GX 0086

Ollscoil na hÉireann, Gaillimh
National University of Ireland, Galway

Semester 1 Examinations, 2005 / 2006

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. J. A. Keane
Internal Examiner(s)	Dr. M. Madden
	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	3
Department(s)	Information Technology

Q.1.

(i) *10 marks*
Assume that you are a network security consultant who is hired by a bank to check out network vulnerabilities. One of your duties is to make staff aware of typical security threats in a network environment.
Therefore describe the **four** conceptual types of security attacks. Use real-world examples to illustrate these threats.

(ii) 10 *marks*
Assume that you are a software engineer working for a mobile phone company. For demonstration purposes you are asked to implement a simple stream cipher algorithm in a mobile phone, which encodes and decodes a serial voice-data stream bit by bit. The stream key should be based on a linear feedback shift register.
Provide a diagram and some pseudo-code that describe the generating of the stream key as well as the encoding and decoding of the voice data.

(iii) 10 *marks*
For educational purposes you are asked to provide a software-simulator of a rotor machine that implements a *Rotor-Cipher* (or *N-Stage Polyalphabetic Substitution Cipher*) consisting of three rotors. The simulator should provide sufficient details for a user to understand the concept of a rotor cipher. How would you design the GUI of the simulator and what level of detail for the cipher should the GUI provide?

Q.2.

(i) *6 marks*
In your job as a security consultant you come across a company that still uses 56-bit DES for data encryption. What alternatives would you suggest to this company to increase security?

(ii) *12 marks*
Assume that you are hired by a company to implement the Diffie-Hellman Key exchange algorithm in one of their products.
Outline the algorithm in some detail and describe, how you intent
- to implement the required prime number test,
- to implement the required primitive root test, and
- to accelerate/simplify the calculation of expressions A^B mod C.

(iii) *12 marks*
The same company asks you to develop a (secret) session key exchange protocol that is based on the public-key encryption algorithm RSA (remark: the exchanged session key will be used for a symmetric key encryption algorithm like DES).
Describe the major steps that are required to exchange a session key. Your proposal should provide both authentication and confidentiality and should resist a man-in-the-middle attack.

Q.3.

(i) *15 marks*
A company hires you to introduce/implement message authentication for their internal email system. The aim is to provide authentication for every single email that is sent around. Provide
- two procedures that take advantage of public key encryption,
- two procedures that are based on hash functions, and
- two procedures that are based on message authentication codes.

(ii) *15 marks*
The Western Health Board hires you to develop the prototype a new medical card that is based on a smartcard, which contains a small microprocessor. An external card reader will be used to authenticate the card and to retrieve patient information that is stored in it. Due to hardware constraints a zero-knowledge protocol (ZKP) must be used for the card authentication.
Your task is to
- choose an appropriate ZKP,
- show how the chosen ZKP is executed both on the card reader and the smartcard, and
- describe how accreditation is achieved during a number of ZKP iterations.

Q.4.

(i) *10 marks*
Describe in some detail how *Kerberos* provides authentication in a client-server environment.
How can authentication be provided between realms?

(ii) *10 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 CA (Certification Authority) organisation 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, and
- a simple procedure, which allows a user to verify the integrity of a certificate.

(iii) *10 marks*
Describe in some detail possible network security threats and suitable firewall solutions for the following scenarios:
- A private user surfs occasionally on the Internet. He/she uses an ordinary PC and has a 56K modem to connect to the local Internet provider.
- A company is connected to the Internet through a leased line. Its intranet consists of a web-server, a mail server and a few PC workstations. PC users are allowed to access the Internet.

Q.5.

(i) *15 marks*
Network security is an important issue with wireless networks. Based on 802.11 show in some detail, how existing security protocols and security measurements are already applied or can be applied.

(ii) *15 marks*
Describe in some detail the *medium access* (MAC) sublayer of 802.11 by looking at the following issues:
- Distinguish between the operation modes BSS (Basis Service Set) and ESS (extended service set).
- How does message *fragmentation* and *reassembly* work?
- Why and how are data transmissions acknowledged?
- What is the *hidden node* problem and how is it solved?
- 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*?