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 2018**
Year 3 Annual Examinations

Advanced Telecommunications

Wednesday 2nd May 2018 **RDS Main Hall** **14:00 – 16:00**

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 instructed to do so by the invigilator.

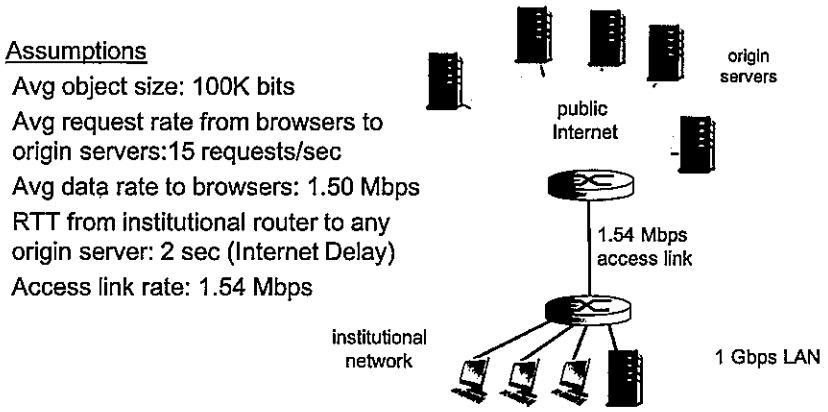
Exam paper is not to be removed from the venue.

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) What is the role of a "web proxy" in a large institutional network? What are the main advantages of installing a proxy server? [4 marks]

(b) Given the network and associated assumptions in the figure below, calculate:



- The LAN Utilization
- Access Link Utilization
- Total Delay

Now assume that we install a web proxy server into the institutional network with a hit rate of 40%, calculate:

- Access Link Utilization
- Total Delay

[14 marks]

(c) Describe the basic server hierarchy within the domain name system (DNS). 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) 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? [8 marks]

(e) Describe in detail the main components of a X.509 certificate. Explain the "handshake" procedure used in the secure sockets layer (SSL) protocol to establish a secure tunnel between a web browser and server. [12 marks]

2. (a) List the main components of an electronic mail system and describe the functionality of each of them. Distinguish between the POP, IMAP and Webmail protocols. What do you understand by the term "stateless protocol"? Is IMAP stateless? [10 marks]

   (b) Draw the finite state machine (FSM) for the 3-way TCP handshake from both the client and server perspectives. You are required to detail the state transitions in the FSM [10 marks]

   (c) What is the "SYN Flood Attack" in TCP? Describe in detail as to how this attack can be mitigated using "SYN Cookies". [8 marks]

   (d) 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]

   (e) What is Fermat's Little Theorem and why is it useful in the context of primality testing? Show that 29 is a prime number using Fermat's theorem. In the context of primality testing Fermat's Little Theorem can produce false positives. What can be done to mitigate this problem? [10 marks]

3. (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]