北京郵電大學

Queen Mary University of London

For examiners' use only

1	
2	
3	
4	
Total	

EBU714U A

Joint Programme Examinations 2018/19

EBU714U Security and Authentication

Paper A

Time allowed 2 hours

Answer ALL questions

Complete the information below about yourself very carefully.

QM student number										
BUPT student number										
Class number										

NOT allowed: electronic calculators and electronic dictionaries.

INSTRUCTIONS

1. **You must NOT take answer books, used or unused, from the examination room.**
2. Write only with a black or blue pen **and in English**.
3. Do all rough work in the answer book – **do not tear out any pages**.
4. If you use Supplementary Answer Books, tie them to the end of this book.
5. Write clearly and legibly.
6. **Read the instructions on the inside cover.**

Examiners

Dr Yasir Alfadhl, Dr Na Yao

Copyright © Beijing University of Posts and Telecommunications & © Queen Mary University of London 2018

Instructions

Before the start of the examination

1) Place your BUPT and QM student cards on the corner of your desk so that your picture is visible.

2) Put all bags, coats and other belongings at the back/front of the room. All small items in your pockets, including wallets, mobile phones and other electronic devices must be **placed in your bag in advance**. **Possession of mobile phones, electronic devices and unauthorised materials is an offence.**

3) Please ensure your mobile phone is switched off and that no alarm will sound during the exam. **A mobile phone causing a disruption is also an assessment offence.**

4) Do not turn over your question paper or begin writing until told to do.

During the examination

1) You must not communicate with or copy from another student.

2) If you require any assistance or wish to leave the examination room for any reason, please raise your hand to attract the attention of the invigilator.

3) If you finish the examination early you may leave, but not in the first 30 minutes or the last 10 minutes.

4) For 2 hour examinations you may **not** leave temporarily.

5) For examinations longer than 2 hours you **may** leave temporarily but not in the first 2 hours or the last 30 minutes.

At the end of the examination

1) You must stop writing immediately – **if you continue writing after being told to stop, that is an assessment offence.**

2) Remain in your seat until you are told you may leave.

Question 1

a) Advanced Encryption Standard (AES) was established a few decades following the Data Encryption Standard (DES). Fill in the table below with the appropriate answers which respond to each method.

	DES	**AES**
Stream or Block cipher?		
Plaintext block size		
Key size		
Number of rounds		
		/ 8 marks

b) An S-box is also used AES as part of the 'substitute byte' operation. Explain what it is, and how it is used. **[6 marks]**

	Do not write in this column
	6 marks

c) If the same 64-bit block of plaintext appears more than once in a message, it always produces the same ciphertext. In order to avoid such security weakness, DES can be deployed in different modes of operations. Briefly describe the purpose of such modes of operations and provide a detailed analysis of the encryption/decryption processes in the Cipher Block Chaining (CBC) Mode. What's the error propagation for CBC? (Use diagrams to support your answer) **[11 marks]**

	Do not write in this column
	11 marks

Question marking: $\frac{\quad}{8} + \frac{\quad}{6} + \frac{\quad}{11} = \frac{\quad}{25}$

Question 2

a) What is the difference between ***symmetric*** *encryption* and ***asymmetric*** *encryption*? Give an example of each type of encryption methods. **[4 marks]**

	Do not write in this column
	4 marks

b) User *A* and *B* decide to use the *Diffie-Hellman* key exchange technique with a common prime q=11 and a primitive root α=2 to establish a unique secret key. Assume that *A*'s random number is 9 and *B*'s number is 4. Answer the following questions: **[10 marks]**

(i) Demonstrate the procedure of key establishment step-by-step. What's the secret key?

(ii) Is the secret key established in (i) practical? Explain your answer.

	Do not write in this column
	10 marks

c) Using your knowledge of RSA, answer the following: **[6 marks]**

(i) Explain what RSA is in terms of the number of keys used, and the way in which data is processed.

(ii) Use mathematical functions to describe both encryption and decryption processes.

(iii) List two security mechanisms RSA can be used in.

	Do not write in this column
	6 marks

d) Briefly explain *message authentication code (MAC)* and *one-way hash function*. Which security service do they both provide? **[5 marks]**

	Do not write in this column
	5 marks

Question marking: $\frac{}{4} + \frac{}{10} + \frac{}{6} + \frac{}{5} = \frac{}{25}$

Question 3

a) In Internet Protocol Security (IPSec), what is the domain of interpretation (DOI)? **[5 marks]**

	Do not write in this column
	5 marks

b) Briefly explain how the Tunnel and Transport Modes operate in IPSec. **[4 marks]**

	Do not write in this column
	4 marks

c) Kerberos is an authentication service designed for use in a distributed environment. Kerberos services are required to be secure, reliable, transparent, and scalable. What mechanisms are used within Kerberos to achieve these requirements? **[8 marks]**

Requirement	**Mechanism**
Secure	
Reliable	
Transparent	
Scalable	
	/ 8 marks

d) In Firewalls, what is a circuit-level gateway? Support your answer with a diagram. **[8 marks]**

	Do not write in this column
	8 marks

Question marking: $\frac{}{5} + \frac{}{4} + \frac{}{8} + \frac{}{8} = \frac{}{25}$

Question 4

a) Define the following two important Secure Sockets Layer (SSL) concepts: **[4 marks]**

i) SSL connection (2 marks)

ii) SSL session (2 marks)

	Do not write in this column
	4 marks

b) Explain the **purposes** of *handshake protocol* and *record protocol* in SSL/TLS, and the **tasks** performed by the two protocols. **[8 marks]**

	Do not write in this column

	8 marks

c) How many encryptions keys are used/generated in PGP? Explain how PGP manages the encryption keys. **[7 marks]**

	Do not write in this column
	7 marks

d) List three different types of malicious software and briefly explain each one. **[6 marks]**

	Do not write in this column
	6 marks

Question marking: $\frac{}{4} + \frac{}{7} + \frac{}{8} + \frac{}{6} = \frac{}{25}$

Do not write in this column

2018-2019

Rough Working

Page 12 of 14

Do not write in this column

2018-2019

Rough Working

Page 13 of 14

Do not write in this column

2018-2019

Rough Working

Page 14 of 14