UNIVERSITY OF LONDON
IMPERIAL COLLEGE OF SCIENCE, TECHNOLOGY AND MEDICINE

EXAMINATIONS 2000

MEng Honours Degree in Information Systems Engineering Part IV
MEng Honours Degree in Mathematics and Computer Science Part IV
MEng Honours Degrees in Computing Part IV
MSc 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 Associateship of the City and Guilds of London Institute
This paper is also taken for the relevant examinations for the Associateship of the Royal College of Science

PAPER C430=I4.14

NETWORK SECURITY

Tuesday 16 May 2000, 14:30
Duration: 120 minutes

Answer THREE questions

Paper contains 4 questions

1a Explain the terms *diffusion*, *confusion* and the *avalanche effect* as applied to a block cipher such as DES?

b What is a Feistel Cipher? Illustrate your answer by showing the encryption steps for a 3 round Fiestel cipher.

c For the 3 round Feistel cipher derived in part b, prove that the decryption of the ciphertext produces the original plaintext.

d For a block cipher such as DES, explain the consequences if the following were true:

$$E_{k1}(E_{k2}(P)) = E_{k3}(P)$$

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

2a Define the terms, *one-way function* and *trapdoor one-way function*. In what way is RSA one-way?

b Is RSA unconditionally secure? Explain.

c You discover a method for factorising very large numbers very quickly. Explain how you can use this knowledge to recover the plaintext of an RSA encrypted message. Provide an example with small numbers to illustrate your recovery method.

d Trent is a trusted third party. Alice wants him to sign a document, but doesn't want him to see the contents of the document. Trent is happy with this, his signature is proof that he signed the document and it will convince Trent that he signed the document if it is ever shown to him.

Using RSA we have the following message exchange:

A→T: $C = R^E * P \bmod N$, R is a random number, gcd(R, N)=1, P is the document. E and D are Trent's encryption and decryption keys.

T→A: $C^D \bmod N$

Using the properties of RSA and modular arithmetic, show how Alice can use this message exchange to subsequently extract a document S signed by Trent.

The four parts carry, respectively, 20%, 10%, 40%, and 30% of the marks.

3a Discuss the risks of using timestamps in cryptographic protocols to ensure freshness and detect replays. How should a timestamp check function be implemented?

b Consider the following protocol for authentication and key exchange where Alice is the initiator, Bob is the responder, and Trent the trusted third party:

	From	Message	To
Message 1.1 A→T: $E_{K_{AT}}(T_A, B, K)$	Alice	**Only: AliceTrent** AliceT: 25/12/2000, 16:12:56 To: Bob SessionK: –1	Trent
Message 1.2 T→B: $E_{K_{BT}}(T_T, A, K)$	Trent	**Only: BobTrent** TrentT: 25/12/2000, 16:12:57 From: Alice SessionK: –1	Bob

For this protocol outline the purpose of each message and describe how the protocol works. Identify at least 3 weaknesses in the protocol and explain whether the protocol achieves mutual authentication. Assume that the protocol is not run concurrently between two parties.

c Now assume that Alice can run the protocol once as an initiator and once as a responder, possibly concurrently. Show that this leads to a simple attack for an adversary. Identify another attack an adversary could perform if Bob could run the protocol concurrently.

d An adversary Max intercepts message 1.2 and sends it to Trent as a new request (call this message 2.1).

Trent responds with message 2.2, which is also intercepted by Max.

Max sends message 2.2 to Trent as another new request (message 3.1).

Trent responds with message 3.2, which Max also intercepts.

Finally Max sends message 3.2 to Bob.

There are two problems that this message play highlights. What are they?

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

4a Discuss the risks to a web user's privacy posed by the following:

i) Web Server log files

ii) Refer Links

iii) Cookies

iv) Search Engines

b Suggest 10 security precautions that a *Web server administrator* should adopt.

c You are asked to examine the source of a CGI-script to see if it is safe to deploy. Describe 5 things that you would you look for? Give reasons for your choices.

d Describe how a web site such as **www.doc.ic.ac.uk** might be spoofed by someone in New Zealand. You can assume that only web pages are transferred. Would the use of **https** prevent the spoofing? Explain.

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