



THE UNIVERSITY OF THE WEST INDIES

Semester I ☒ Semester II ☐ Supplemental/Summer School ☐

Examinations of December ☐ April/May ☐ July ☒ 2017

Originating Campus: Cave Hill ☐ Mona ☒ St. Augustine ☐ Open ☐

Mode: On Campus ☒ By Distance ☐

Course Code and Title: **COMP2190 – Net Centric Computing**

Date: **December 12, 2017**

Time: **4 pm**

Duration: **2 Hours**

Paper No: **1**

Materials required:

Answer booklet: Normal ☒ Special ☐ Not required ☐

Calculator: Programmable ☐ Non-Programmable ☒ Not required ☐
(where applicable)

Multiple Choice
answer sheets: numerical ☐ alphabetical ☐ 1-20 ☒ 1-100 ☐

Auxiliary/Other material(s): None

Instructions to Candidates: This paper has 8 page(s) and 5 questions

Candidates are reminded that the examiners shall take into account the proper use of the English Language in determining the mark for each response.

Answer all questions in Section 1 and any two (2) from Section 2.

The maximum number of marks you may earn for the entire paper is **50**. The number in [] by each question indicates the number of marks allotted to the question. Justify all your answers; full credit will be given only for properly supported answers, partial credit will be given where applicable. Some useful information is provided on the last page for your reference.

Please write legibly and keep your answers concise. Points will be deducted for correct answers that also include incorrect or irrelevant information. Good skill!

Facts to remember

- The IP header and the TCP header, each without options, are 20 bytes
- The UDP header is 8 bytes
- 1 Gbps is 10^9 bits/sec; 1 Mbps is 10^6 bits/sec
- 1 msec is 10^{-3} seconds.

NB: This paper may not be removed from the examination room.

DO NOT WRITE OR TYPE ON THE BACK OF THIS SHEET: USE ONE SIDE ONLY

INSTRUCTIONS: Each page must be signed by the First and Second Examiners, and where applicable the University and External Examiners. Completed forms should be handed to the Assistant Registrar (Examinations). Where applicable, the EXTERNAL EXAMINER is requested to sign the question paper and return it with comments, if any, (on a

Section 1**Question 1** *10 multiple choice sub-questions* [10]

OVER...

DO NOT WRITE OR TYPE ON THE BACK OF THIS SHEET: USE ONE SIDE ONLY

INSTRUCTIONS: Each page must be signed by the First and Second Examiners, and where applicable the University and External Examiners. Completed forms should be handed to the Assistant Registrar (Examinations). Where applicable, the EXTERNAL EXAMINER is requested to sign the question paper and return it with comments, if any, (on a

Question 2 [20]

- a. Why do protocols such as HTTP, FTP, and SMTP run on top of TCP rather than on UDP? What is meant by a handshaking protocol? [4]
- b. Host A and B are communicating over a TCP connection, and Host B has already received from A all bytes up through byte 511. Suppose Host A then sends two segments to Host B back-to-back. The first and second segments contain 200 and 1000 bytes of data, respectively. In the first segment, the sequence number is 512, the source port number is 8020, and the destination port number is 80. Host B sends an acknowledgment whenever it receives a segment from Host A. If the second segment arrives before the first segment, in the acknowledgment of the first arriving segment what is the acknowledgment number, the source port number, and the destination port number? [3]
- c. A forwarding table for a router in a network using CIDR is given below.

Address/mask	Next hop
64.28.128.0/20	Interface 0
64.28.135.0/24	Interface 1
192.65.160.0/21	Interface 2
192.171.120.0/21	Interface 3
196.2.0.0/23	Interface 4
196.3.0.0/21	Interface 5
198.58.0.0/23	Interface 6
198.58.0.0/24	Interface 7
198.58.1.0/24	Interface 8
0.0.0.0/0	Interface 9

State the next hop for the following destination addresses:

- (i) 198.58.0.2 [3]
- (ii) 64.28.134.100
- (iii) 196.3.8.128
- d. What do we mean when we say that MAC addresses are flat? What is the benefit of having a flat addressing scheme? [3]
- e. Can a stateless firewall block TCP connection initiation requests from an external location to any local host, but at the same time allow returning traffic from connections initiated by local hosts? Why or why not? [3]
- f. (i) What is the difference between marking an element with the CSS "display:none;" and marking the element "visibility:hidden;" ? [2]
- (ii) Explain the difference between a CSS position of fixed and absolute. [2]

OVER...

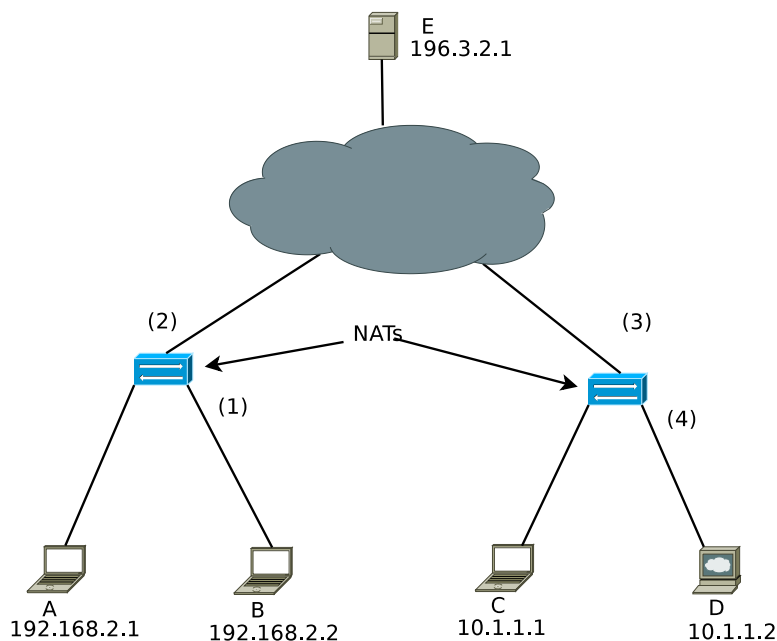
DO NOT WRITE OR TYPE ON THE BACK OF THIS SHEET: USE ONE SIDE ONLY

INSTRUCTIONS: Each page must be signed by the First and Second Examiners, and where applicable the University and External Examiners. Completed forms should be handed to the Assistant Registrar (Examinations). Where applicable, the EXTERNAL EXAMINER is requested to sign the question paper and return it with comments if any. (—)

Section 2

Question 3 [10]

Consider the scenario in the following figure, in which two residential LANs with routers that implement NAT are connected to a remote server with a public IP address.



- a. The following packet header diagrams are for a packet from the left-hand network going to the server. The first shows the header when the packet arrives at the NAT box, and the second shows it when the packet leaves the NAT box.

192.168.2.1	196.3.2.1	7312	443
207.204.252.169	196.3.2.1	5666	443
src IP	dst IP	src port	dst port

What is the public IP address of the left-hand NAT box?

[2]

OVER...

- b. The following packet header diagrams are for a packet from the right-hand network going to a host in the left-hand network.

10.1.1.2		8051	3712
64.28.128.184		6789	3712
64.28.128.184	192.168.2.2	6789	22

What is the address contained in the blank boxes above? What is the public IP address of the right-hand NAT box? [2]

- c. In the diagrams below fill in the header fields that would be used by a response to the packet in part b (the response goes from the left-hand network to the right). Hint: These header values would correspond to points (1), (2) and (4) in the figure.

You may use any valid port number.

[6]

Question 4 [10]

- a. In an RSA system, the public key of a given user is $e = 11$, $n = 1147$. What is the private key of this user? Use the Extended Euclidean algorithm, and show all of your work. [6]
- b. Suppose that Bob and Alice have access to a public key system that makes their public keys available to each other. Each knows its own private key.
- Suppose Bob has a document, m , that he wants to digitally sign. Give an overview of how he should go about doing so. Note: Efficiency is not a concern here, any digital signature technique is fine. [2]
 - What does Alice do to verify Bob's digital signature? [2]

OVER...

DO NOT WRITE OR TYPE ON THE BACK OF THIS SHEET: USE ONE SIDE ONLY

INSTRUCTIONS: Each page must be signed by the First and Second Examiners, and where applicable the University and External Examiners. Completed forms should be handed to the Assistant Registrar (Examinations). Where applicable, the EXTERNAL EXAMINER is requested to sign the question and read out its with comments if any. (or)

Question 5 [10]

a) Given the following code for a form:

```
<form action="q2f.php" method="post">
  <?php
    session_start();
    $hid_val = md5(session_id());
  ?>
  <fieldset>
    Discipline <input type="text" name="crsDisc"> <br />
    Code <input type="text" name="crsCode"> <br />
    Title <input type="text" name="crsTitle"> <br />
    Hours <input type="text" name="crsCrds"> <br />
    <input type="hidden" name="auth" value="<?= $hid_val ?>" /><br />
    <input type="submit" />
  </fieldset>
</form>
```

Complete the following blocks of code to insert the values from the form into the **Courses** table in the **CourseMgmtDB**. The **Courses** table contains the following columns: Discipline, Code, Title, and Hours. [5]

```
$db = new PDO("mysql:dbname=CourseMgmtDB;host=ar.cs.uwimona.edu.jm;
              port=22231","appMgrSA" , "test");
$db->setAttribute(PDO::ATTR_ERRMODE , PDO::ERRMODE_EXCEPTION);

if ($_SERVER['REQUEST_METHOD'] == "POST") {
    handle_post($db);
}

function handle_post($db) {
    $cDisc =  ;
    $cCode =  ;
    $cTitle =  ;
    $cHours =  ;

    $cDisc = $db->quote($cDisc);
    $cCode = $db->quote($cCode);
    $cTitle = $db->quote($cTitle);
    $cHours = $db->quote($cHours);

    $db->query(  );
}
```

b) Write a PHP function to ensure that the value of the hidden form element posted to the server matches the md5 hash of the session_id. [4]

c) Write the SQL statement to get all courses from the **Courses** table. [1]

OVER...

DO NOT WRITE OR TYPE ON THE BACK OF THIS SHEET: USE ONE SIDE ONLY

INSTRUCTIONS: Each page must be signed by the First and Second Examiners, and where applicable the University and External Examiners. Completed forms should be handed to the Assistant Registrar (Examinations). Where applicable, the EXTERNAL EXAMINER is requested to sign the question and answer sheet with signature if any. (one

Useful Information

Algorithm 1 Extended_Euclidean(m, n)

```

( $A_1, A_2, A_3$ )  $\leftarrow$  ( $1, 0, m$ )
( $B_1, B_2, B_3$ )  $\leftarrow$  ( $0, 1, n$ )
while true do
  if  $B_3 == 0$  then
    return  $A_3$  {//No inverse}
  end if
  if  $B_3 == 1$  then
    return  $B_2$  {// $B_2 \equiv n^{-1} \pmod{m}$ }
  end if
   $Q \leftarrow \left\lfloor \frac{A_3}{B_3} \right\rfloor$ 
  ( $T_1, T_2, T_3$ )  $\leftarrow$  ( $A_1 - Q \times B_1, A_2 - Q \times B_2, A_3 - Q \times B_3$ )
  ( $A_1, A_2, A_3$ )  $\leftarrow$  ( $B_1, B_2, B_3$ )
  ( $B_1, B_2, B_3$ )  $\leftarrow$  ( $T_1, T_2, T_3$ )
end while

```

END

DO NOT WRITE OR TYPE ON THE BACK OF THIS SHEET: USE ONE SIDE ONLY

INSTRUCTIONS: Each page must be signed by the First and Second Examiners, and where applicable the University and External Examiners. Completed forms should be handed to the Assistant Registrar (Examinations). Where applicable the EXTERNAL EXAMINER is requested to sign the question and answer sheet with signature if any (name).