UNIVERSITY OF DUBLIN

TRINITY COLLEGE

Faculty of Engineering, Mathematics & Science
School of Computer Science & Statistics

Integrated Computer Science Programme **Trinity Term 2014**
Year 3 Annual Examinations

Advanced Telecommunications (CS3031)

Monday 28th April, 2014 RDS, Main Hall 14:00 – 16:00

Mr. Niall O'Hara

Instructions to Candidates:

- Answer TWO questions
- All questions carry equal marks
- Use diagrams where appropriate

Materials permitted for this examination:

- Non-programmable calculators are permitted for this examination

Q1

a) Describe in detail the four fundamental channel-access schemes used in a telecommunications system highlighting their strengths and weaknesses. Give an example of an application of each scheme (or a combination of them).

(16 marks)

b) With the aid of a diagram describe the main entities that comprise a 2G (GSM) and 3G (UMTS) mobile network architecture. List the purpose and functions of each component and the interactions between them.

(15 marks)

c) Explain what is meant by the "Hidden Terminal" and "Exposed Terminal" problems; give examples of each. Describe in detail a multiple access method used in 802.11 networks to avoid collisions.

(15 marks)

d) Sometimes when a mobile user crosses the boundary from one cell to another, the current call is abruptly terminated, even though all transmitters and receivers are functioning perfectly. Why?

(4 marks)

[50 marks]

Q2

a) The Diffie-Hellman key exchange is being used to establish a secret key between Alice and Bob. Alice sends Bob (227, 5, 82). Bob responds with (125). Alice's secret number, x, is 12, and Bob's secret number, y, is 3. Show how Alice and Bob compute the secret key.

(15 marks)

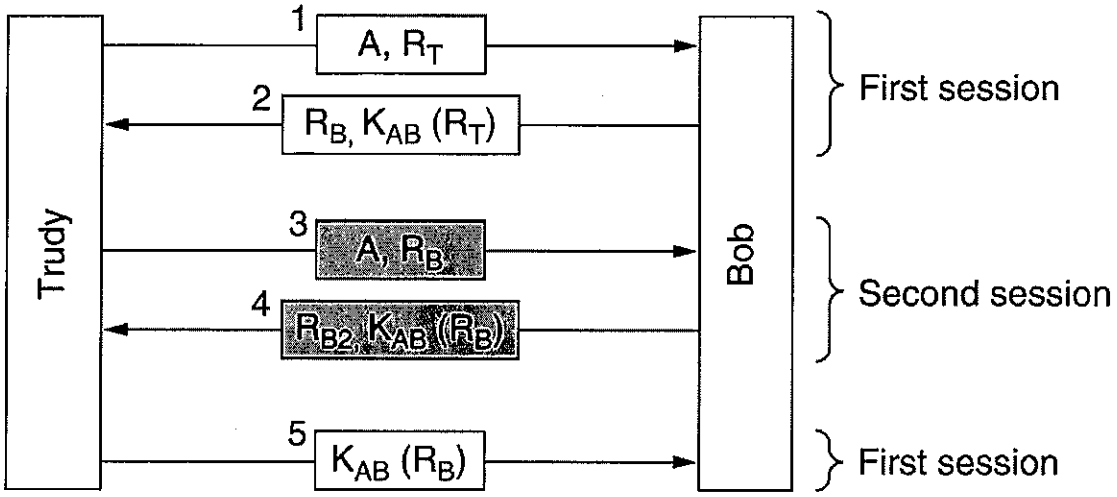
b) Alice used a transposition cipher to encrypt her messages to Bob. For added security, she encrypted the transposition cipher key using a substitution cipher, and kept the encrypted cipher in her computer. Trudy managed to get hold of the encrypted transposition cipher key. Can Trudy decipher Alice's messages to Bob? Why or why not?

(15 marks)

c) Alice wants to communicate with Bob using public-key cryptography. She establishes a connection to someone she hopes is Bob. She asks him for his public key and he sends it to her in plaintext along with an X.509 certificate signed by the root CA. Alice already has the public key of the root CA. What steps does Alice carry out to verify that she is talking to Bob?

(15 marks)

d) Change one message in the exchange below in a minor way to make it resistant to the reflection attack. Explain why this change works.



(5 marks)

[50 marks]

Q3

a) Explain the difference between the TCP and UDP Internet Protocols (IP) under the following headings: Connection, Function, Usage (Suitable for), Reliability, Packet Ordering, Speed of transfer, Data Flow Control, Error Checking, Handshake, Examples (e.g. HTTP = TCP).

(20 marks)

b) What is DNS, what protocol does it use and what would the implications be if all DNS servers worldwide went offline at the same time?

(5 marks)

c) Describe in detail the operation of and the benefits provided by a Content Distribution Network (CDN).

(10 marks)

d) How can a multimedia application recover from packet loss without the need for retransmission? Describe in detail three methods discussed in lectures.

(15 marks)

[50 marks]