CANDIDATE: please attach Student Support Unit sticker, if relevant

G6077

THE UNIVERSITY OF SUSSEX

INFORMATICS

BSc FINAL YEAR EXAMINATION 2021
MComp THIRD YEAR EXAMINATION 2021

January 2021 (A1)

Introduction to Computer Security

Candidates should answer TWO questions out of THREE. If all three questions are attempted only the first two answers will be marked.

Each question is worth 50 marks.

Write your answers on A4 paper, scan and save as a single PDF file and upload to Canvas

PDF file name: candidate number_module title

Read Academic Integrity Statement

You are reminded that, unless you have been authorised to do so in School or specific assessment guidance, you should not access online materials, notes etc. during this examination or discuss this assessment with others before the end of its 24 hour window. By submitting this assessment you confirm that you have read the above Statement and are responsible for understanding and complying with our academic misconduct regulations (found on Student Hub and here: Academic Misconduct regulations).

1.

a) Consider the following SQL statement and answer the questions listed below.

```
$conn= new mysqli("localhost", "root", "rootUser",
     "Record");          // $conn holds connection to the Record DB.
     $sqlQuery = "SELECT * FROM student
       WHERE studentID = '$studentID' AND
          PIN =  '$PIN'";
```

i) A malicious user wants to delete the database. What values should the malicious user provide for the `$studentID` and `$PIN` to carry out the attack? What does the malicious user needs to assume about the database and why?

ii) Provide reasons why the SQL statement is vulnerable and modify the code to avoid manipulation.

[26 marks]

b) Use the RSA algorithm and the following values to answer the questions listed below. Values are: n = 2419, p=59 and e = 7. You only need to show equations with the given values, you don't need to do calculations.

i) Find the q value;

ii) Show the equation of decryption and encryption for the given values;

iii) Encrypt the message 26;

iv) Sign the message 100.

[10 marks]

c) Suppose the fictional company *BrightonTravels* store their users' passwords as hashes. For login, a programmer wants to hash passwords at the client side rather than at the server. Do you think it is a good idea or not? Explain your view.

[14 marks]

2.

a) Describe how the Diffie Hellman Key Exchange protocol allows for the generation of a shared key. What are the possible attacks on such a protocol?

Assume that Alice and Bob have a common primitive q=23 and a primitive root α=5.

i) If Alice has public key Y_A=10, show the process and derive the value of Alice's private key X_A.

ii) If Bob has the public key Y_B = 8, what is the value of the shared secret key K?

[30 marks]

b) Alice wants to use AES to send emails to Bob. Which AES encryption mode would be appropriate and how will this ensure confidentiality and integrity of the emails?

[20 marks]

3.

a) Suppose Bobby and Alice are registered users in `freeTime`, a social application. Alice refused to add Bobby as a friend. Bobby wants to develop an attack so that he can be added to Alice' friends list without her consent. Bobby added Charlie and noted the following URL was used in the call to add a friend:

```
http://www.freeTime.com/friends/add?friend=42
```

i) Why did Bobby add Charlie first?
ii) What information can Bobby get from the URL?
iii) What else does Bobby need for the attack to happen?
iv) How an anti-CSRF token can avoid this attack?
v) What is Same Origin Policy and how it will help in avoiding this attack?

[30 marks]

b) John has arranged a blind date for Kelly and Brendan. They are both cryptographers and they didn't know each other before. John has given Kelly and Brendan a secret number K and no one else knows K. Brendan wants to make sure that the person he is dating is actually Kelly, not somebody else. Explain how cryptographically Kelly can prove herself without revealing the secret number K.

[10 marks]

c) Charles is a junior software developer who wants to learn public-key cryptosystems to apply it in an e-commerce web application. Before applying it in his project, what are the general requirements of public-key cryptosystems that he should be aware of?

[10 marks]

End of paper