Not for circulation

THE UNIVERSITY OF HONG KONG

FACULTY OF ENGINEERING
DEPARTMENT OF COMPUTER SCIENCE

COMP3355: Cyber Security

Date: 20 December 2019 Time: 2:30pm – 4:30pm

This paper has a total of 100 marks.

Please download this Examination Question and Answer Book in MS Word file format from HKU Moodle or at this URL: http://www.cs.hku.hk/~chow/c3355/2019ans.rar
Password to extract the Answer Book is: BX$!c(8@qXr%eB#/

Answer ALL questions. Write SHORT AND SUCCINCT answers in the spaces provided on the examination paper. The space provided for each question should be more than sufficient to accommodate your answer.

Only approved calculators as announced by the Examinations Secretary can be used in this examination. It is candidates' responsibility to ensure their calculator operates satisfactorily, and candidates must record the brand and model of the calculator after the University Number in their answer script.

You must stop working on the examination answer at the end of the examination. Then submit your answer in one single file in either MS Word, PDF or ZIP to the Online Exam (OLEX) system before the submission end time. Submission via other channels and/or late submission is not accepted.

CANDIDATE'S UNIVERSITY NO.: _____

	MARKS
QUESTION 1 (30)	
QUESTION 2 (20)	
QUESTION 3 (25)	
QUESTION 4 (25)	
TOTAL (100)	

QUESTION 1. (30 Marks)

Short questions. Give a short answer to each of the following question.

(a) If the key length of the RSA key of the personal certificate is 1024, what should be the key length of the CA certificate? When is the length of the key when AES is used? (4 marks)

	Key length
CA certificate RSA key	
AES key	

(b) What is the principle behind CAPTCHA? (4 marks)

(c) Can the usage of SSL protect against the Man-in-the-Browser attack? Explain your answer. (4 marks)

(d) What are the 2 basic operations in symmetric key encryption? What is the purpose of each basic operation? (4 marks)

	Name of operation	Purpose of operation
Operation 1		
Operation 2		

(e) HTTP servers listen to port no. 40 and HTTPS servers listen to port no. 443. An enterprise allows employees inside the corporate network to connect to the Gmail server (gmail.com) on the Internet using HTTPS. Email clients are not allowed to connect to the Gmail server. Following are common port numbers that are used in email:

i. Port 110 - this is the default POP3 non-encrypted port
ii. Port 995 - this is the port you need to use if you want to connect using POP3 securely
iii. Port 143 - this is the default IMAP non-encrypted port
iv. Port 993 - this is the port you need to use if you want to connect using IMAP securely
v. Port 25 - this is the default SMTP non-encrypted port
vi. Port 465 - this is the port used, if you want to send messages using SMTP securely

Define **minimal** set of firewall rules in the following table. Assume there are only 2 possible actions: Allow and Deny. (4 marks)

Rule	Direction	Type	Source IP	Dest. IP	Source Port	Dest. Port	Action
1							
2							

(f) Consider the following ACLs for files e6031.doc, e6031.exe, project.doc, e6031exam.doc and e6031ans.doc. You can assume there is no ACL for files not in the following list. (10 marks)

File	**Allow/Deny**	**SID**	**Permission**
e6031.doc	AccessAllowed	Chow	Read, Write
	AccessAllowed	TA	Read, Write
e6031.exe	NO ACLS		
project.doc	AccessAllowed	Chow	Read, Write
	AccessAllowed	TA	Read, Write
	AccessAllowed	Student	Read
e6031exam.doc	AccessAllowed	Chow	Read, Write
	AccessAllowed	TA	Read
e6031ans.doc	NO ACLS		

Determine if the following file access is allowed or not.

SID	**File**	**Action**	**Access successful or fail**
Chow	e6031.doc	Write	Successful
Vivien	e6031.doc	Write	
Chow	e6031.exe	Read	
Vivien	e6031.exe	Read	
Student	project.doc	Read	
TA	project.doc	Write	
Vivien	project.doc	Read	
Chow	e6031exam.doc	Write	
Chow	e6031ans.doc	Write	
Student	e6031ans.doc	Read	
Vivien	e6031ans.doc	Read	

QUESTION 2. (20 Marks)

Consider company A and company B signed a contract C using digital signature. Both A and B obtain their public key certficates (PKCs) from Certification Authority Hong Kong Post (HKP). All PKCs are signed by an Intermediate CA and the Intermediate CA is signed by the root CA HKP. Assume A signs the contract C on date D1 and B signs the contract C on date D2. Both digital signatures are attached to the contract C.

The process can be summarized as follow:

1. A digitally signs the contract C using A's private key on D1;
2. A sends his digital signature and his PKC together with the contract C to B;
3. B receives A's digital signature and A's PKC together with the contract C from A;
4. B verifies A's digital signature using A's PKC with respect to the contract C. B then signs the contract C using B's private key on D2;
5. B sends his digital signature and his PKC together with A's signature and the contract C back to A;
6. A receives B's digital signature and B's PKC together with his own signature and the contract C.
7. A then checks the received contract C is identifical to the contract he sent to B in step 2.

(a) Besides the verification steps 7 above, describe 8 other checkings to be carried out by A when he receives documents from B in step 6. (16 marks)

	Process	**To be checked using**
	Checks the received contract C is identifical to the contract A sent to B in step 2	Comparing the hash values of the received contract C and the contract A sent to B in step 2
1		
2		

3		
4		
5		
6		

(b) In steps 2 and 5, both A and B sent their PKCs to the other party. Can the receiving party trusted the PKC sent from another party? Why? (4 marks)

QUESTION 3. (25 Marks)

You are a cryptanalyst for an agency. You were told that 2 targets (A and B) were communicating using public key encryption RSA. You were able to obtain the public key of A, which is (1613, 1073). You then intercepted a message sent from B to A, which was 176. Describe how you can decrypt the message step by step. Show all your steps in details. (Insert additional page(s) when needed.)

Step	**Details**	**Result of calculation**
1		

QUESTION 4. (25 Marks)

An airline company launches a mobile Apps, MyFlight, for its customers. For each customer, MyFlight uses the customer's email address as the user ID and the HKID no. or his passport no. as the password. When a user logs on to MyFlight with his email address and his password (HKID no. or passport no.), MyFlight will send the user ID and the hashed password (using SHA1) to the server for authentication. The communication between MyFlight and the server is not encrypted.

(a) If an attacker is able to capture the communication between MyFlight and the server, can the attacker guess the password? Explain your answer. (8 marks)

(b) Assume the attacker is only interested in user ID that the password is the HKID no. and the HKID no. is of the format `X999999(9)`, where `X` is any letter between 'A' and 'Z' and `9` is any digit between '0' and '9'. The last digit (the digit enclosed inside brackets), called check digit, can be calculated from the first letter together with the other 6 digits. Assume the time required to calculate the SHA1 value for one HKID no. is *x* milliseconds and the time required to calculate the check digit is insignificant, estimate the **average** time required to find the HKID no. corresponding to a SHA1 value capture over the communication. (9 marks)

In order to prevent replay attack from hackers, the web server will generate a Session ID for each client's session. The Session ID is generated by appending a random number after SHA1 value of the client's IP address.

(c) Is the proposed approach to generate the Session ID secure? If no, exaplain how the hacker can steal the client's personal information? (8 marks)

*** END OF PAPER ***