties without use of a trusted third party. Suppose your system is required to send large files. Design your system to have have perfect forward secrecy (explain what this means and why it does).

C. **Breaking RSA (10 marks)**
Show mathematically how knowing the factorisation of $n = pq$ that RSA can be broken.

Question 3: Authentication (25 marks)

Suppose a hacker manages to break into the LazySSL certification authority (CA) and steal their private key.

A. Can the hacker eavesdrop on SSL connections to and from BigCorp's website if its uses a certificate issued by LazySSL? (5 marks)

B. BigCorp's website is set up with password based challenge-response authentication over SSL. Explain step by step how the authentication protocol works. (10 marks)

C. Can the hacker impersonate BigCorp to others? If so, please provide an example attack they might launch. If not, explain why BigCorp is still secure. (5 marks)

D. Suppose the hacker instead records an entire SSL session between a BigCorp and a customer. Can the hacker sends this recorded session to BigCorp, logging in as the user? Explain why this may or may not be possible. What is this attack called? (5 marks)

Question 4: General Questions (25 marks)

A. What is bit committment? Explain the purpose and the steps in a bit committment scheme. Design one. (5 marks)

B. Describe an attack on TCP/IP due to lack of strong authentication. (5 marks)

C. What is a buffer overflow? Draw a diagram. Is this more or less of a problem than using weak crypto? (5 marks)

D. What is blinding? Show mathematically how a blinding attack can be made against RSA to trick someone to decode a message. (5 marks)

E. What's worse for security? The invention of PIN numbers or PostIt notes? (5 marks)

This is the end of your questions.

This page has been left blank Intentionally

This page has been left blank Intentionally

This page has been left blank Intentionally