Ollscoil na hÉireann, Gaillimh
National University of Ireland, Galway

GX 1489

Semester 1 Examinations, 2003 / 2004

Exam Code(s)	4IF1
Exam(s)	Fourth University Examination in Information Technology
Module Code(s)	CT425
Module(s)	Advanced Communications
Paper No.	1
External Examiner(s)	Prof. P. Nixon
Internal Examiner(s)	Prof. G. Lyons Dr. M. Schukat

Instructions: Answer any 3 questions.
All questions will be marked equally.

Duration	2 hrs
No. of Answer Books	1
No. of Pages	4
Department(s)	Information Technology

Q.1.

(i) *10 marks*
Explain in some detail, how both *Feistel Ciphers* and *Feistel Networks* are used in cryptographic algorithms.
Give an example of how subkeys can be derived from a private key in order to facilitate a Feistel Network.

(ii) 10 *marks*
How can a *Pseudo-Random Generator* (PRG) be used to implement a stream cipher? Design a PRG based on a *Linear Feedback Shift Register* (LFSR) and provide some (pseudo-) code fragments, which detail how a LFSR can be implemented.

(iii) 10 *marks*
Describe in some detail the features of the *DES* algorithm outlining both strengths and weaknesses of this algorithm. Distinguish between the following block cipher modes of operation:

- electronic codebook mode
- cipher block chaining mode
- cipher feedback mode

Q.2.

(i) *10 marks*
Describe some problems associated with private key distribution for conventional encryption and show the benefits of a *key distribution center* (KDC) and the use of *master keys* and *session keys*.

(ii) *10 marks*
Outline advantages and disadvantages of the following management and distribution strategies for public keys:

- uncontrolled publication
- public key directories
- public key authorities
- certificate authorities

(iii) *10 marks*
Describe in some detail, how the *Diffie-Hellman* key exchange algorithm and the *RSA* algorithm can be used to distribute session keys suitable for private key encryption algorithms.

Q.3.

(i) *15 marks*
Describe in some detail, how

- private key encryption,
- public key encryption,
- message authentication codes (MACs) and
- hash functions

can be used for message authentication.

(ii) *15 marks*
What are the characteristics of a *zero-knowledge protocol*?
Outline the core features of the *Goldreich-Micali-Wigderson* protocol (which is based on graph-isomorphism) and explain the terms *accreditation* and *cut-and-choose*.

Q.4.

(i) *15 marks*
Write an essay on *IPSec* looking at the following issues:

- Distinguish between the terms *encapsulating security payload* (ESP) and *authentication header* (AH).
- Describe the different services which AH and ESP can provide.
- Distinguish between the terms *transport mode security association* and *tunnel mode security association*.
- Describe how IPSec provides an *anti-replay* service.
- Explain in some detail, how security associations can be combined. Use examples to illustrate your answer.

(ii) *15 marks*
Your task is to design an *authentication service* to be used by NUI Galway students and staff members. This authentication service provides certificates on request, each containing one signed public key. The public key will be used to provide authentication and/or confidentiality of emails.
Your proposal should be based on the X.509 recommendation and should give details about

- a suitable *certification authority* (CA) organization or hierarchy.
- the structure and format of two different certificate classes e.g. a *simple* certificate for private emails and a *trusted* certificate for official emails.
- mechanisms or protocols, which allow a user to acquire a *simple* or *trusted* certificate by getting his/her public key signed by the CA.
- a simple procedure which allows a user to verify the integrity of a certificate.

Q.5.

(i) *15 marks*
Network security is an important issue with 802.11. Describe features and characteristics of the *wireless equivalent privacy* (WEP) encryption and show how alternative security measurements can improve or complete authentication and encryption in wireless networks based on 802.11.

(ii) *15 marks*
Describe in some detail the *medium access* (MAC) sublayer of 802.11 by looking at the following issues:

- Why and how are data transmissions acknowledged?
- What is the *hidden node* problem and how is it solved?
- Distinguish between the *distributed coordination function* (DCF) and the *point coordination function* (PCF).
- Distinguish between the *physical carrier-sensing function* and the *virtual carrier-sensing function*, which is based on the *network allocation vector* (NAV).
- What is the purpose of *interframe spacing*?
- How is packet *fragmentation* and *reassembly* achieved?

Q.6.

(i) *15 marks*
Write an essay on *Bluetooth technology* covering the following topics:

- What is a *piconet* and what does a piconet topology look like?
- How are *piconets* set up?
- How is *data transmission* and *data retransmission* between a master and a slave device realized?
- Distinguish between *asynchronous connectionless link* (ASL) and *synchronous connection-oriented link* (SCO).
- What are the Bluetooth *core protocols* and what functionality do they have?

(ii) *15 marks*
Explain in some detail how Bluetooth is currently used in computer, telecommunication and consumer products.
Identify new areas and products, which could be used for Bluetooth or Bluetooth-like technologies in five years time.