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 2017/18

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										

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, Dr Yuanwei Liu

Filename: 1718_EBU714U_A No answer book required

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) Within the context of security requirements, define **integrity** and **authentication.** For each of the two requirements, list two security mechanisms that can achieve it. **[6 marks]**

Security requirement	Meaning	Security Mechanism
Integrity		
Authentication		
		6 marks

b) Answer the questions below about *AES:* **[8 marks]**

i) AES is a block cipher. What is a block cipher? (2 marks)

ii) AES uses techniques of substitution and permutation during the operation. Briefly define the terms substitution and permutation. (4 marks)

iii) What is the purpose of the key expansion algorithm used in AES? (2 marks)

	Do not write in this column

	8 marks

c) DES is a block-cipher and its basic mode of operation is Electronic Code Book (ECB). In this mode of operation, 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 a security weakness, DES can be deployed in different modes of operation such as the Cipher Block Chaining (CBC) mode. Briefly explain how CBC mode works with the help of a diagram. What's the error propagation of CBC if one block of ciphertext is corrupted during transmission? **[11 marks]**

	Do not write in this column

	11 marks

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

Question 2

a) Using your knowledge of RSA public key encryption, answer the following: **[12 marks]**

(i) Use mathematical functions to describe both encryption and decryption processes. (6 marks)

(ii) Explain how RSA can be used in 'digital signatures' and in 'data confidentiality'. (4 marks)

(iii) Traditionally, session keys (conventional encryption) are used together with public keys to achieve data confidentiality. Briefly explain why is it more effective to use such a combination to encrypt large volume of data. (2 marks)

	Do not write in this column

12 marks

b) Using your knowledge of message authentication methods, answer the following: **[13 marks]**

i) What is the difference between a Message Authentication Code (MAC) and a one-way hash function? (4 marks)

ii) What changes are required to replace a HMAC with an underlying hash function? (3 marks)

iii) Explain what is the birthday attack (hash attack)? (6 marks)

	Do not write in this column

	13 marks

Question marking: $\frac{\quad}{12} + \frac{\quad}{13} = \frac{\quad}{25}$

Question 3

a) A simple way for a server to authenticate a client is to ask for a password. In Kerberos this authentication is not used, why? How does Kerberos authenticate the server and the clients?

[6 marks]

	Do not write in this column
	6 marks

b) Kerberos services are required to be secure, reliable, transparent, and scalable. What mechanisms are used within Kerberos systems to achieve these requirements? **[4 marks]**

Requirement	Mechanism
Secure	
Reliable	
Transparent	
Scalable	
	4 marks

c) Based on your knowledge in IPSec, answer the following: **[15 marks]**

i) Briefly explain what is meant by IPSec, and why it is important? (3 marks)

ii) List the two IPSec modes of operation. Explain how one can achieve protection against traffic analysis using either mode. (4 marks)

iii) List four of the parameters used to characterise the nature of a particular Security Associate (SA). (4 marks)

iv) In IPSec, what are the specific key exchange algorithms in ISAKMP? What are the roles of the Oakley key determination protocol and ISAKMP? (4 marks)

	Do not write in this column

	15 marks

Question marking: $\frac{}{6}+\frac{}{4}+\frac{}{15}=\frac{}{25}$

Question 4

a) Within the context of Secure Socket Layers, answer the following sections: **[9 marks]**

i) Explain the meaning of the terms 'SSL connection' and 'SSL session'. (4 marks)

ii) What protocols are included in SSL architecture? Support your answer with a diagram. (5 marks)

	Do not write in this column
	9 marks

b) 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

c) In PGP key management, there is a possibility of multiple public keys per user, therefore the recipient of the message needs to know which of his/her public keys was used for encryption. Explain how PGP identifies the public key. **[4 marks]**

	Do not write in this column
	4 marks

d) Explain the Certificates Processing of S/MIME. **[5 marks]**

	Do not write in this column
	5 marks

Question marking: $\frac{}{9} + \frac{}{7} + \frac{}{4} + \frac{}{5} = \frac{}{25}$

Do not write in this column

2017-2018

Rough Working

Page 16 of 18

Do not write in this column

2017-2018

Rough Working

Page 17 of 18

Do not write in this column

2017-2018

Rough Working

Page 18 of 18