THE UNIVERSITY OF HONG KONG

Department of Computer Science

COMP 3355 Cyber security

Date: 5 November 2019 Time: 1:30 pm – 3:00 pm

Answer **ALL** questions. Write **SHORT AND SUCCINCT** answers in the spaces provided.

This paper has a total of 100 marks.

CANDIDATE'S UNIVERSITY NO.: ______________________________

	MARKS
QUESTION 1 (20)	
QUESTION 2 (25)	
QUESTION 3 (20)	
QUESTION 4 (15)	
QUESTION 5 (20)	
TOTAL (100)	

QUESTION 1. (20 Marks)

Multiple choice questions. (2 marks for each question. Put your answers in the following table.)

(1)	E
(2)	ABD
(3)	E
(4)	DE
(5)	C
(6)	ABCDE
(7)	BDE
(8)	A
(9)	CD
(10)	ABCD

1. Which of the following is/are NOT collect?

A. Encryption is a process of encoding a message so that the meaning of the message is not obvious, decryption is the processing of transforming an encrypted message back into its normal form.

B. The weakness of monoalphabetic ciphers is the frequency distribution reflects the distribution of the underlying alphabet.

C. Index of coincidence can measure how often character could theoretically appear next to each other, based on the frequency analysis of the text. It is a measure of the variation between frequencies in a distribution.

D. Kasiski method is used to determine when a pattern of encrypting permutations has repeated to predict the number of alphabets used for substitutions.

E. None of the above.

2. Which of the following is/are collect? (Choose all that apply)

A. A transposition, also called permutation, is an encryption in which the letters of the messages are rearranged.
B. RSA does not support confusion and diffusion.
C. DES does not support confusion and diffusion.
D. Good diffusion means that the attacker needs access to many ciphertexts in order to infer the algorithm.
E. The substitution ciphers provides good diffusion.

3. In the Internet model(TCP/IP model), the most important task of the Internet layer is routing which is based on ____-byte IP address(IPv4) splitting into ___-bit network ID and ____-bit host ID.

A. 4, 24, 8

B. 4, 16, 16

C. 6, 16, 32

D. 6, 32, 16

E. 4, 8, 24

4. Which of the following is/are NOT symmetric key encryption? (Choose all that apply)

A. AES

B. DES

C. RC4

D. RSA

E. SHA-256

5. Using the square & multiple exponentiation algorithm to calculate m^{10100} mod p, how many multiply operations are needed?

A. 5

B. 6

C. 7

D. 8

E. 9

6. Which of the following about certificate is/are collect? (Choose all that apply)

A. A certificate has a life time.

B. A certificate contains start date/time and expiration date/time.

C. Expired certificate are only used to verify signature on an old document.

D. A new certificate should be issued to the subscriber when his/her old certificate is expired.

E. In event of suspected key compromise, a new certificate should be issued, and the old certificate should be “revoked” prior to its expiry date.

7. When checking the digital signature, we need to do ( )? (Choose all that apply)

A. Verify the digital signature with signer’s private key in signer’s PKC

B. Verify the digital signature with signer’s public key in signer’s PKC.

C. Verify signer’s PKC using CA’s private key in the root cert.

D. Verify signer’s PKC using CA’s public key in the root cert.

E. Confirm the signer’s PKC is not yet expired.

8. Which of the following about Certificate Revocation List (CRL) is/are NOT correct?

A. CRL will contain certificates that are expired.

B. CRLs are digitally signed, thus can be sent via unprotected channels.

C. CRLs are distributed regularly, e.g. hourly, daily, etc.

D. Each revoked cert is identified by a certificate serial number.

E. CRL is a time-stamped list of revoked certs, digitally signed by the CA, available to all users.

9. Which of the following is/are correct? (Choose all that apply)

A. SSL VPNs can support all IP-based services.

B. IPsec VPNs are best for Web-enabled applications, file sharing and emails.

C. Gateways are usually implemented on the perimeter firewall in IPsec VPN.

D. Gateways are typically deployed behind the perimeter firewall in SSL VPN.

E. The accessibility of SSL is formal access with controlled user base.

10. Which of the following component(s) do(es) Unified Threat Management (UTM) contain? (Choose all that apply)

A. Network address translation

B. Anti-virus

C. Content filtering by proxy server

D. URL filtering

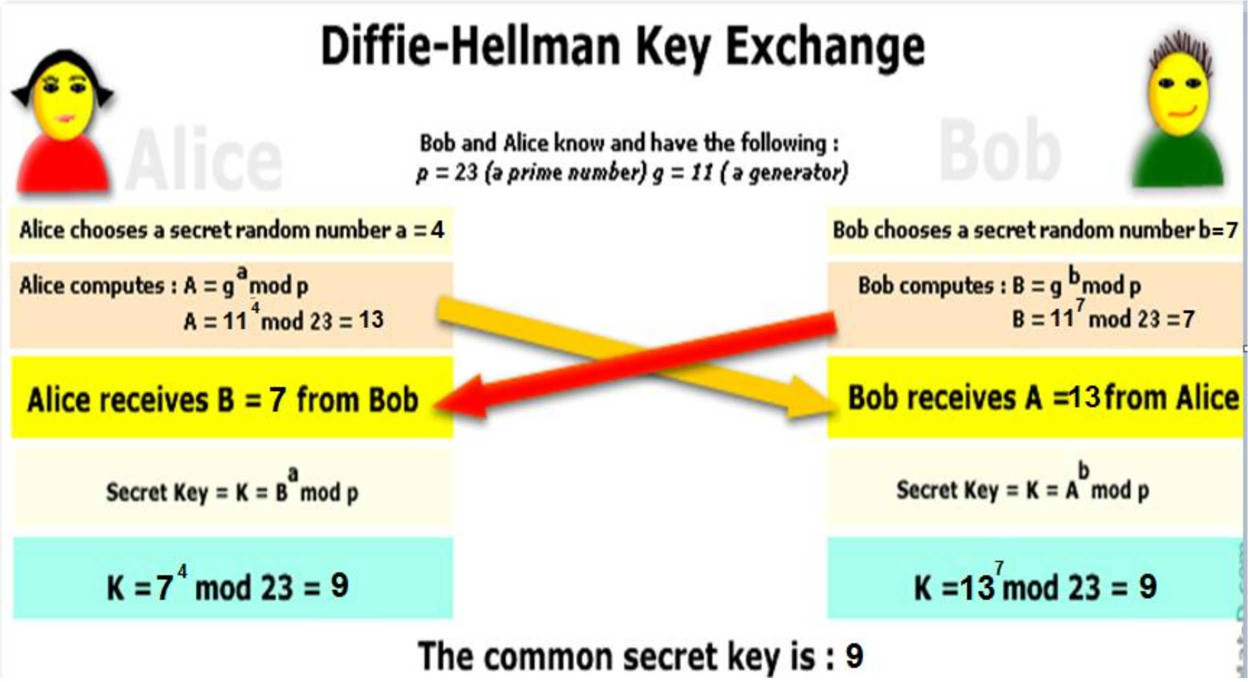
E. None of the above

QUESTION 2. (25 Marks)

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

(a) Consider the Diffle-Hellman key exchange scheme between Alice and Bob. Assuming the public known information is *p* (23) and *g* (11), Alice's private key is *a* (4) and Bob's public key is *b* (7). Describe how Alice and Bob exchange information to generate a shared secret key *s*. What is *s*? (10 Marks)

Ans:



Diffie-Hellman Key Exchange

Bob and Alice know and have the following :
$p = 23$ (a prime number) $g = 11$ (a generator)

Alice chooses a secret random number a = 4

Alice computes : $A = g^{a} \bmod p$
$A = 11^{4} \bmod 23 = 13$

Alice receives B = 7 from Bob

Secret Key = $K = B^{a} \bmod p$

$K = 7^{4} \bmod 23 = 9$

Bob chooses a secret random number b=7

Bob computes : $B = g^{b} \bmod p$
$B = 11^{7} \bmod 23 = 7$

Bob receives A =13 from Alice

Secret Key = $K = A^{b} \bmod p$

$K = 13^{7} \bmod 23 = 9$

The common secret key is : 9

s = 9

(b) Give one reason why SSL is better than IPsec when users are sales and marketing staffs. Give one reason why IPsec is better than SSL when users are IT technical staffs. (10 Marks)

Ans:

	SSL	**IPsec**
Applications	Web-enabled applications, file sharing and emails	All IP-based services
Encryption	Strong but vary	Strong and consistent

Authentication	One or two way authentication	Strong: two way authentication
Users	Sales, marketing, …	HR, finance, IT staff, ...
Accessibility	Casual access	Formal access with controlled user base
Complexity	Moderate	High
Easy of use	Very high	Moderate
Scalability	High	High

One reason why SSL is better than IPsec when users are sales and marketing staffs:

SSL is easier to use, less complex and more casual to access than IPsec.

One reason why IPsec is better than SSL when users are IT technical staffs:

IPsec has stronger authentication, more formal accessibility with controlled user base and higher complexity than SSL.

(c) In RSA generation, we need to generate 2 large prime numbers *p* and *q*. Probabilistic algorithm is used to test if the generated number is prime or not. Explain why probabilistic algorithm is used instead of deterministic algorithm. (5 Marks)

Ans:

For a large number that is 2000 bits long, i.e. >= 2^{1999} and <= 2^{2000}, there is about 1 prime in every 1386 numbers. The deterministic algorithm is very slow to check the numbers one by one. The probabilistic approach is quicker which repeatedly running the same test and reduce the probability of error to an acceptable level.

QUESTION 3. (20 Marks)

Consider an attacker has intercepted an encrypted message “16” from Alice to Bob which was encrypted using RSA public key cryptographic system. It was found that Alice’s public key was (11, 15), Bob’s public key was (7, 33).

(a) Describe how the attacker can decrypt the message. (8 Marks)
Ans:

The cipher text (*c* = 16) was sent from Alice to Bob and encrypted by RSA public key cryptographic system. It means Alice encrypted the plain text (*m*) with Bob’s public key (e, n) and sent c = m^e mod n = 16. In order to decrypt the message, the attacker should try to get Bob’s private key (d, n). Then the attacker can decrypt the cipher text and get the original message m = c^d mod n.

(b) What is the original message after the attacker apply the steps in (a). Show details of your calculation. (4 Marks)
Ans:

First, the attacker try to get Bob’s private key:

Since p, q = 3, 11 and GCD (7, 20) = 1, 7^{-1} mod 20 exists. 7^{-1} mod 20 = 3. So Bob’s private key is (3, 33).

Then, according to RSA public key cryptographic system: m = c^d md n = 16^3 mod 33 = 4.

(c) If Alice wants to sign message “3” to Bob by RSA public key cryptographic system, what will Bob receive? (8 Marks)

Ans:

If Alice wants to sign the message m = 3 to Bob by RSA public key cryptographic system, she will use her private key (d, n) to sign the message and send s = m^d mod n to Bob.

Since p, q = 3, 5 and GCD (11, 8) = 1, 11^{-1} mod 8 exists. 11^{-1} mod 8 = 3. So Alice’s private key is (3, 15).

Bob will receive s = 3^3 mod 15 = 12.

QUESTION 4. (15 Marks)

Considering the Chief Security Officer (CSO) of a company who plan to implement the following intrusion detection rule when a user failed to provide the correct password when he/she tried to login to the company server:

- If the number of the times that a user fails to provide the correct password is greater than or equals to X, an alert message saying that "potential intruder fails to login to company server because too many attempts." will be generated and the message will be send to the Chief Security Officer.

The CSO has measured the number of login attempts by users in the past 3 months and found that the average number of times to login successfully is 1.7 and the standard deviation is 0.5.

Estimate the number X such that the probability of the alert message corresponds to a real intruder is >= 0.99.

Ans:

$X>=1.7+3*0.5=3.2$

number X should be 4

QUESTION 5. (20 Marks)

Consider a company has a mail server supports both IMAP and POP3 mail protocols for mail client connection, and allows mail client to send email using SMTP protocol. Generally speaking, SMTP is used for email delivering. While, IMAP and POP3 are used for retrieving email from a mail server, the main difference between POP3 and IMAP is: POP3 protocol downloads emails to the local client PC, but IMAP protocol always stores emails in the mail server. Following are common port numbers that are used in the POP3 and IMAP protocols:

1. Port 110 - this is the default POP3 non-encrypted port
2. Port 995 - this is the port you need to use if you want to connect using POP3 securely
3. Port 143 - this is the default IMAP non-encrypted port
4. Port 993 - this is the port you need to use if you want to connect using IMAP securely
5. Port 25 - this is the default SMTP non-encrypted port
6. Port 465 - this is the port used, if you want to send messages using SMTP securely

The mail server is behind the company's firewall with IP address 125.14.6.5.

In the company's intranet, employees can access the mail server with insecure connection. The company also allows employees to access the mail server from home but requires secure connection from the mail client to the mail server. Define the necessary firewall rules in the following table.

Rule	Direction	Type	Source IP	Dest. IP	Source Port	Dest. Port	Action
1							
2							
3							
	Any	Any	*.*.*.*	*.*.*.*	Any	Any	Deny

Ans:

Rule	Direction	Type	Source IP	Dest. IP	Source Port	Dest. Port	Action
1	Inbound	TCP/IMAP	external	internal	>=1024	993	Permit
2	Inbound	TCP/IMAP	internal	external	993	>=1024	Permit
3	Inbound	TCP/POP3	external	internal	>=1024	995	Permit
4	Inbound	TCP/POP3	internal	external	995	>=1024	Permit
5	Inbound	TCP/SMTP	external	internal	>=1024	465	Permit
6	Inbound	TCP/SMTP	internal	external	465	>=1024	Permit
7	Inbound	SMTP	internal	internal	25	>=1024	Permit
8	Inbound	SMTP	internal	internal	>=1024	25	Permit
	Any	Any	*.*.*.*	*.*.*.*	Any	Any	Deny