UNIVERSITY OF LONDON
IMPERIAL COLLEGE OF SCIENCE, TECHNOLOGY AND MEDICINE

EXAMINATIONS 1998

MEng Honours Degrees in Computing Part IV
MEng Honours Degree in Information Systems Engineering Part IV
MSci Honours Degree in Mathematics and Computer Science Part IV
MSc Degree in Advanced Computing
for Internal Students of the Imperial College of Science, Technology and Medicine

This paper is also taken for the relevant examinations for the
Diploma of Membership of Imperial College
Associateship of the City and Guilds of London Institute
Associateship of the Royal College of Science

PAPER 4.30 / I4.14

NETWORK SECURITY

Wednesday, May 13th 1998, 10.00 - 12.00

Answer THREE questions

For admin. only: paper contains 4 questions

1a Alice shares a key K with Bob. She uses this to send a ciphertext C to Bob who is able to recover the original plaintext P which contains top-secret information. The police intercept C and demand that Alice surrender her key. Alice surrenders *a key*. The message the police recover is not P but rather a different innocuous message D with no top-secret information.

How did Alice manage to fool the police?

(Hint: use the XOR function for encryption/decryption)

b i) Using diagrams, describe how Cipher Block Chaining (CBC) mode operates at both the sender and receiver.

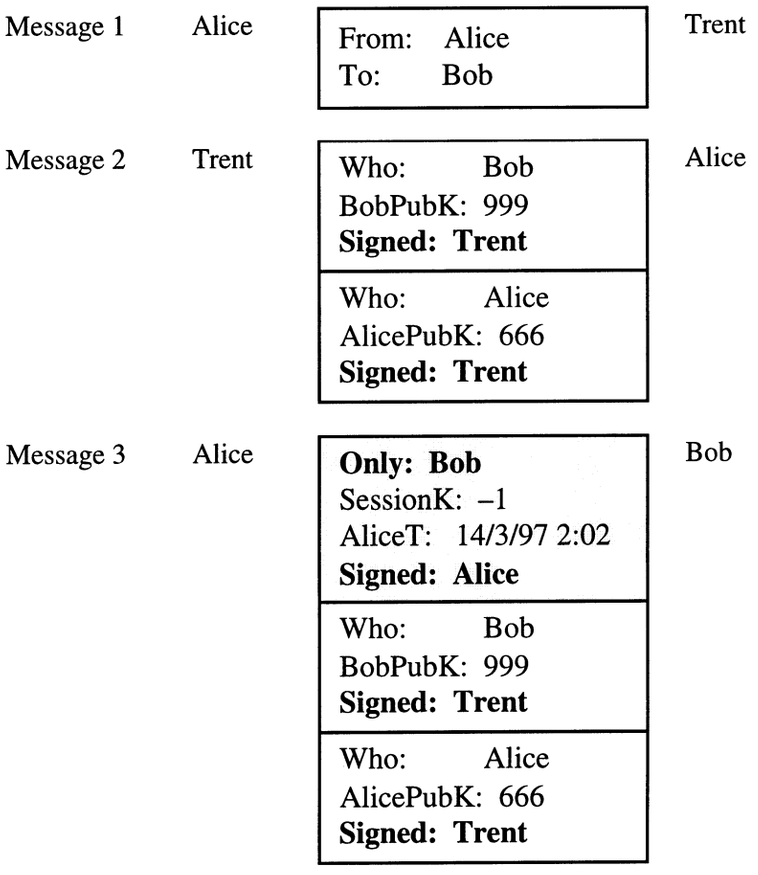
ii) For CBC mode, comment on the effect of a single-bit error in the received ciphertext. i.e. how much of the "decrypted" plaintext will be affected?

iii) For CBC mode, comment on the effect of an intruder inserting or deleting a block of cipher text, i.e. how much of the "decrypted" plaintext will be affected?

c Give two reasons why using a compression/decompression algorithm with encryption /decryption can be worthwhile. If compression is used, is it better to compress before encryption or after? Give reasons for your answer.

The three parts carry, respectively, 25%, 45% and 30% of the marks.

2 Consider the following protocol for authentication and key exchange (Alice and Bob are the main parties, Trent is the trusted 3rd party):



a Outline the purpose of each message and describe how the protocol works.

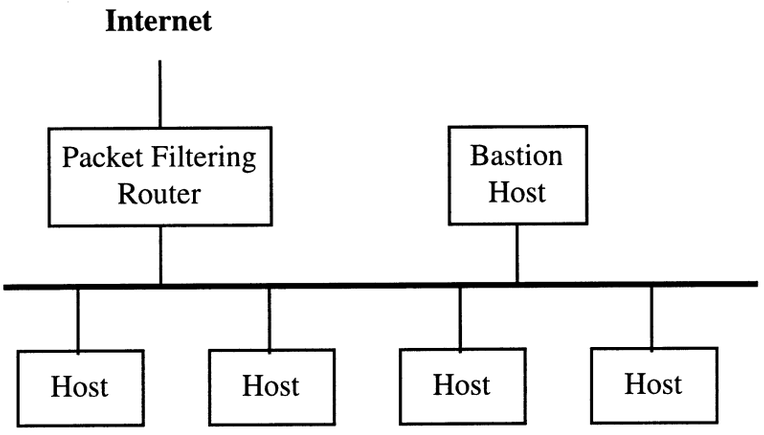
b The protocol can be attacked by Bob, show how Bob can masquerade as Alice for a limited time.

c Finally show how the protocol can be modified to prevent the attack given in part b.

The three parts carry, respectively, 40%, 40% and 20% of the marks.

Turn over...

3a Your organisation decides to adopt the following firewall architecture:



Give a rationale for this architecture and describe how the Bastion Host and the Packet Filtering Router operate.

b Describe how the firewall architecture given in part a could be setup to prevent JAVA applets executing within the companies hosts, whilst allowing other access to non-JAVA web pages on the Internet.

c You are asked to evaluate a firewall solution. List 3 pertinent questions you would ask about each of the following firewall components:

i) Packet Filtering Routers

ii) Application-level Gateways

iii) Circuit-level Gateways

Do not reuse questions in parts (i), (ii) or (iii).

d Your organisation uses a firewall to protect its internal network from external attacks. It is planning on adding a web server. What are the advantages and disadvantages of locating the web server outside of the organisation's firewall?

The four parts carry, respectively, 20%, 20%, 30% and 30% of the marks.

4a What is "salt"? In what way does the salt increase the security of a password system? Would a salt size of 64-bits effectively thwart password cracking? Give a reason for your answer.

b Suppose that the UNIX password file is removed and replaced with a publicly readable file called /etc/publickey. The entry in the file for a user consists of the user's login id, the user's public key (RSA 512 bits) and an encrypted version of the corresponding private key (RSA 512 bits). The private key is encrypted using DES where the DES key is the user's login password.

i) Explain how the system can verify that a password is correct.

ii) Explain how an opponent could attack this password system using a dictionary attack

iii) Work out the number of DES encryptions/decryptions and RSA encryptions/decryptions required for the dictionary attack given in step b(ii) given a dictionary of 4 million words and a password file of 100 users.

iv) Work out the number of DES encryptions required for the dictionary attack against the normal UNIX password system. Again assume a dictionary of 4 million words and a password file of 100 users.

c A top computing department in London has a group of brilliant lecturers who regularly travel around the world collaborating with colleagues. The travelling lecturers always take up any invitation to use their colleagues computers to telnet back to their department's system. Show how one-time passwords can be used to counteract eavesdroppers and password sniffers that are interested in acquiring our traveller's passwords. List the disadvantages (if any) of using one-time passwords.

The three parts carry, respectively, 20%, 60% and 20% of the marks.

End of paper