KOLEJ UNIVERSITI TUNKU ABDUL RAHMAN

FACULTY OF COMPUTING AND INFORMATION TECHNOLOGY

ACADEMIC YEAR 2021/2022

OCTOBER EXAMINATION

INFORMATION TECHNOLOGY BAIT1093
INTRODUCTION TO COMPUTER SECURITY

FRIDAY, 1 OCTOBER 2021 TIME: 9.00 AM – 12.00 NOON (3 HOURS)

BACHELOR OF COMPUTER SCIENCE (HONOURS) IN SOFTWARE ENGINEERING

BACHELOR OF INFORMATION SYSTEMS (HONOURS) IN ENTERPRISE INFORMATION SYSTEMS

BACHELOR OF INFORMATION TECHNOLOGY (HONOURS) IN SOFTWARE SYSTEMS DEVELOPMENT

Instructions to Candidates:

Answer **ALL** questions in the requested format or template provided.

- This is an open book final online assessment. You MUST answer the assessment questions on your own without any assistance from other persons.
- You must submit your answers within the following time frame allowed for this online assessment:
  - The deadline for the submission of your answers is **half an hour** from the end time of this online assessment.
- Penalty as below **WILL BE IMPOSED** on students who submit their answers late as follows:
  - The final marks of this online assessment will be reduced by 10 marks for answer scripts that are submitted within 30 minutes after the deadline for the submission of answers for this online assessment.
  - The final marks of this online assessment will be downgraded to zero (0) mark for any answer scripts that are submitted after one hour from the end time of this online assessment.
- Extenuation Mitigating Circumstance (EMC) encountered, if any, must be submitted to the Faculty/Branch/Centre within 48 hours after the date of this online assessment. All EMC applications must be supported with valid reasons and evidence. The UC EMC Guidelines apply.

FOCS Additional Instructions to Candidates:

- Include your **FULL NAME**, **STUDENT ID** and **PROGRAMME OF STUDY** in your submission of answer.
- Read all the questions carefully and understand what you are being asked to answer.
- Marks are awarded for your own (original) analysis. Therefore, use the time and information to build well-constructed answers.

BAIT1093 INTRODUCTION TO COMPUTER SECURITY

STUDENT'S DECLARATION OF ORIGINALITY

By submitting this online assessment, I declare that this submitted work is free from all forms of plagiarism and for all intents and purposes is my own properly derived work. I understand that I have to bear the consequences if I fail to do so.

Final Online Assessment Submission
Course Code:
Course Title:
Signature:
Name of Student:
Student ID:
Date:

BAIT1093 INTRODUCTION TO COMPUTER SECURITY

Question 1

RSA and Diffie-Hellman are the most widely used public-key encryption algorithms. A number of commercial products have adopted these two public key algorithms for many years.

a) (i) With example, describe how the public key and private key are generated. (8 marks)

Chapter 4 slide 21

(ii) Based on RSA algorithm, describe **THREE (3)** requirements must to be fulfilled to perform the process of encryption and decryption with suitable example. (8 marks)

Chapter 4 slide 22

b) Consider a Diffie-Hellman scheme with a common prime q = 23 and a primitive root α= 5. Use the Diffie-Hellman Key Exchange Algorithm, as shown in Figure 1.

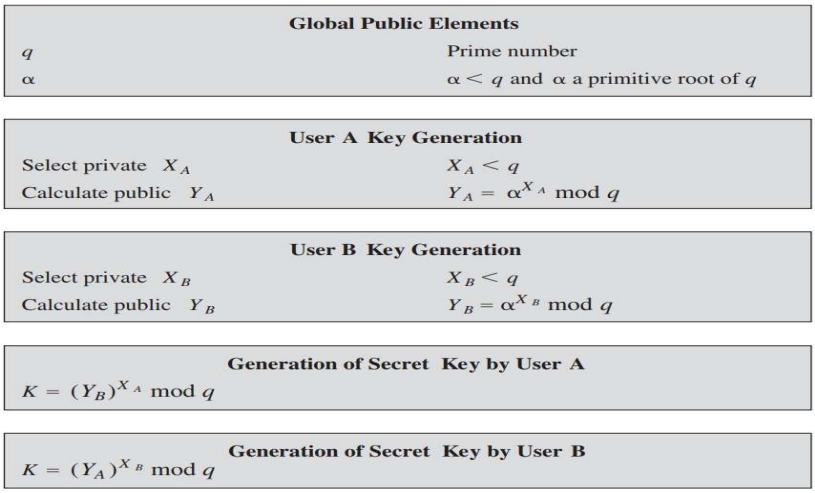

Figure 1: The Diffie-Hellman Key Exchange Algorithm

(i) If user A has public key $Y_A = 10$, what is A's private key X_A? (3 marks)

(ii) If user B has public key $Y_B = 8$, what is the shared secret key K? *[Note: MUST find X_B value to prove shared key]* (6 marks)

K=6

[Total: 25 marks]

Question 2

a) Advanced Encryption Standard (AES) is a block cipher. The AES use cryptographic keys to encrypt and decrypt data. AES does not use a Feistel structure but processes the entire data block in parallel during each round using substitutions and permutation.

diagram

(i) By using own words, describe substitutions and permutation with appropriate example. (4 marks)

Substitution can be defined as each of the element in the plain text will be replaced by another letter, number or symbol

Permutation can be defined as the order/position for each of the the element in the plain text is rearranged.

Question 2 a) (Continued)

(ii) Given following matrix, perform substitute byte transformation and shift row transformation. *Note: Refer Table1: AES S-Box.* (10 marks)

$$\begin{bmatrix} 09 & 36 & 40 & 82 \\ 6A & A5 & 7C & 9B \\ D5 & 38 & E3 & 2F \\ 30 & BF & 39 & FF \end{bmatrix}$$

		y															
		0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
x	0	63	7C	77	7B	F2	6B	6F	C5	30	01	67	2B	FE	D7	AB	76
	1	CA	82	C9	7D	FA	59	47	F0	AD	D4	A2	AF	9C	A4	72	C0
	2	B7	FD	93	26	36	3F	F7	CC	34	A5	E5	F1	71	D8	31	15
	3	04	C7	23	C3	18	96	05	9A	07	12	80	E2	EB	27	B2	75
	4	09	83	2C	1A	1B	6E	5A	A0	52	3B	D6	B3	29	E3	2F	84
	5	53	D1	00	ED	20	FC	BI	5B	6A	CB	BE	39	4A	4C	58	CF
	6	D0	EF	AA	FB	43	4D	33	85	45	F9	02	7F	50	3C	9F	A8
	7	51	A3	40	8F	92	9D	38	F5	BC	B6	DA	21	10	FF	F3	D2
	8	CD	0C	13	EC	5F	97	44	17	C4	A7	7E	3D	64	5D	19	73
	9	60	81	4F	DC	22	2A	90	88	46	EE	B8	14	DE	5E	0B	DB
	A	E0	32	3A	0A	49	06	24	5C	C2	D3	AC	62	91	95	E4	79
	B	E7	C8	37	6D	8D	D5	4E	A9	6C	56	F4	EA	65	7A	AE	08
	C	BA	78	25	2E	1C	A6	B4	C6	E8	DD	74	1F	4B	BD	8B	8A
	D	70	3E	B5	66	48	03	F6	0E	61	35	57	B9	86	C1	1D	9E
	E	E1	F8	98	11	69	D9	8E	94	9B	1E	87	E9	CE	55	28	DF
	F	8C	A1	89	0D	BF	E6	42	68	41	99	2D	0F	B0	54	BB	16

Table1: AES S-Box

b) List **TWO (2)** types of symmetric encryption techniques used. (1 mark)

block cipher and stream cipher

c) Companies depend on information systems to support its daily business operations. It is important for companies to protect information systems at all times. One important security aspect is physical security. The role of physical security is to protect the physical assets that support the storage and processing of information.

(i) State and describe **THREE (3)** categories of physical threats caused by humans. (6 marks)

unauthorized physical access, theft of equipment/data, vandalism of equipment's/data, misuse of resource

(ii) Specify the difference between infrastructure security and premises security? (4 marks)

[Total: 25 marks]

Infrastructure security aims to protect physical assets such as personnel who operate the system and data.

Question 3

a) Explain the suitability or unsuitability of the following passwords: (3 marks)

(i) Florida Not suitable because a password should have at least 8 characters with at least 3 combinations from symbol, uppercase letter, lowercase letter, numeral or Unicode character.

(ii) *laptop_admin# Suitable because the password length is greater than 8 characters with the combination of symbol and letter

b) Access control policy which can be embodied in an authorization database, dictates what types of access are permitted, under what circumstances and by whom. Access control policies are generally grouped into 4 categories. One of the categories is Discretionary Access Control (DAC).

(i) By using own words, Describe DAC. owner control the file access. (2 marks)

(ii) Alice owns File 1 and File 3, Bob owns File 2 and Christopher owns File 4. Each owner of the file(s) has the authorization to assign access rights of one subject to one resource (also known as object) where Alice allows Bob to read File 1 and write File 3 and meanwhile allows Christopher to read and write File 1. Bob only allows Christopher to read File 2 and whereas Christopher allows bob to read File 4 only. You are required to formulate an access matrix indicates the access rights of a particular subject for a particular object based on each owners' authorization requirements for their file(s). (6 marks)

(iii) Draw directed graphs that corresponds to the access matrix which was created in Question 3 b) (ii). The directed graphs show access control lists and capability lists for files as specified in the authorization requirements. (9 marks)

c) With suitable example, describe the usage of IPsec. (5 marks)

application of IPsec

[Total: 25 marks]

Question 4

a) Under security risk assessment, there are four main approaches which are being implemented to identify and mitigate risks to an organization's IT infrastructure.

(i) State all the **FOUR (4)** risk assessment approaches. (4 marks)
baseline approach, informal approach, detailed risk analysis & combined approach

(ii) State **FOUR (4)** specifications that determine which one is the suitable risk assessment approach that can be implemented to an organization (8 marks)

The resource available to the organization, initial high level analysis how valuable the IT systems, how critical to the organization's business objectives, legal and regulatory (slide 14)

b) Follow-up phase is an important phase in IT security management. There are four elements of follow-up phase. One of the elements is Change and Configuration management.

(i) Specify the other **THREE (3)** elements from the follow-up phase of IT security management. (3 marks)
- Maintenance of security controls
- Security compliance checking
- Incident handling

Question 4 b) (Continued)

(ii) State **TWO (2)** reasons why it is so important to implement the follow-up phase and specify **FOUR (4)** processes need to be carried out by the IT security management to reduce the chance of security breach. (10 marks)

[Total: 25 marks]

Maintenance, Security compliance, Change and configuration management & incident handling