Coláiste na Tríonóide, Baile Átha Cliath
Trinity College Dublin
Ollscoil Átha Cliath | The University of Dublin

Faculty of Engineering, Mathematics and Science

School of Computer Science & Statistics

Integrated Computer Science Programme **Trinity Term 2019**
Year 3 Annual Examinations

Advanced Telecommunications

Sample Paper

Dr Hitesh Tewari

Instructions to Candidates:

Answer all questions. Each question is scored out of a total of 50 marks.

You may not start this examination until instructed to do so by the invigilator.

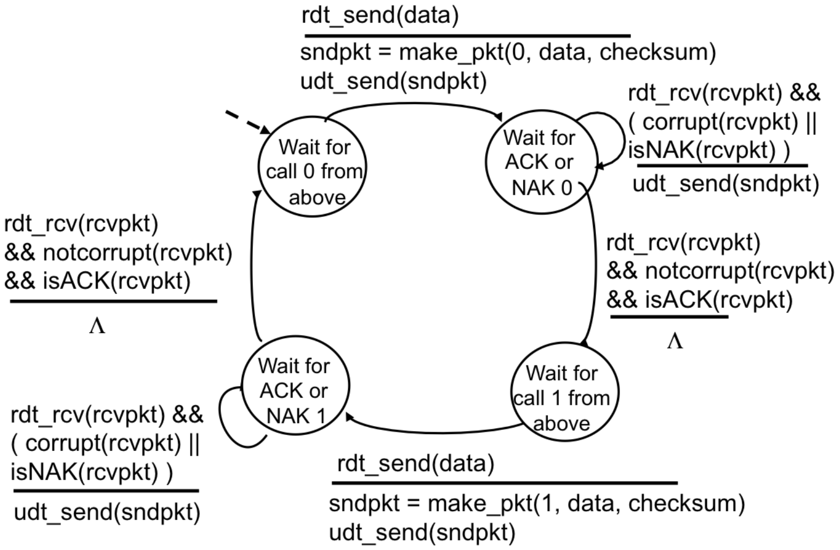
Exam paper is not to be removed from the venue.

Materials Permitted for this Examination:

Non-programmable calculators are permitted for this examination — please indicate the make and model of your calculator on each answer book used.

1. (a) Distinguish between the user datagram protocol (UDP) and the transport control protocol (TCP) in terms of reliable data transfer, header size and connection overheads. For IP Telephony and IP Videoconferencing, which one of TCP and UDP would be preferable. Justify your answer. [10 marks]

   (b) The diagram below shows the finite state machine (FSM) for a reliable sender that can handle garbled ACKs and NAKs. Draw the FSM for the corresponding receiver.



[12 marks]

   (c) With the help of a FSM describe the main building blocks of the TCP Congestion Control algorithm. You are required to detail the state transitions in the FSM. [12 marks]

   (d) What is the role of a "web proxy" in a large institutional network? What are the main advantages of installing a proxy server? [6 marks]

   (e) What is a "websocket" and what are its advantages over technologies such as AJAX and Comet? Why are websockets more efficient than traditional HTTP exchanges - explain? [10 marks]

2. (a) Describe the electronic code book (ECB) mode used in the DES cipher. Explain how the cipher block chaining (CBC) mode overcomes the block substitution attack of ECB mode. Explain why the output feedback mode (OFB) is described as being a "synchronous stream cipher". [10 marks]

(b) Computing modular exponentiation efficiently is inevitable for the practicability of RSA. Compute the following exponentiation x^e mod m by applying the square-and-multiply algorithm:

$$x = 2, e = 79, m = 101$$

After every iteration, show the exponent of the intermediate result. [10 marks]

(c) What are the distinguishing characteristics of a Group? What is the order $ord(a)$ of a group $(G, \circ)$? Determine the order of $a = 3$ in $\mathbb{Z}_{11}^*$. Let G be a finite cyclic group. Find the number of primitive elements in $\mathbb{Z}_5^*$. [10 marks]

(d) Describe in detail the cryptographic techniques used to achieve "distributed consensus" in the Bitcoin network using the proof-of-work (PoW) algorithm. What are the limiting factors of the scheme? [8 marks]

(e) Given the elliptic curve E over $\mathbb{Z}_{17}$ and the base point $P = (5, 1)$:

$$E : y^2 = x^3 + 4x + 20 \ mod\ 17$$

Calculate the following point multiplication $2P$ using the formulas provided below:

$$x_3 = s^2 - x_1 - x_2 \bmod p$$
$$y_3 = s(x_1 - x_3) - y_1 \bmod p$$

where

$$s = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} \bmod p \text{ ; if } P \neq Q \text{ (point addition)} \\ \frac{3x_1^2 + a}{2y_1} \bmod p \text{ ; if } P = Q \text{ (point doubling)} \end{cases}$$

You are required to show the extended euclidean algorithm (EEA) calculation for computing the multiplicative inverse.

[12 marks]