

NATIONAL UNIVERSITY OF IRELAND, GALWAY
OLLSCOIL NA hÉIREANN

SEMESTER I, AUTUMN 2002 EXAMINATION

Fourth University Examination in Information Technology

CT425 Advanced Communications

Prof. P. Nixon
Prof. G. Lyons
Dr. M. Schukat

Time Allowed: **Two Hours**

Answer any three questions

Q.1.

(i) *10 marks*

Outline the operation of

- a S-Box,
- a P-Box and
- a Substitution-Permutation Network.

Provide some (pseudo-) code fragments, which implement a S-Box and a P-Box.

(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 implement a LFSR.

(iii) *10 marks*

Based on the prime number $p = 5$ describe the relevant steps of a Diffie-Hellman key exchange between two partners A and B:

- Choose a primitive root a , which is used by both parties.
- Select private values X_A and X_B
- Calculate public values Y_A and Y_B
- "Exchange" Y_A and Y_B and calculate the key value K .

Q.2.

(i) 15 marks

Write an essay on IPSec.

(ii) 15 marks

Design a *Virtual Private Network* architecture based on IPSec suitable for the following scenario:

- A business consists of two branch offices and one home office. Each branch office has an intranet with a central server and a number of clients. They are connected to the Internet using a leased line each. The home office consists of a single PC-client with a DSL or 56K modem connection. The client dials into the Internet via an Internet Service Provider.

Provide a VPN solution that provides secure authentication and confidentiality for any kind of internal/external client/server communication by choosing suitable combined security associations. Draw a schematic to illustrate your design.

Q.3.

(i) 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 can 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) 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 allows 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.

(ii) 15 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.
- Four PC owners living in the same house want to share a fast DSL connection. They have already set up their own intranet, but have not bought any modem or firewall equipment yet.
- A company is already 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.4.

(i) 15 marks

Write an essay on 802.11.

(ii) 15 marks

AerRianta wants to implement a wireless information system based on 802.11 in Dublin Airport. This service will be offered to *all* passengers or visitors with wireless connectivity (like a laptop/palmtop with a 802.11 PCMCIA card) within the terminal buildings. The system will provide some general information like departure + arrival times, maps, parking info etc.

Your task is to submit a proposal for the overall system architecture focusing on

- the design of the wireless network
- the requirements of and the services to be offered by the Access Points
- the connectivity to a Web-server, which provides the information

Q.5.

(i) 15 marks

Write an essay on Bluetooth.

(ii) 15 marks

What are the main differences and similarities between Bluetooth and 802.11? Describe the role both technologies will have in coming years and describe (existing and if possible new) domains, where these technologies are used or will be used.