**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** **Semester 2 2019**
**Year 3 Annual Examinations**

# Advanced Telecommunications

**Saturday 27th April 2019** **RDS-Sim Court** **09:30 – 11:30**

**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.

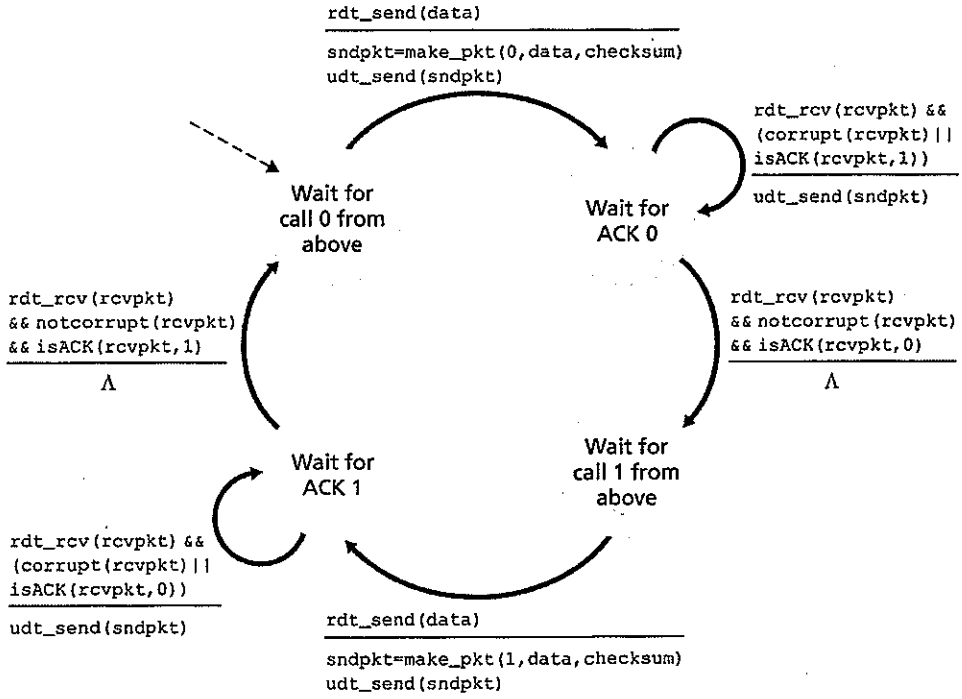
Exam paper is not to be removed from the venue.

## 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) Explain how the transmission control protocol (TCP) uses the services of an unreliable network layer to provide reliable end-to-end communications? Show with the aid of an example how TCP can correctly demultiplex packets arriving from two hosts (A and B), who by coincidence happen to pick the same source port number (5099), and are communicating with the same web server on port 80. [8 marks]

   (b) The figure below depicts a finite state machine (FSM) for a NAK-free reliable data transfer protocol for a channel with bit errors.




   Draw the corresponding FSM for the receiver side of the protocol. What additions are required to the FSM on the receiver side in order to use an ACK only primitive? [14 marks]

   (c) Consider transferring an enormous file of $L$ bytes from Host A to Host B. Assume a maximum segment size (MSS) of 536 bytes.

      i. What is the maximum value of $L$ such that the TCP sequence numbers are not exhausted?

      ii. For the $L$ you obtain in (i), find how long it takes to transmit the file? Assume that a total of 66 bytes of transport, network and data-link header

are added to each segment before the resulting packet is sent out over a 155 Mbps link. Ignore flow and congestion control, and assume that Host A can pump out the segments back to back and continuously.

[12 marks]

(d) With the aid of a diagram distinguish between "persistent" and "non-persistent" HTTP connections in terms of the round trip time (RTT) and TCP overhead. What improvements can "pipelining" bring to a persistent HTTP connection in terms of the RTT? [7 marks]

(e) Imagine a peer-to-peer network (P2P) where $N$ users want to communicate in an authenticated and confidential manner without a centralized trusted third party (TTP).

i. How many keys are collectively needed if symmetric key algorithms are deployed?

ii. How are the numbers changed if we make use of a key distribution center (KDC)?

iii. How many keys are needed if we make use of asymmetric key algorithms?

[9 marks]

2. (a) One of the most attractive applications for public-key cryptography is the establishment of a secure "session key". In practice it is desirable that both communication parties influence the selection of the session key, so as to prevent one party from choosing a *weak key*. Develop a protocol in which both Alice and Bob who posses a pair of public/private keys of the RSA cryptosystem are able to influence the selection of the session key. [6 marks]

   (b) Using the Miller-Rabin primality test show how one can assume with a high probability that the number 269 is a prime number, given that the decomposition of an odd prime candidate can be represented by $\tilde{p} - 1 = 2^u \cdot r$, where $r$ is odd. [10 marks]

   (c) Let $\mathbb{Z}^*_{269}$ be a finite cyclic group. Find the number of primitive roots in $\mathbb{Z}^*_{269}$. Find the least primitive root of $\mathbb{Z}^*_{269}$. [10 marks]

   (d) Given the elliptic curve $E$ over $\mathbb{Z}_{29}$ and the base point $P = (8, 10)$:

   $$E : y^2 = x^3 + 4x + 20 \bmod 29$$

   Calculate the following point multiplication $k \cdot P$ (where $k = 2$) using the formulae 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]

   (e) What are the advantages of a virtual private network (VPN) over a dedicated private secure Internet link? Describe the functionality of the IPsec "Transport" and "Tunnel" modes. In particular, describe with the aid of a diagram how the header and payload of an IP datagram can be protected by deploying IPsec in "Tunnel Mode with ESP" (ESP - encapsulation security payload). Note that you are required to identify the relevant IPsec header and trailer fields. [12 marks]