الفرقة الرابعة نصف العام ٢٠٢٢
حاسبات

Menoufia University
Faculty of Electronic Engineering
Computer Science and Eng. Dept.
Academic Year: 2022 / 2023
4th Year – 1st Semester

Final Exam
Course: Elective Course 5 (CSE416)
Exam Date: 12/1/2023
Exam Time: 10:00 AM to 01:00 PM
Exam Code: FECV22

Answer the following questions: **Total marks [70]**

First question (Choose the correct answer): [50 marks]

Calculator is allowed.

Note: Fill in the table shown on **Page 9** with the correct answers to the first and second questions.

1. **Which of the following corresponds to labelling each pixel according to the object it belongs to:**
   (a) Image classification.
   (b) Semantic segmentation.
   (c) Object detection.
   (d) Optical Flow.
2. **Which of the following is true for Eigenfaces (PCA)**
   (a) Is invariant to geometric transforms.
   (b) Is invariant to shadows.
   (c) Can be used to effectively detect deformable objects.
   (d) Can be used for lossy image compression.
3. **…………………. learns a function to classify arbitrary 3D points as inside / outside the shape.**
   (a) Point cloud.
   (b) Implicit surface.
   (c) Volumetric.
   (d) RGB-D image.
4. **Which of the following is considered a generative approach to handle classification problems:**
   (a) Principal Component Analysis.
   (b) Adaboost.
   (c) Support Vector Machines.
   (d) (c) and (b).
5. **Data pre-processing include the following …………… .**
   (a) centring.
   (b) whitening.
   (c) standardizing.
   (d) All of the above.
6. **A robust binary classifier is tested on an image of a novel category, the values of the output probability vector should be ………….. .**

(a) [0.0, 1.0]
(b) [0.5, 0.5]
(c) [1.0, 0.0]
(d) [1.0, 1.0]

7. **Object detection can be considered a .... problem.**

(a) classification
(b) regression
(c) classification and regression
(d) None of the above

8. **The discriminative technique focuses on .... to handle the classification task.**

(a) learning decision boundaries
(b) building a model for each class
(c) class scalability
(d) None of the above

9. **When applying a Hough transform, noise can be countered by .... :**

(a) decreasing the threshold on the number of votes a valid model has to obtain.
(b) considering only a random subset of the points since these might be inliers.
(c) a finer discretization of the accumulator.
(d) increasing the threshold on the number of votes a valid model has to obtain.

10. **Which of the following can be considered a machine learning problem:**

(a) Computing the factorial of non-negative integer numbers.
(b) Diagnosing new human disease that has not shown yet.
(c) Recommending new movies based on the interest of a Netflix subscriber.
(d) None of the above.

11. **Suppose we are using a Hough transform to do line fitting, but we notice that our system is detecting two lines where there is actually one in some example image. Which of the following is most likely to alleviate this problem?**

(a) Make the image larger.
(b) Sharpen the image.
(c) Increase the size of the bins in the Hough transform.
(d) Decrease the size of the bins in the Hough transform.

12. **The purpose of PCA algorithm is the following ....**

(a) Visualization
(b) Noise removal
(c) Regression
(d) All of them

13. **Which of the following is considered a variant of semantic segmentation:**

(a) Pose estimation.
(b) Panoptic segmentation.

(c) Semantic image synthesis.

(d) (a) and (b)

14. .... is the ability to easily generate realistic random image.

(a) Image classification

(b) Semantic segmentation

(c) Image synthesis

(d) Pose estimation

15. Which of the following is true about Transformers on images:

(a) Require large amount of annotated data compared to CNNs.

(b) Their fundamental component is self-attention.

(c) Are faster than RNNs in training and inference.

(d) All of them.

16. The pixel dimension of depth image is ....

(a) 1

(b) 2

(c) 3

(d) 4

17. When U-Net is trained on images, the expected output type is ....

(a) category label.

(b) image.

(c) Float number.

(d) text.

18. .... is sensitive to outliers.

(a) Least square fit

(b) RANSAC

(c) Hough transform

(d) (b) and (c)

19. Which of the following is considered a mid-level vision:

(a) Panorama Stitching.

(b) Image Adjustments.

(c) Edge detection.

(d) All of the above.

20. Which of the following is considered distance metric:

(a) Cross-entropy measure.

(b) Euclidean measure.

(c) Mahalanobis measure.

(d) (b) and (c).

21. .... is considered as an unsupervised learning loss function.

(a) Cross-entropy

(b) Triplet loss

(c) L2 loss
(d) All of the above

22. Which of the following is considered a single-stage object detector network:

(a) YOLO.
(b) Fast R-CNN.
(c) Faster R-CNN.
(d) U-Net.

23. NMS algorithm is used for ………… .

(a) proposing a number of plausible rectangular regions.
(b) removing weaker detections that have too much overlap with stronger detections.
(c) classifying each detection while also producing a confidence score.
(d) Measuring the accuracy of each bounding box.

24. ……………… is about logic planning and proving, such as forming beliefs, making decisions.

(a) Cognition
(b) Perception
(c) Machine learning
(d) Hough transform

25. …………… find likely images based on keywords.

(a) Visual similarity search
(b) Instance retrieval
(c) Image search
(d) Instance recognition

<u>Second question (True (T) or False (F))</u>: [8 marks]

1. Hough transform is computationally efficient. ( )
2. PCA is a linear unsupervised machine learning algorithm. ( )
3. VAE consists of a discriminator and generator networks to synthesize images.( )
4. Automatic medical diagnosis usually relies on symmetric cost evaluation of the classification model. ( )
5. K-nearest neighbors can be used for both classification and regression. ( )
6. Generative approach is suitable for handling scalable classification problems.( )
7. In feature-based recognition, it is preferable to get the interest points (keypoints) that lie on edges. ( )
8. In computer vision, we can rely on physics and probabilistic models to overcome the missing information. ( )

Third question: [12 marks]

1. Explain the main properties of keypoint descriptors.

2. What are the properties that computer vision algorithms should satisfy?

3. Given a collection of 3 images $\{\mathbf{x}^{(1)}, \mathbf{x}^{(2)}, \ \mathbf{x}^{(3)}\}$ in $\mathbb{R}^2$, where

$$\mathbf{x}^{(1)} = \begin{bmatrix} 1.0 \\ 1.2 \end{bmatrix} \qquad \mathbf{x}^{(2)} = \begin{bmatrix} 2.0 \\ 1.8 \end{bmatrix} \qquad \mathbf{x}^{(3)} = \begin{bmatrix} 3.0 \\ 3.0 \end{bmatrix}$$

The eigen values and eigen vectors of the estimated covariance of the given data are the following:

$$\lambda_1 = 0.017, \ \ \lambda_2 = 1.82 \quad \boldsymbol{v}_1 = \begin{bmatrix} 0.7 \\ -0.71 \end{bmatrix}, \ \boldsymbol{v}_2 = \begin{bmatrix} -0.7 \\ -0.7 \end{bmatrix}$$

Answer the following:

a) Calculate the data mean

b) Let's suppose the encoding function $f\left(\mathbf{x}^{(i)}\right) = z^{(i)}$ is used to project each data sample onto a line that best fits the given data using PCA algorithm, calculate the values of $\boldsymbol{z}^{(3)}$

c) Calculate the reconstructed image $\tilde{\mathbf{x}}^{(3)}$

d) Calculate **DIFS₃**

e) Calculate **DFFS₃**

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

....

Answer to the first question:

1.	
2.	
3.	
4.	
5.	
6.	
7.	
8.	
9.	
10.	
11.	
12.	
13.	

14.	
15.	
16.	
17.	
18.	
19.	
20.	
21.	
22.	
23.	
24.	
25.	

Answer to the second question (Write '**T**' for True and '**F**' for False)***:***

1.	
2.	
3.	
4.	
5.	
6.	
7.	
8.	

حاسبات الفرقة الرابعة نصف العام ٢٠٢٢

University	: *Menoufia*		*Date*	:	*5 /01/2023*
Faculty	: *Electronic Engineering*		*Time*	:	*3 Hours*
Department	: *Computer Science&Eng.*		*No. of pages*	:	*2*
Academic level	: *4th Year*		*Full Mark*	:	*70 Marks*
Course Name	: *Distributed Systems*		*Exam*	:	*Final Exam*
Course Code	: *: CSE 468*	جـامعـة المنوفيـة	*Examiner*	:	*Assoc. Prof: Nirmeen A. El-Bahnasawy*

Answer the following questions:

Question No. 1 : (30 Marks)

a) What are the four benefits of using cloud computing?

b) Explain different models for deployment in cloud computing?

c) State the difference between allocation problem and scheduling problem.

d) Give only three IoT – ENVIRONMENTAL MONITORING applications.

e) State the Fog Computing Architecture?

f) Give a block diagram explains How IoT model works

Question No 2: (20 Marks)

a) Give the Gantt chart of a schedule for the sample task graph of Figure 1 on three homogeneous processors. Calculate speedup and efficiency parameters.

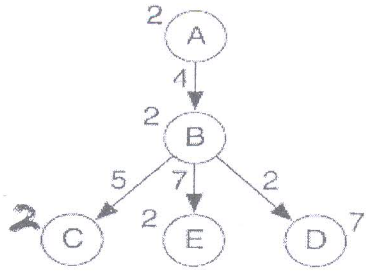


Fig. 1

b) Program for x = a ∗ 7 + (a ∗ 5 + 2) As a DAG and get Gantt chart onto 2 processors. Take unit of time is unity and no communication cost.

Question No 3 : (10 Marks)

State is the main concept of the following topics:

1. First Come First Serve algorithm.

2. **Max-min algorithm.**
3. **Virtualization.**
4. **Challenges of big data in cloud computing.**
5. **IoT – Disadvantages.**

Question No 4 :

Choose the correct answer: **(10 Marks)**

1. Tasks carry out independently. This refers to (concurrency – no global clock)?
2. Interfaces should allow components to be added or replaced. (Openness – scalability)?
3. Protection against disclosure to unauthorized individual. (Confidentiality – integrity)?
4. Enables local and remote resources to be accessed using identical operations. (Concurrency transparency - Access transparency)?
5. It is closer proximity to small end users, its wider consumer reach, and better mobility. Refers to (Edge computing – Fog computing)?
6. Communication delay between two tasks allocated to the same processors is (negligible – idle time)?
7. Systems enhanced data collection (IoT – Foggy)?
8. The extension or lowering of cloud computing capabilities to the bottom/edge of the network in order to provide faster ICT (communication, storage, software, etc.) services to the lower end users.(edge computing – fog computing)?
9. Is being one of the characteristic provide the concept of commissioning and decommissioning of large amount of resource capacity dynamically. (Scalability – elasticity)?
10. Service provides cloud applications which are used by the user directly without installing anything on the system. The application remains on the cloud and it can be saved and edited in there only. ((SaaS) - (IaaS))?

Best Wishes

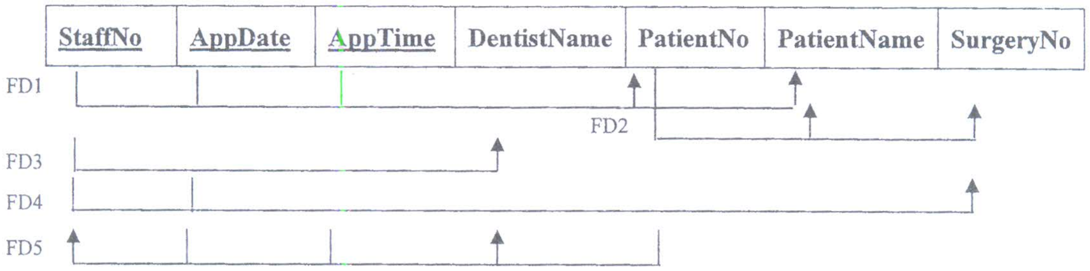
الفرقة الرابعة نصف العام ٢٠٢٢

University	:	*Menoufia*	*Date*	:	*9/01/2023*
Faculty	:	*Electronic Engineering*	*Exam*	:	*Final Exam*
Department	:	*Computer Science and Engineering*	*Examiner*	:	*Dr. Ahmed Shehata*
Academic Level	:	*4th Year*	*No. of Questions*	:	*5*
Course Name	:	*Advanced Database*	*Full Mark*	:	*90*
Course Code	:	*CSE 414*	*No. of pages*	:	*2*
Academic Year	:	*2022/2023*	*Start Time*	:	*10 AM*
Semester	:	*1st*	*Exam Duration*	:	*3 Hours*

Answer all the following questions:

Question No 1: **[8 Marks]**

Based on the given primary key of the following relation, Is this relation in 1NF, 2NF or 3NF? Why or why not? How would you successively normalize it completely?



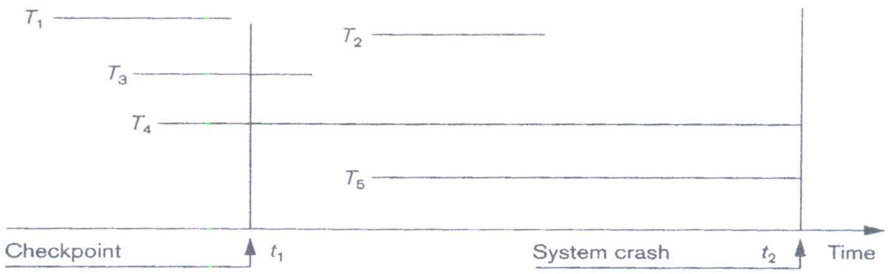
Question No 2: **[20 Marks]**

a) What is the purpose of database recovery? [5 M]

b) Differentiate between: Immediate Update and Deferred Update according to transaction status (executed, on commit and when rolled back). [5 M]

c) Discuss the operation of deferred update recovery technique concurrent users environments. [5 M]

d) Apply and explain the update recovery transaction process on the following timeline transactions using immediate update technique. [5 M]



Question No 3: **[20 Marks]**

a. What are the types of threats to databases? And what are the kinds of countermeasures that can be implemented to protect databases against these types of threats? [8 M]

b. Compare between discretionary and mandatory security mechanisms. [8 M]

c. Explain the two restrictions are enforced on data access based on the subject/object in Mandatory Access Control [4 M]

Question No 4: [22 Marks]

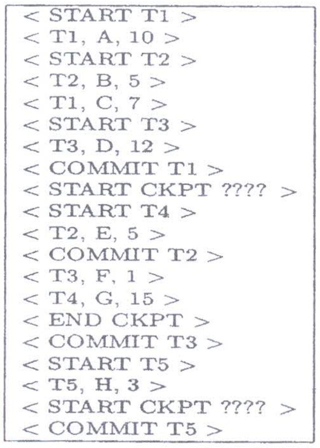
a. **State the main steps of the ARIES Recovery Algorithm** **[6 M]**

b. **Consider the content of the following undo log** **[8 M]**

```
LSN1    <START T1>
LSN2    <T1 X 5>
LSN3    <START T2>
LSN4    <T1 Y 7>
LSN5    <T2 X 9>
LSN6    <START T3>
LSN7    <T3 Z 11>
LSN8    <COMMIT T1>
LSN9    <START CKPT(T2,T3)>
LSN10   <T2 X 13>
LSN11   <T3 Y 15>
        *C*R*A*S*H*
```

1. Show how far back in the recovery manager needs to read the log. Write below the earliest LSN that the recovery manager reads.
2. Show below the values of variables and actions of the recovery manager during recovery:
3. What is the value of X at the end of the recovery

c. **After a system crash, the redo-log using non-quiescent checkpointing contains the following data:** **[8 M]**



```
< START T1 >
< T1, A, 10 >
< START T2 >
< T2, B, 5 >
< T1, C, 7 >
< START T3 >
< T3, D, 12 >
< COMMIT T1 >
< START CKPT ???? >
< START T4 >
< T2, E, 5 >
< COMMIT T2 >
< T3, F, 1 >
< T4, G, 15 >
< END CKPT >
< COMMIT T3 >
< START T5 >
< T5, H, 3 >
< START CKPT ???? >
< COMMIT T5 >
```

1. What are the correct values of the two <START CKPT ????> records? You have to provide two correct values for the two ????s.
2. Indicate and explain what fragment of the log the recovery manager needs to read.
3. Assuming that the two < START CKPT ??? > records are correctly stored in the log, according to your answer above, show which elements are recovered by the redo recovery manager and compute their values after recovery.

Question No 5: [20 Marks]

a. Draw the diagram of Knowledge Discovery (KDD) process. [4 M]

b. State the main tasks in Data Preprocessing? [4 M]

c. How to handle missing data? [4 M]

d. Use min-max normalization method by setting min=1 and max=10 to normalize the following values: 200, 250, 10, 40 [4 M]

e. What is the main steps to assure Data Quality? [4 M]

رابعة — حاسبات
نصف العام ٢٠٢٢

كلية الهندسة الإلكترونية

جامعة المنوفية

كلية الهندسة الإلكترونية

قسم هندسة وعلوم الحاسبات

جامعة المنوفية

Fall 2022 Final Exam
Digital Multimedia
Total 70 marks Time: 180 min
Examiner : Prof. Mohamed Abdou Berbar.

Q1(28)	Q2 (18)	Q3 (24)	Total (70)

Answer all the following

Question 1:

Which of the following statements is **False** and which is **True**:**[28 Marks]**

1) The decoder has to know the Huffman code table as used for encoding, either by default values or by explicit transmission of those table. [ ]

2) For any particular coding scheme, encoding and decoding algorithms will have the same run time. [ ]

3) Lossless, or entropy, compression does not ignore the semantics (meaning) of the data. [ ]

4) Lossy compression is based purely on the statistics of the symbols in the data. [ ]

5) Run-length encoding (RLE) is considered as Statistical Compression. [ ]

6) *Sampling* – restrict the value to a fixed set of *levels*. [ ]

7) *Quantization* –measure the value at discrete intervals. [ ]

8) Range of human hearing: roughly 20kHz–40kHz [ ]

9) Oversampling :
Samples 'too far apart' so cannot accurately reconstruct original signal. [ ]

10) Each time lossy compression applied, size of date decreases and quality of level of the file increases [ ]

11) Higher sampling rate and the larger the sample size, the more accurately sound can be digitized. [ ]

12) There is no guarantee that encoding and decoding algorithms will have the same run time. [ ]

13) For some applications, symmetric coding is necessary, while for others one end (typically the encoder) can be allowed to take significantly more time. [ ]

14) In symmetric applications, the hardware and the available processing time is usually also symmetric, while for asymmetric applications one end may have much faster hardware and/or more time. [ ]

15) Pulse-code modulation (PCM) is a method used to digitally represent sampled analog signals. [ ]

16) Any periodic waveform can be decomposed into a collection of *frequency components* [ ]

17) Sampling rate is the number of times per second that samples are taken; [ ]

18) Bit-depth determines the number of possible digital values that each sample can take. [ ]

19) Analog-to-Digital Converter (ADC) captures a snapshot of the electric voltage on an audio line and represents it as a digital number that can be sent to a computer. [ ]

20) The decoder has to know the LZW code table that used for encoding by explicit transmission of those tables. [ ]

21) In JPEG, after discrete cosine transform (DCT), The AC 64 values are read as a linear sequence using a default zig-zag-order. [ ]

22) In MPEG-1, B-frames are encoded with respect to previously encoded *I*- or P-frames. [ ]

23) The decoding part of the JPEG baseline algorithm is a sequence of operations, starting with"+128" (at all 64 pixels), followed by DCT and subsequent quantization (using a quantization table), and further followed by Huffman coding (using a Huffman code table).[ ]

24) In JPEG, the decoder has to know the quantization table and the Huffman code table as used for encoding, either by default values or by explicit transmission of those tables [ ]

25) In MPEG-1, the luminance channel is retained, but the chrominance channels are sub-sampled 2:1 in both coordinate directions.

[ ]

26) I-frames are encoded like still images (e.g. ,using for ex. the JPEG baseline algorithm). [ ]

27) In JPEG, there are I-frames, P-frames, and B-frames. [ ]

28) In MPEG-1, P-frames are encoded with respect to previously encoded I- or P-frames. [ ]

Question 2

(a) Given the following frequency table (Table 1), do the following:

Alphabet	H	G	F	E	D	C	B	A
Frequency	90	40	100	80	320	160	200	360

I. **Draw** Huffman tree **[2 Marks]**
II. **Find** Huffman Codes (code1) **[2 Marks]**
III. **Find** average length of coded character **[2 Marks]**

Solution

A	
B	
C	
D	
E	
F	
G	
H	

Code1 Average length = …..

Code2 Average length = ….

Code 1 is better in ………
Code 2 is better in ………

(b) Apply Dictionary based compression algorithm to decompress (decode) the following code **[1 - 2 - 3 - 2 - 5 - 4 - 6 - 11 – 1]** assuming that compressed alphabet consisting of 4 symbols (S1, S2, S3, S4). **[4 marks]**

(c) In MPEG, **Why** AC-coefficients of B and P frames are usually very large values, whereas those of I frame are very small? **[2 Marks]**

Answer:

(d) It is required to store a 24-bit true colour (with spatial resolution 1024 x 768) uncompressed video of 3-hours duration on the hard disk. **What is the storage size of that video?** Assuming you applied sampling 4:1:1 and applying a compression technique with (1:26) compression rate. **What is the storage size of that video?** **[2 Marks]**

Answer:

(e) In MPEG-1, There are different search strategies used in MPEG-1 for detecting matching macroblocks. Does the decoder require that the used search strategy is known? **[2 Marks]**

i. no **ii.** Yes **iii.** at least for the intensity channel

iv. at least for one of the three channels, no matter whether intensity or chroma channels

Answer:

(f) In MPEG-1, A macroblock in this coding scheme is defined by

i. one 8 _ 8 block in the intensity channel, and two 8 _ 8 blocks in the two chroma channels.

ii. four 8 _ 8 blocks in the intensity channel, and four 8 _ 8 blocks in the two chroma channels.

iii. four 8 _ 8 blocks in the intensity channel, and two 8 _ 8 blocks in the two chroma channels.

iv. four 8 _ 8 blocks in the intensity channel, and eight 8 _ 8 blocks in the two chroma channels. **[2 Marks]**

Answer:

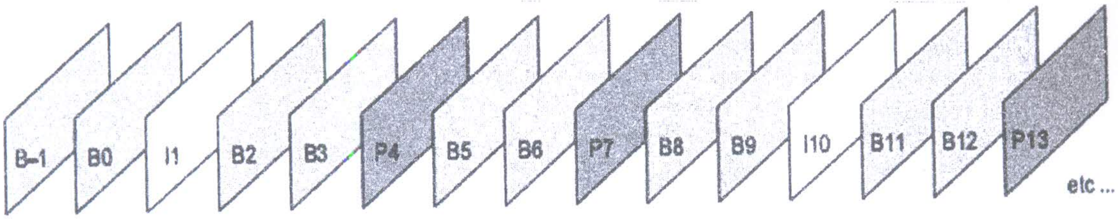
Question 3

(a) Explain the interleaving and error correction scheme (CIRC) *Cross Interleave Reed-Solomon Code* used in audio CD encoding. You can use the following example: CD-DA data is considered to be in two stereo channels sampled at 44.1kHz at 16 bits/sample. The samples from each channel are arranged in alternating order (left 16 bits, right 16 bits, etc.) to yield 32-bit sampling periods. [3 **Marks**]

b) If the display order of the flowing video frames as shown below, **show how** the transmission order should be.

[4 Marks]

Display order



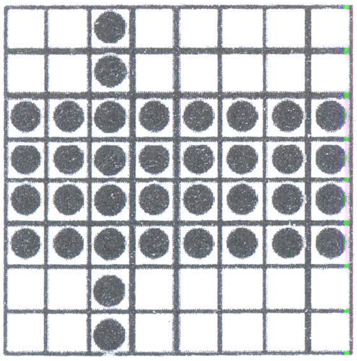
Answer:

[c] What we should be concerned with the compression algorithm characteristics. [**3 Marks**]

Answer:

[d] **Write** an algorithm that performs simple, lossy DPCM coding on sampled audio. For samples of people speaking. For the DCPM examples, **can you** gain any additional compression by applying run-length coding to the output of the DPCM coder? **Why** or why not? [3 Marks]

[e] **Write** an algorithm that performs run-length coding on images. Use the image in the following figure for processing purposes, **What** percent compression do you get.



[3 Marks]

[f] Explain the characteristics of following: [3 Marks]

Frequency Masking - Temporal masking

Menoufia University
Faculty of Electronic Engineering
Computer Science & Engineering
Department

Network Security (4th year)
Exam Date: Sunday Jan 2, 2023
Exam Duration: **3 hours**

Final Exam
(2022/2023 – 1st Semester)

Instructions

1-Write your name in the outside ***cover page only (do not provide any identity information in this booklet).***

2- Make sure that there ***are 6 questions*** *in this* ***6 pages booklet*** *(cover pages are not counted). Use your time wisely.*

3-Answer all the questions ***here in*** *this booklet.* ***Do not use any other external papers****.*

4-Points of each question are equally divided unless otherwise mentioned.

Marking Scheme						
Q1 /10	**Q2 /16**	**Q3 /12**	**Q4 / 16**	**Q5 / 16**	**Q6 /20**	**Total / 90**

Q1: Define [10 points]

a. Replay attack.

b. Strict Avalanche Criterion.

c. Bit Independence Criterion.

d. Polyalphabetic cipher.

e. Masquerading.

Q2: Select the correct answer [16 points]

1. In public cryptosystems, the sender of the message uses................to create cipher text:

(b) Own private key **(b) Receiver's private key** **(c) Receiver's public key**

2. Euler's totient function Φ (8 * 7) is

a) 4 *6 **b) 7 * 6** **c) 7 * 3** **d) 7 * 4**

3. The final output of DES is

a) IP (R_{16} ||L_{16}) **b) IP (L_{16} ||R_{16})** **c) IP^{-1} (R_{16} ||L_{16})** **d) IP^{-1} (L_{16} ||R_{16})**

4. The matrix used in Play Fair encryption is of size

a) 4×8 **b) 5×5** **c) 8×8** **d) 5×8**

5. The input to the DES is

a) IP (R_0 ||L_0) **b) IP (L_0 ||R_0)** **c) IP^{-1} (R_0 ||L_0)** **d) IP^{-1} (L_0 ||R_0)**

6. The **minimum number** of cryptographic keys in 3DES required to achieve a higher level of security than DES is:

a) 1 **b) 2** **c) 3** **d) 4**

7. Which is the largest disadvantage of the asymmetric Encryption? **a) Complex and time-consuming.** **b) Problem of the transmission of the Secret Key.** **c) Less secure encryption function.**

8. In the DES algorithm the Round Input is 32 bits, which is expanded to 48 bits via **a) Scaling of the existing bits** **b) Duplication of the existing bits** **c) addition of ones.**

Q3: True or False. [12 points]

1. Eavesdropping is the network attack that floods the network with useless traffic.	
2. Symmetric key cryptography needs a mechanism for key distribution.	
3. Brute force attack can be used to break RSA.	
4. The input block length in DES is 128 bits.	
5. Symmetric key is also called a Secret key.	
6. All Stream ciphers are unbreakable.	
7.RSA depends on a two-way function that is easy to go in both directions.	
8. Public Key cryptography is limited to key exchange	
9. The number of tests required to break the 3DES algorithm are 2^{113}	
10. When used together, a secret key scheme is used for session keys encryption and a public key scheme is used for messages encryption.	
11. In RSA, the values of e and d must be inverse multiplicative with respect to n.	
12. Symmetric encryptions cannot be used for Digital signature.	

Q4: Solve [16 points]

a- Use the **fast exponentiation algorithm** to find the result of 11^{17} mod 4.

b- Encrypt “I love this course” with “Double Rail Fence” with key = 2.(hint: encrypt twice with key =2)

c- How can we get the 48 bits of the key that are used as the cipher key if the original key is 64 bits?

d -What are the weakness and strengths of DES?

Q5: Justify [16 points]

a-In **RSA**, if we can easy factoring n, the security of the algorithm could be compromised.

b- Even though anonymity could be seen as the opposite of accountability, both are goals of security.

c- Two popular choices of the value e in RSA are *e*=3 and *e*=17.

d- In RSA, Φ (n)=(p-1)(q-1).

Q6: Critical Thinking. [20 points]

a- Assume DES with a key length of 56 bits is used for encryption, how much time is required for a brute-force attack to break the cipher if the machine is performing one DES decryption per microsecond?

b- Explain the steps to perform the Meet-in-the–middle attack on double encryption DES (with equations).

c- Explain how permutation and substitution is performed in Feistel Structure

d -Explain "Swapping the result after round 16 makes DES decryption works in the same way as encryption". What if there is no swap?

حاسبات
الفرقة الرابعة نصف العام ٢٠٢٢

Menoufia University
Faculty of Electronic Engineering
Computer Science & Engineering
Department

Network Security (4th year)
Exam Date: Sunday Jan 2, 2023
Exam Duration: **3 hours**

Final Exam
(2022/2023 – 1st Semester)

Instructions

1-Write your name in the outside ***cover page only (do not provide any identity information in this booklet).***

2- Make sure that there ***are 6 questions*** *in this* ***6 pages booklet*** *(cover pages are not counted). Use your time wisely.*

3-Answer all the questions ***here in*** *this booklet.* ***Do not use any other external papers.***

4-Points of each question are equally divided unless otherwise mentioned.

Marking Scheme						
Q1 /10	**Q2 /16**	**Q3 /12**	**Q4 / 16**	**Q5 / 16**	**Q6 /20**	**Total /90**

Q1: Define [10 points]

a. Replay attack.

b. Strict Avalanche Criterion.

c. Bit Independence Criterion.

d. Polyalphabetic cipher.

e. Masquerading.

Q2: Select the correct answer [16 points]

1. In public cryptosystems, the sender of the message uses................to create cipher text:

(b) Own private key **(b) Receiver's private key** **(c) Receiver's public key**

2. Euler's totient function Φ (8 * 7) is

a) 4 *6 **b) 7 * 6** **c) 7 * 3** **d) 7 * 4**

3. The final output of DES is

a) $IP (R_{16} || L_{16})$ **b)** $IP (L_{16} || R_{16})$ **c)** $IP^{-1} (R_{16} || L_{16})$ **d)** $IP^{-1} (L_{16} || R_{16})$

4. The matrix used in Play Fair encryption is of size

a) 4×8 **b) 5×5** **c) 8×8** **d) 5×8**

5. The input to the DES is

a) $IP (R_0 || L_0)$ **b)** $IP (L_0 || R_0)$ **c)** $IP^{-1} (R_0 || L_0)$ **d)** $IP^{-1} (L_0 || R_0)$

6. The **minimum number** of cryptographic keys in 3DES required to achieve a higher level of security than DES is:

a) 1 **b) 2** **c) 3** **d) 4**

7. Which is the largest disadvantage of the asymmetric Encryption? **a) Complex and time-consuming.** **b) Problem of the transmission of the Secret Key.** **c) Less secure encryption function.**

8. In the DES algorithm the Round Input is 32 bits, which is expanded to 48 bits via **a) Scaling of the existing bits** **b) Duplication of the existing bits** **c) addition of ones.**

Q3: True or False. [12 points]

1. Eavesdropping is the network attack that floods the network with useless traffic.	
2. Symmetric key cryptography needs a mechanism for key distribution.	
3. Brute force attack can be used to break RSA.	
4. The input block length in DES is 128 bits.	
5. Symmetric key is also called a Secret key.	
6. All Stream ciphers are unbreakable.	
7.RSA depends on a two-way function that is easy to go in both directions.	
8. Public Key cryptography is limited to key exchange	
9. The number of tests required to break the 3DES algorithm are 2^{113}	
10. When used together, a secret key scheme is used for session keys encryption and a public key scheme is used for messages encryption.	
11. In RSA, the values of e and d must be inverse multiplicative with respect to n.	
12. Symmetric encryptions cannot be used for Digital signature.	

Q4: Solve [16 points]

a- Use the **fast exponentiation algorithm** to find the result of 11^{17} mod 4.

b- Encrypt “I love this course” with “Double Rail Fence” with key = 2.(hint: encrypt twice with key =2)

c- How can we get the 48 bits of the key that are used as the cipher key if the original key is 64 bits?

d -What are the weakness and strengths of DES?

Q5: Justify [16 points]

a-In **RSA**, if we can easy factoring n, the security of the algorithm could be compromised.

b- Even though anonymity could be seen as the opposite of accountability, both are goals of security.

c- Two popular choices of the value e in RSA are e=3 and e=17.

d- In RSA, Φ (n)=(p-1)(q-1).

Q6: Critical Thinking. [20 points]

a- Assume DES with a key length of 56 bits is used for encryption, how much time is required for a brute-force attack to break the cipher if the machine is performing one DES decryption per microsecond?

b- Explain the steps to perform the Meet-in-the–middle attack on double encryption DES (with equations).

c- Explain how permutation and substitution is performed in Feistel Structure

d -Explain "Swapping the result after round 16 makes DES decryption works in the same way as encryption". What if there is no swap?

الفرقة الرابعة نصف العام ٢٠٢٢ حاسبات

University : Menoufia		Date	: 5 /01/2023
Faculty : Electronic Engineering		Time	: 3 Hours
Department : Computer Science&Eng.		No. of pages	: 2
Academic level : 4th Year		Full Mark	: 70 Marks
Course Name : Distributed Systems		Exam	: Final Exam
Course Code : : CSE 468	جامعة المنوفية	Examiner	: Assoc. Prof: Nirmeen A. El-Bahnasawy

Answer the following questions:

Question No. 1 : **(30 Marks)**

a) What are the four benefits of using cloud computing?
b) Explain different models for deployment in cloud computing?
c) State the difference between allocation problem and scheduling problem.
d) Give only three IoT – ENVIRONMENTAL MONITORING applications.
e) State the Fog Computing Architecture?
f) Give a block diagram explains How IoT model works

Question No 2: **(20 Marks)**

a) Give the Gantt chart of a schedule for the sample task graph of Figure 1 on three homogeneous processors. Calculate speedup and efficiency parameters.

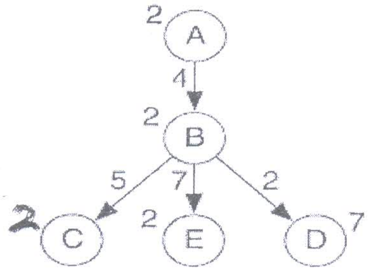


Fig. 1

b) Program for x = a ∗ 7 + (a ∗ 5 + 2) As a DAG and get Gantt chart onto 2 processors. Take unit of time is unity and no communication cost.

Question No 3 : **(10 Marks)**

State is the main concept of the following topics:

1. First Come First Serve algorithm.

2. **Max-min algorithm.**
3. **Virtualization.**
4. **Challenges of big data in cloud computing.**
5. **IoT – Disadvantages.**

Question No 4 :

Choose the correct answer: **(10 Marks)**

1. **Tasks carry out independently. This refers to (concurrency – no global clock)?**
2. **Interfaces should allow components to be added or replaced. (Openness – scalability)?**
3. **Protection against disclosure to unauthorized individual. (Confidentiality – integrity)?**
4. **Enables local and remote resources to be accessed using identical operations. (Concurrency transparency - Access transparency)?**
5. **It is closer proximity to small end users, its wider consumer reach, and better mobility. Refers to (Edge computing – Fog computing)?**
6. **Communication delay between two tasks allocated to the same processors is (negligible – idle time)?**
7. **Systems enhanced data collection (IoT – Foggy)?**
8. **The extension or lowering of cloud computing capabilities to the bottom/edge of the network in order to provide faster ICT (communication, storage, software, etc.) services to the lower end users.(edge computing – fog computing)?**
9. **Is being one of the characteristic provide the concept of commissioning and decommissioning of large amount of resource capacity dynamically. (Scalability – elasticity)?**
10. **Service provides cloud applications which are used by the user directly without installing anything on the system. The application remains on the cloud and it can be saved and edited in there only. ((SaaS) - (IaaS))?**

Best Wishes