UNIVERSITY OF LONDON

IMPERIAL COLLEGE OF SCIENCE, TECHNOLOGY AND MEDICINE

EXAMINATIONS 1997

MEng Honours Degrees in Computing Part IV
MEng Honours Degree in Information Systems Engineering 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

PAPER 4.30 / I4.14

NETWORK SECURITY

Wednesday, May 7th 1997, 10.00 - 12.00

Answer THREE questions

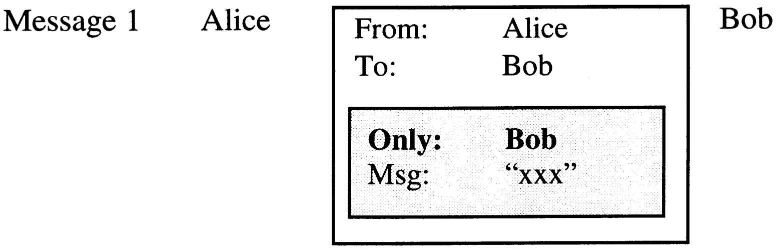
For admin. only: paper contains 4 questions

1a Suppose that someone suggests the following scheme for confirming that you have the same secret key as a collaborator. You create a random bit string the same length as the key, XOR it with the key, and send the XORed result over the network to your collaborator. Your collaborator XORs the incoming message with the key (which is the same as your key) and sends the result back to you. You check the reply message, and if what you receive is your original random string, you would have verified that your collaborator has the same secret key, yet neither of you has transmitted the key.

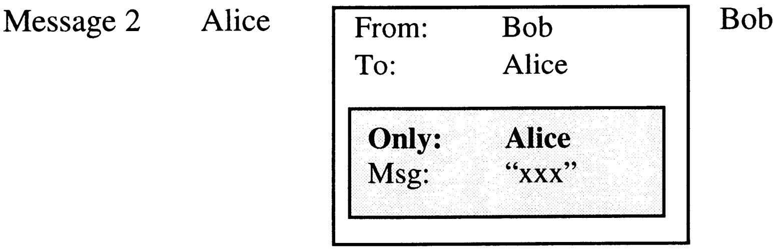
What is the flaw in this scheme?

b A small company decides to adopt the following message protocol for confidential communications between its network users (e.g. Alice, Bob, Carol, and Max):

- Alice (the sender) encrypts her message for Bob with Bob's public key and sends it to Bob along with her id and Bob's id, i.e:



- Bob (the recipient) always acknowledges receipt by sending an encrypted copy of the message back to Alice along with his id and Alice's id. The copy is encrypted with Alice's public key, i.e:



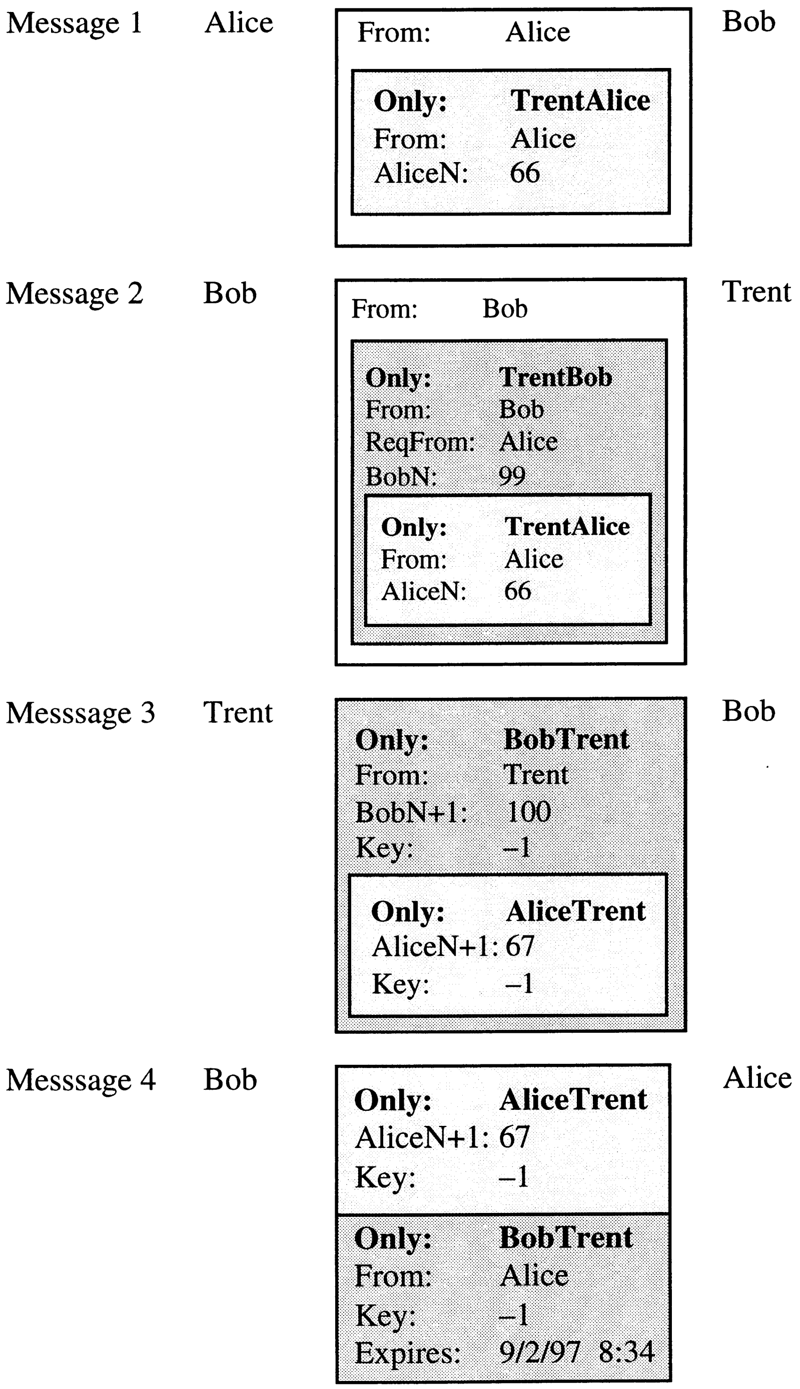
i) Show that it is possible for another network user (e.g. Max) to recover the message "xxx".

ii) Without using nonces or timestamps explain how the protocol can be modified to prevent the attack that you give in 1b(i).

c Without using any other party, extend the Diffie-Hellman protocol to work with 3 parties, Alice, Bob and Carol.

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

2 Consider the following protocol for mutual authentication and key exchange in client-server applications (Alice is the client, Bob is the Server, Trent is the authentication server):



Message 1 Alice → Bob

From: Alice

Only: **TrentAlice**
From: Alice
AliceN: 66

Message 2 Bob → Trent

From: Bob

Only: **TrentBob**
From: Bob
ReqFrom: Alice
BobN: 99

Only: **TrentAlice**
From: Alice
AliceN: 66

Messsage 3 Trent → Bob

Only: **BobTrent**
From: Trent
BobN+1: 100
Key: -1

Only: **AliceTrent**
AliceN+1: 67
Key: -1

Messsage 4 Bob → Alice

Only: **AliceTrent**
AliceN+1: 67
Key: -1

Only: **BobTrent**
From: Alice
Key: -1
Expires: 9/2/97 8:34

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

b For each message explain what happens if the message is replayed to the recipient by an intruder.

c Using the encrypted BobTrent portion of message 4, develop a protocol that can be used by Alice for a subsequent authentication with Bob.

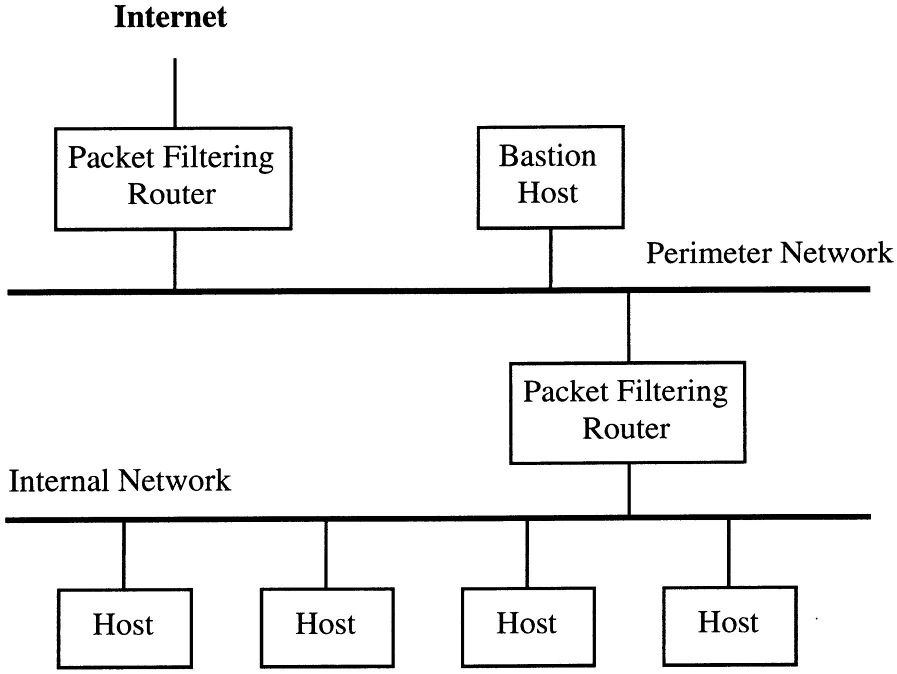
The three parts carry, respectively, 50%, 25% and 25% of the marks.

Turn over ...

3a i) Describe how packet filtering is performed, for example by a packet filtering router.

ii) Some protocols, such as FTP, perform a dynamic "call-back" connection from the server. Explain how this can pose problems for packet-filtering routers and what filtering rules can be used to reduce the security risk.

b A company adopts the following firewall architecture:



Give a rationale for this architecture and describe how the bastion host and each of the packet filtering routers operate.

c A company has two separate sites each with its own network. The company would like to use the Internet to securely interconnect the two sites such that users and hosts at either site can communicate with users and hosts at the other site. The company does not want users at either of the sites to have access to the Internet, or for Internet users to be able to access any company machine. Devise a suitable solution for the company.

The three parts carry, respectively, 30%, 50% and 20% of the marks.

4a Define the terms: virus, worm, trojan horse and trapdoor.

b Describe the four categories of potential attacks Java applets could facilitate and give an example of each.

c Explain why Java applets are not allowed to open network connections to any machine and also why Java applets are not allowed to open incoming network connections.

d Describe how a malicious applet could exploit the network connection allowed back to the downloading host machine to attack the Java end-user.

e Discuss the pros and cons of using digital signatures to sign Java applets.

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

End of paper