KAPASA MAKASA UNIVERSITY

SCHOOL OF APPLIED SCIENCE AND OPEN LEARNING

DEPARTMENT OF INFORMATION AND COMMUNICATION TECHNOLOGY

BARCHELOR OF SCIENCE IN CYBER SECURITY

CYS 121 - INFORMATION SYSTEMS SECURITY

SESSIONAL EXAMINATIONS

Date: 5th November,2024. **Time: 3 hours**

Total Marks: 100

Instructions to Candidates:

There are three (3) sections in this paper.

- SECTION A: Answer all questions in this section. 10 Marks
- SECTION B: Answer all questions in this section. 30 Marks
- SECTION C: Answer question 1 and choose any two 60 Marks

Write your student Identification Number on the Answer Booklet provided.
Calculators are allowed.

SECTION A [10 MARKS]

1. A program designed to destroy data on your computer which can travel to "infect" other computers is called a _?

A. Disease
B. Torpedo
C. Hurricane
D. Virus

2. Software such as viruses, worms and trojan horses that has malicious intent is known as .....

A. Spyware
B. Adware
C. Spam
D. Malware

3. An act to injure, corrupt or threaten a system or network is characterized as which of the listed below?

A. Digital crime
B. Threats
C. System hijacking
D. Cyber-attack.

4. Which of the following statements best describes how the principle would be broken if a computer was no longer accessible?

A. Confidentiality
B. Access control
C. Availability
D. Denial

5. Which of the following is a method of hiding information inside a picture?

A. Image rendering
B. Steganography
C. Rootkits
D. Bitmapping

6. They are malicious hackers whose primary goal is to commit cybercrimes to make money. Who are they in this context?

A. White Hat hackers
B. Black Hat hackers
C. Hacktivists
D. Gray Hat hackers

7. What is changed when cypher algorithms are used?

A. Scalar text
B. Plain text
C. Complex text
D. Cipher text

8. A person who uses his or her expertise to gain access to other people's computers to get information illegally or do damage is called a?
A. Hacker
B. Analyst
C. Spammer
D. Programmer.

9. A _____ can be a hardware device or software program that filters all the packets of data that comes through a network, the internet etc.
A. Firewall
B. Antivirus
C. Malware
D. Cookies

10. The process of encoding data to protect it from unauthorized access is known as ____?
A. Encryption
B. Firewall
C. Intrusion detection
D. Multi-factor authentication.

SECTION B [30 MARKS]

Answer all questions in this section.

1. Write short notes on the following types of attacks;
   i. Denial-of-service attacks (DoS) [4 marks]
   ii. Spoofing [4 marks]
   iii. Man In middle attack [4 marks]
   iv. Sniffing [4 marks]
   v. Masquerading [4 marks]

2. With the help of diagrams explain what Denial of service Attack (DoS) and Distributed Denial of Service Attack (DDoS) is. [10 marks]

SECTION C [60 MARKS]

Answer three (3) questions from this section. Question 1 is a compulsory question

1. Explain the difference between viruses, worms, Trojan horses, and ransomware. How do they operate and differ in their spread? [20 marks]

2. What are **zero-day** exploits and how do they pose a unique challenge for cybersecurity professionals? Discuss mitigation strategies. [20 marks]

3. Discuss the CIA triad in relation to cyber security. Use relevant examples in your explanation. [20 marks]

4. Encrypt "**freedom has come** "using the substitution technique method of Caesar Cipher, use the key = 3. Show all the steps of your working. [20 marks]

SCHOOL OF APPLIED SCIENCE AND OPEN LEARNING

DEPARTMENT OF INFORMATION AND COMMUNICATION TECHNOLOGY

BACHELOR OF CYBER SECURITY

COMMUNICATION SKILLS
CYS 122

SESSIONAL EXAMINATION

DATE: 25-Oct-24 TIME: 09.00 - 12.00 HRS, 3 HOURS

Instructions to candidates

1. Write your **Name** and **Student ID** on the **Answer Sheet** provided
2. There are **Seven (7) questions** in this paper. Attempt any **five (5).** Indicate on the Answer sheet your choice from the optional questions.
3. Write your Answers on the answer Sheet provided.
4. No Foreign material will be allowed in this examination.
5. The number of marks is shown in brackets [ ] at the end of each question or part question.
6. Clear handwriting and neat work is encouraged.
7. Incorrect spellings and wrong grammar will result in loss of marks.
8. The total number of marks for this paper is **100**

DO NOT TURN THIS PAGE UNTIL YOU ARE TOLD TO DO SO.

QUESTION ONE (1): INTRODUCTION TO COMMUNICATION SKILLS AND PROTOCOL

(a) With the help of a communication model (diagram), outline the Communication Process. (10 marks)

(b) Discuss some consequences of poor Communication and Protocol Breaches in Cybersecurity or any other field. (10 marks)

QUESTION TWO (2): VERBAL AND NON VERBAL COMMUNICATION AND COMMUNICATION IN LEADERSHIP

(a) Suggest oral (verbal) ways of preventing and resolving conflicts in the work- place. (10 marks).
(b) Explain some cultural differences that may be encountered during non-verbal Communication (10 marks).

QUESTION THREE (3): WRITTEN COMMUNICATION

As Chairperson of the Cybersecurity Society at Kapasa Makasa University, you attended a workshop which was reviewing the Zambia Cybersecurity and Cyber Crimes Act Number 2 of 2021.

You took down the following points:

- The Zambia Cybersecurity and Crimes Act seeks to:

- Provide for cybersecurity in Zambia
- Ensure protection of persons against Cybercrimes, including online child protection
- Facilitate the identification, declaration and protection of critical information infrastructure
- Promote the responsible use of social media Platforms
- Foster the creation of a secure, reliable and trustworthy cyber environment that increases confidence.

Using the points above and any of your own, write a report to the Head of Department for I. C.T. about the purpose of the Zambia Cybersecurity and Cyber Crimes Act of 2021.

Remember to include a recommendation. (20 marks)

QUESTION FOUR (4): SPECIALISED (BUSINESS) COMMUNICATION SKILLS

(a) Write a letter addressed to the Chief Executive Officer of ABSA Bank Headquarters in Lusaka on P.O. Box 500163, applying for the advertised vacant post of Cybersecurity Specialist.

Briefly state your age, education background, qualifications, experience, hobbies and referees. (10 marks)

(c) Enclose your one paged Curriculum Vitae (CV). (10 marks)

QUESTION 5: PROTOCOL, ETIQUETTE AND DIGITAL COMMUNICATION NETIQUETTE

With appropriate examples, distinguish between etiquette and netiquette. (20 marks)

QUESTION SIX (6): SPECIALISED VERBAL COMMUNICATION

(a) State any five (5) things you would do to adequately prepare for an oral job interview, and write five (5) points about how you would conduct yourself during the oral interview for a Cybersecurity Specialist at ZAMTEL. (10 marks)

(b) With appropriate examples, propose workable strategies you would use to effectively handle crisis Communication at your institution or place of work. (10 marks)

QUESTION SEVEN (7: WRITTEN COMMUNICATION

With at least one example on each agenda item, formulate the layout of meeting minutes from the title to the adjournment of the meeting. (20 marks)

THE END!

KAPASA MAKASA UNIVERSITY

ICT DEPARTMENT

CYS 120 FINAL EXAMS

21ST OCTOBER, 2024

TIME 14:00 – 17:00HRS

INSTRUCTIONS

Do not turn this page until you are told to do so

This Question paper contains 6 Questions

Attempt a total of 4 questions.

Question 1 is compulsory and carries 40 Marks.

Question 2 – 6 Carries 20 Marks each

Write your answers clearly

Time allowed is **3 hours** only

Only calculators are allowed in the Exam room.

[QUESTION 1]

As network Engineer for NET Consultancy Limited, you have been hired by the Bank of Zambia to carry out a network design and implementation. Apart from the Ndola and Lusaka offices, BOZ has also opened a new office in Livingstone which will have 1008 hosts while the Lusaka and Ndola branches will have 420 and 250 hosts respectively using **172.16.0.0/16**

i. Use VLSM to subnet the internetwork showing clearly the network addresses, the valid hosts and broadcast addresses for each subnet assuming three WAN links connect the three offices. **[20 Marks]**

ii. If the branch managers want to have virtual private networks for their weekly meeting, how many SAs should be created? Justify your answer. **[5 Marks]**

iii. Clearly explain how the Router between Lusaka and Livingstone converts the "original IPv4 datagram" into an IPsec datagram. **[5 Marks]**

iv. Explain the four stages of the 802.11i framework stating how separating the authentication server from the AP allows one authentication server to serve many Aps in a wireless network. Use diagrams where appropriate. **[10 Marks]**

[QUESTION 2]

A. Mention and describe any two cyber-attacks following under each of the following categories **[8]**

I. Social engineering attacks
II. Malware attacks
III. Active Attacks
IV. Passive Attacks

B. A packet segment has amongst other things the SYN field and source IP address Field. At what layer do you find the network element that processes the packet? Explain your answer. **[3]**

C. Explain any two draw backs of symmetric-key system despite being easy and faster compared to asymmetric-key system. **[4]**

D. List the steps that are taken in order to come up with the public and private key in RSA. **[5]**

[Total 20 Marks]

[QUESTION 3]

A. What attacks are avoided by the following methods and how? **[4]**

I. Nonce (OTP)
II. Sequence Number

B. Explain how the following attacks can be avoided. **[5]**

I. Tampering attack
II. Truncation attack

C. Use a table to give any three comparisons between PGP and a S/MIME **[3]**

D. The Client named Alice and Server called Bob want to use Diffie-Helman Key Exchange to exchange a symmetric key that they are going to use to share information over the public communication Channel. If they have selected the prime modular p of 7.

I. Select the generator g that will result in a common shared key of the form g mod p **[2]**

II. Show how you can use the shared key g mod n to come up with final secrete symmetric key that will be used to encrypt the message. Show your calculations clearly. [6]

[**Total 20 Marks**]

[QUESTION 4]

A. Explain why Bob and Alice might sometimes choose to use a MAC over a Digital signature to carry out authentication. [3]

B. Alice intends to send a message **m** to Bob but wants to make sure that the message has **integrity** and is both **authenticated** and **confidential** before sending it. Explain how would achieve the following using appropriate diagrams. [12]

I. Message Integrity
II. Authentication
III. Confidentiality
IV. Non-Repudiation

C. Before sending the message **Haris Beats Trump,** you are required to use a check sum algorithm and hash the message to get a message digest. What would be hash message? You might need to use ASCII to help you with your calculations. [5]

[QUESTION 5]

A. What is the function of a fire wall in a network security? Hence list and explain the three goals of a fire wall. [5]

B. Firewalls can be classified in three primary categories. List and explain each one of them. [6]

C. Explain the importance of having an Intrusion Detection System in a Network and how they can be classified. [3]

D. Kalebwangu is an online business that students at Kapasa Makasa use to buy commodities they want and can be brought to their do stops. Highlight how SSL (TLS version 3) can be used to prevent Trudy from playing any Man in the middle attack. [6]

[QUESTION 6]

A. Clearly give the differences between the following terminologies used in network security [10]

I. Message Digest and Message Authentication Code (MAC)
II. Packet analysis and Packet Sniffing
III. Message Authentication and End Point Authentication
IV. A switch and a Router
V. TCP and UDP

B. A virus attacks a single user's computer and within one hour embeds itself in 80 e-mail attachment files sent out to other users. By the end of the hour, 10% of these have been opened and have infected their host machines. If this process continues, how many machines will be infected at the end of 5 hours? Can you find a formula for the number of machines infected after n hours? [5]

C. Why do we need network security? [2]

D. List the function(S) of each of the following three of the seven layers of the OSI model [3]

I. Transport Layer
II. Network Layer
III. Data Link Layer

SCHOOL OF APPLIED SCIENCE AND OPEN LEARNING

DEPARTMENT OF INFORMATION AND COMMUNICATION TECHNOLOGY

BACHELOR OF CYBER SECURITY

SECURE SOFTWARE ENGINEERING
CYS 111

SESSIONAL EXAMINATION

DATE: 31-Oct-24 TIME: 14.00 - 17.00 HRS. 3 HOURS

Instructions to candidates

1. Write your **Name** and **Student ID** on the **Answer Sheet** provided
2. There are **Six (6) questions** in this paper. Attempt only any **five (5).**
3. Write your Answers on the answer Sheet provided.
4. No Foreign material will be allowed in this examination.
5. The number of marks is shown in brackets [ ] at the end of each question or part question.
6. Clear handwriting and neat work is encouraged.
7. The total number of marks for this paper is **100**

DO NOT TURN THIS PAGE UNTIL YOU ARE TOLD TO DO SO.

QUESTION ONE

a) What do you understand the term prototyping and give two advantages and disadvantages?

5Marks

b) What is the significance of the closed system concept in software engineering?

3Marks

c) Name Four types of system Testing and why do we test systems

9Marks

d) What is the main reasons for evaluation during system maintenance?

3Marks

QUESTION TWO

a) Explain six core processes required in the development of any new application?

6 Marks

b) i. In life, a system can be ether open or closed. State what is the difference between closed and open systems give one example of each system?

4 Marks

ii. Draw well labeled diagram of Closed and Open system.

4 Marks

iii) explain any three types of information system

6 Marks

QUESTION THREE

a) As a software engineer, why is it necessary to consider the confidentiality of our clients:

6 Marks

b) Draw well labeled diagram and explain each stages of the traditional system development life cycle (waterfall model)

10 Marks

c) Name three main issues that the functional requirements report should outline:

4 Marks

QUESTION FOUR

a) Name three advantages of waterfall model?

6 Marks

b) what are the strengths, weaknesses, and limitations of using development methodologies? **6 Marks**

c) What is the significance of the closed system concept in software engineering? **4 Marks**

d) What is the difference between deterministic systems and self-organising systems? **4 Marks**

QUESTION FIVE

a) Explain why organizations initiate information system projects?

3Marks

b) You have just been employed by a company as a Software engineer and they what to embark on developing the new system and you have been asked to be part of the committee that is selecting system projects be embarked on. List and explain the main sources of information systems projects in the organizations?

7Marks

c) Explain the criteria used in organisations when selecting information system projects to invest in

7Marks

d) There are various kinds of committees that select projects. Name any three.

3 Marks

QUESTION SIX

a) What do you understand from the term 'system`s entropy'?

2Marks

b) The process framework encompasses a set of umbrella activities that are applicable across the entire software process. A generic process framework for software engineering encompasses five activities: List and explain these activities?

10Marks

c) You have been on the committee to select projects but you noted that the same project failed feasibility. State any four (4) things that can be done to projects that fail feasibility test?

4Marks

d) State any two (2) reasons why we need to apply standards when approving the feasibility study.

4Marks

END OF EXAM

KAPASA MAKASA UNIVERSITY

ICT DEPARTMENT

CYS 110 FINAL EXAM

14th OCTOBER 2024

TIME: 09:00 – 12:00 HRS

INSTRUCTIONS

Do not turn this page until you are told to do so

This Question paper contains 6 Questions, **Attempt any 4 questions including question 1.**

Question 1 is compulsory and carries 40 Marks.

Question 2 – 6 Carries 20 Marks each

Write your answers clearly

Time allowed is **3 hours** only

Only calculators are allowed in the Exam room.

[QUESTION 1]

A. In your opinion, which one is the most important goal from amongst the goals of network security? Convincingly articulate your argument. [3]

B. Using AES algorithm, encode the following hexadecimal message sent using Rinjndael Algorithm. The S-Box, Round Key, initial state array and Predefined matrix are given below. Clearly show the four steps in the first round to get the final sate array in Round one. The S-box, predefined key, initial state array and the round key are given on the last page. [37]

[Total 40 Marks]

[QUESTION 2]

A. Using the RSA encryption algorithm, pick p = 5 and q = 7. Find a set of encryption/decryption keys e and d. **The two keys should be different.** [4]

B. Using the keys that you have found encrypt the word **WORK HARD** assuming that the alphabet is between 1 and 26. [8]

C. Use the decryption key you obtained above to decrypt the cipher text **QOANXFOAWI.** [8]

[QUESTION 3]

A. The centurion who was supposed to inform you of s was killed en route, but you have received the message **VGFRVUREVCNFFBEVSNVY** in a Caesar cipher. Find the value of s and decode the message. Hint: *Use brute force* [5]

B. Your junior course mate asks you to help him decode the message **YANETICGCBETPPNAHSTHOSAARRAERHOYTINB** he has just received from their CYS 110 lecturer. Use columnar transposition cipher to decode and give him the answer using the key **QUARTZ** [5]

C. Using a Caesars cipher with S = 3 and S = 9, Encrypt the message **ACCURACY IS CARDINAL** using a C1C2C2C1C2 sequence [5]

D. The three blocks of hexadecimal numbers **24 45 37, 64 44 A1** and **3B 22 09** need to be hushed in order to get a check sum so that the information they contain maintains its integrity. Calculate the checksum using hexadecimal addition. [5]

[QUESTION 4]

A. You need to encode the message **ATTACK** using a block encoding scheme with the encoding matrix, shown below [5]

$$M = \begin{bmatrix} 3 & 2 \\ 7 & 5 \end{bmatrix} \quad M' = \begin{bmatrix} 5 & 24 \\ 19 & 3 \end{bmatrix}$$

B. Prove that M x M' = $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ [5]

C. Using the RSA encryption algorithm, let p = 3 and q =5. Then n = 15 and m = 8. Find the encryption and decryption keys. [5]

D. You receive a message **QYNKERYF** encoded with the block cipher above. Decode to get the original message. [5]

[QUESTION 5]

A. Use columnar transposition to decode the message from your lecture below
TWUSSOHHRETSIECCOESROOABIEUMCYSORELE [5]

B. You are required to encrypt the message "**All the best wishes in your Exams**" using a symmetric key k = 26. Show your work clearly. [5]

C. Convert the following base ten numbers into hexadecimal numbers, 23, 17, 28, 68, and 56. [5]

D. Shimumbi decides to encrypt his already encrypted message with his private key and send to Banamumbi. Explain why he had to do that. [5]

[QUESTION 6]

A. Using RSA, block encoding scheme and stream cipher, encode the word **NEVER DISPAIRE**. For RSA p = 5 and q = 7, for the block encoding use M' in question 4A. The key for the stream cipher keys are S = 4 and S = 6 with sequence C2C1C1C2C2. Note that the output of RSA is fed to the Block Cipher whose output is consequently fed to the stream cipher to get the final cipher text. **For RSA, private and public keys should be different**. [20]

ALL THE BEST WISHES

THE END

S-box

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
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	B1	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

Predefined Key

02	03	01	01
01	02	03	01
01	01	02	03
03	01	01	02

Initial State Array

EA	04	65	85
83	45	5D	96
56	33	98	B0
F0	2D	AD	C5

Round Key

AC	19	28	57
77	FA	D1	5C
66	DC	29	00
F3	21	41	6A