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 2017**
Year 3 Annual Examinations

Advanced Telecoms

3rd May 2017 **RDS Main Hall** **09:30 – 11:30**

Dr Hitesh Tewari

Instructions to Candidates:

Attempt **two** questions. All questions carry equal marks. Each question is scored out of a total of 50 marks.

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

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) Suppose Client A requests a web page from Server S through HTTP and its socket is associated with port 33000.

   (i) What are the source and destination ports for the segments sent from A to S?

   (ii) Can Client A contact Server S using UDP as the transport protocol?

   (iii) Can Client A request multiple resources in a single TCP connection?

   Give reasons for your answers. [6 marks]

   (b) Describe the basic server hierarchy within the domain name system (DNS). Outline the minimum steps required in terms of DNS entries (including the Web and Email domains) that are required to register your new start-up "networkutopia.com". [10 marks]

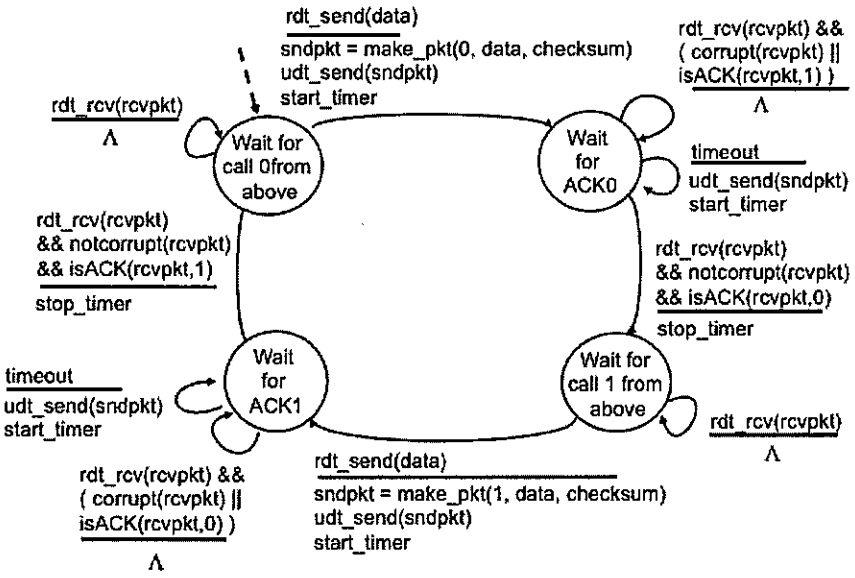
   (c) What are the services provided by the DNSSEC protocol? Describe how DNSSEC validation takes place within a zone by detailing the various Resource Records (RRs), RRsets and Signature Keys that are required to secure a domain. [12 marks]

   (d) Distinguish between centralized and decentralized P2P services. [8 marks]

   (e) Consider distributing a file $F = 15$ Gbits to N peers. The server has an upload rate of $u_s = 30$ Mbps, and each peer has a download rate of $d_i = 2$ Mbps and an upload rate of u. For $N = 1000$ and $u = 2$ Mbps calculate the minimum distribution time for both client-server and P2P configurations. [14 marks]

2. (a) Describe why an application developer might decide to run an application over UDP rather than TCP. How is a UDP socket fully identified? What about a TCP socket? [8 marks]

(b) The diagram below shows a finite state machine (FSM) for a reliable sender over a lossy channel with bit errors. Draw the FSM of the corresponding receiver.

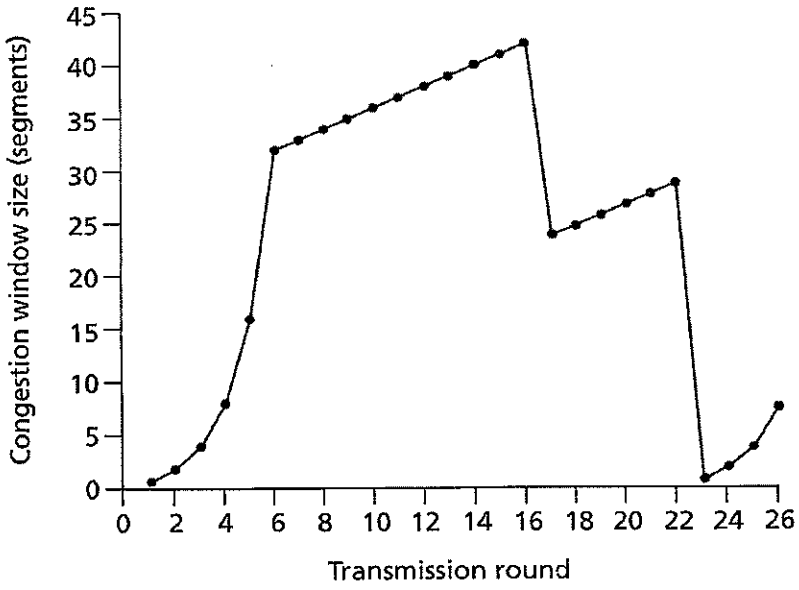


[9 marks]

(c) What do you understand by the term "Congestion Control" in the context of a data transmission network? Describe the two main approaches towards congestion control. In particular, outline as to how congestion control is managed in asynchronous transfer mode (ATM) networks. [8 marks]

(d) Briefly describe the main building blocks of the TCP Congestion Control algorithm [9 marks]

(e) Assuming TCP Reno is the protocol experiencing the behaviour shown in the figure below, answer the following questions. In all cases, you should provide a short discussion justifying your answer.



(i) Identify the intervals of time when TCP slow start is operating.

(ii) Identify the intervals of time when TCP congestion avoidance is operating.

(iii) After the 16^{th} transmission round, is segment loss detected by a triple duplicate ACK or by a timeout?

(iv) What is the value of *ssthresh* at the 18^{th} transmission round?

[16 marks]

3. (a) In modern cryptosystems the encryption technique is known - published, standardised, and available to everyone, even a potential intruder. Then where does the security of an encryption technique come from? [4 marks]

   (b) What is Fermat's Little Theorem and why is it useful in the context of primality testing? Show that 53 is a prime number using Fermat's theorem. [8 marks]

   (c) Suppose that a system uses PKI based on a tree-structured hierarchy of CAs. Alice wants to communicate with Bob, and receives a X.509 certificate from Bob signed by a CA X after establishing communications channel with Bob. Suppose Alice has never heard of X. Describe in detail as to what steps Alice takes in order to verify that she is talking to Bob? [12 marks]

   (d) What are the distinguishing characteristics of a Group? Determine the order of $a = 4$ in the group $\mathbb{Z}_{11}^*$. Is it a primitive element of the group? Give reasons for your answer. [10 marks]

   (e) The Elgamal encryption scheme can be viewed as an extension to the Diffie-Hellman Key Exchange (DHKE) protocol. Describe in detail the shortened two-way Elgamal protocol. Encrypt the message ($x = 26$) with the Elgamal encryption protocol given the parameters $p = 29$ and $\alpha = 2$, $k_{pr} = d = 12$ and $i = 5$. [16 marks]