



COT L300 2nd Semester - Past questions to practice before exams

Algorithms and Data Structure (Université de Buéa)



Scan to open on Studocu

MONTH: May
 YEAR: 2022
 DATE: 24/05/2022
 TIME ALLOWED: 2 HOURS

INSTRUCTION: ALL DOCUMENTS ARE ALLOWED

QUESTION 1

The one-way function for password-checking scheme is used to authenticate a user based on the password and userid.
Implement the scheme using the following table

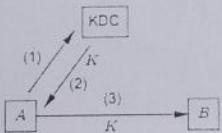
USERID	PASSWORD
A	01001101
B	01111101
C	01000001

Answer the following questions in the implementation.

- i. Use the initialization vector, IV = 010 to establish the one way encryption table
- ii. Explain how the user A could be authenticated.

QUESTION 2

Kiberos authentication service used to authenticate clients and servers in a public network such as the Internet uses a key distribution centre (KDC) as the trusted third party (TTP). The diagram below depicts the basic operation of a KDC.



- Let private keys $K_A = \{3, 2, 0, 1, 7, 6, 5, 4\}$ and $K_B = \{7, 6, 5, 4, 3, 2, 1, 0\}$
- Let the entities identities be $A = 011$ and $B = 101$
- K is considered as mapping in the keyspace, consider the mapping to be $210 = 0102$ corresponding to session key, $K = \{6, 3, 4, 0, 1, 2, 7, 5\}$. Hence in (2) append 010 to the identities of A and B and use K to encrypt message in (3)
- Entity A concatenates its identity to that of B and encrypted with K_A , that is 011101 is encrypted using K_A .
 - i) Implement (1), (2) and (3) using artificial parameters above
 - ii) Implement pairwise communication between A & B
- Let session key, $K = \{6, 3, 4, 0, 1, 2, 7, 5\}$
- Let message, $m = 011010111001$

UNIVERSITY OF BUEA
 COLLEGE OF TECHNOLOGY
 MID SEMESTER EXAMINATIONS
COURSE INSTRUCTOR: SONE EKONDE
COURSE CODE & NUMBER: CEC 304
COURSE TITLE: Date Security & Integrity
TIME: 14.00 – 16.00
CREDIT VALUE: 4

MONTH: April
YEAR: 2022
DATE: 30/04/2022
TIME ALLOWED: 2 HOURS

QUESTION 1

The following question concerns elliptic curve cryptography (ECC). The encryption/ decryption algorithm is as shown.

Encryption/ Decryption

- Private/ public key pairs:
 $(a; P_A = a \cdot B); (b; P_B = b \cdot B)$
where B = basis point
- Encryption
 $P_C = [k \cdot B], (P_M + k \cdot P_B)$
where k = integer and P_M is point on curve
- Decryption
 $(P_M + k \cdot P_B) - [b \cdot (k \cdot B)]$

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

2	2	1	R
2	1	0	1
2	5	0	
2	2	1	
2	1	0	

Use the algorithm and the following parameters to answer the question below:

- elliptic curve $y^2 = x^3 + 3x + 8 \pmod{13}$ with the following complete addition table

	\mathcal{O}	(1, 5)	(1, 8)	(2, 3)	(2, 10)	(9, 6)	(9, 7)	(12, 2)	(12, 11)
\mathcal{O}	\mathcal{O}	(1, 5)	(1, 8)	(2, 3)	(2, 10)	(9, 6)	(9, 7)	(12, 2)	(12, 11)
(1, 5)	(1, 5)	(2, 10)	\mathcal{O}	(1, 8)	(9, 7)	(2, 3)	(12, 2)	(12, 11)	(9, 6)
(1, 8)	(1, 8)	\mathcal{O}	(2, 3)	(9, 6)	(1, 5)	(12, 11)	(2, 10)	(9, 7)	(12, 2)
(2, 3)	(2, 3)	(1, 8)	(9, 6)	(12, 11)	\mathcal{O}	(12, 2)	(1, 5)	(2, 10)	(9, 7)
(2, 10)	(2, 10)	(9, 7)	(1, 5)	\mathcal{O}	(12, 2)	(1, 8)	(12, 11)	(9, 6)	(2, 3)
(9, 6)	(9, 6)	(2, 3)	(12, 11)	(12, 2)	(1, 8)	(9, 7)	\mathcal{O}	(1, 5)	(2, 10)
(9, 7)	(9, 7)	(12, 2)	(2, 10)	(1, 5)	(12, 11)	\mathcal{O}	(9, 6)	(2, 3)	(1, 8)
(12, 2)	(12, 2)	(12, 11)	(9, 7)	(2, 10)	(9, 6)	(1, 5)	(2, 3)	(1, 8)	\mathcal{O}
(12, 11)	(12, 11)	(9, 6)	(12, 2)	(9, 7)	(2, 3)	(2, 10)	(1, 8)	\mathcal{O}	(1, 5)

Encrypt $P_M = (2, 3)$ by using $a = 2; b = 3; k = 4$ and $B = (1, 5)$

(10 marks)

QUESTION 2

Suppose node A₁ wishes to send the plaintext PETER with its decimal equivalent equal to 21 to node A₆ using the RSA algorithm. Use the following data

primes $p = 11; q = 5$ and $e_6 = 27$

$$C = D^e \pmod{n}$$

to answer the following questions

- Compute the ciphertext received by A₆
- Explain how A₆ decrypts message PETER

(HINT: Use binary exponentiation technique in your computation)

(8 marks)

2 | 27 | R
2 | 13

0	1	2	3	4	5	6	7	8	9
a	b	c	d	e	f	g	h	i	j
w	u	m	n	o	p	q	r	s	t
k	l	v	w	x	y	z			
u	v	w	x	y	z				

QUESTION 3

The ciphertext

MKWJAFQCHIUPVPQNWHFDRKEFIROFEHGQMRGM
SC RAMBLES CRAMABLES CRAMABLES CRAM

is the result of encrypting a message in the Vigenere system, using the keyword SCRAMBLE.
Find the message.

(5 marks)

QUESTION 4

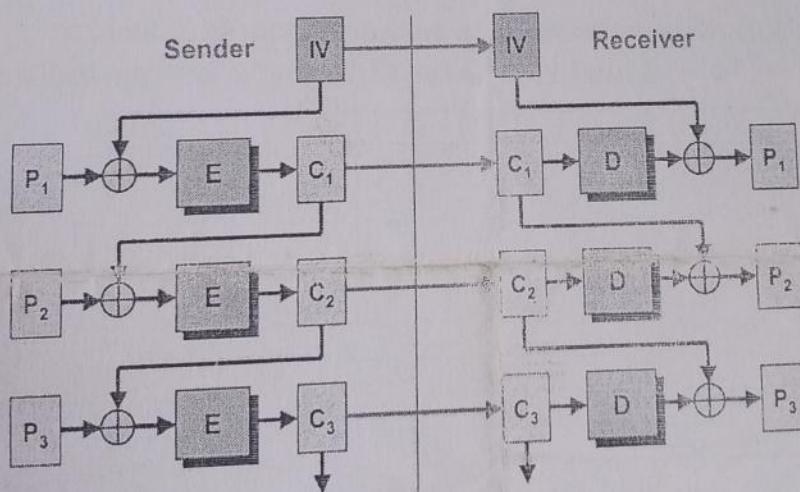
Use the Cipher Block Chaining (CBC) mode to

- a) Encrypt and b) Decrypt
- the message $m = 11010010$

The encryption key, $k_E = \{0, 4, 1, 9, 12, 10, 14, 3, 7, 5, 15, 11, 8, 6, 13, 2\}$

The initialization vector, IV = 0110

The block diagram of CBC is as shown below.



(7 marks)

QUESTION 1 (25 marks)

ECDH

- Public/ private key pairs:
 $(a; P_A = a.B);$
 $(b; P_B = b.B)$
 where B = basis point
- Shared secret
 $K_{ab} = abB$
- Encryption
 $P_C = [(kB), (P_M + kK_{ab})]$
 where k = integer and P_M is point on curve
- Decryption
 $(P_M + kK_{ab}) - [b.(kB)]$

ECDSA

- KEY GENERATION
 A selects a random integer d as the private key, and publishes $Q = dB$ as the public key
- SIGNING
 - Select a random integer k ;
 Compute $kb = (x_1, y_1)$ and $r = x_1 \bmod n$;
 - Compute $k^{-1} \bmod n$;
 - Compute $h(m)$, where h is a hash function of m ;
 - Compute $s = k^{-1}\{h(m) + dr\} \bmod n$.
 (r, s) is A 's signature of message m .

Use the algorithms above and the following parameters to answer the questions below:

- elliptic curve $y^2 = x^3 + 3x + 8 \pmod{13}$ with the following complete addition table

	\mathcal{O}	(1,5)	(1,8)	(2,3)	(2,10)	(9,6)	(9,7)	(12,2)	(12,11)
\mathcal{O}	\mathcal{O}	(1,5)	(1,8)	(2,3)	(2,10)	(9,6)	(9,7)	(12,2)	(12,11)
(1,5)	(1,5)	(2,10)	\mathcal{O}	(1,8)	(9,7)	(2,3)	(12,2)	(12,11)	(9,6)
(1,8)	(1,8)	\mathcal{O}	(2,3)	(9,6)	(1,5)	(12,11)	(2,10)	(9,7)	(12,2)
(2,3)	(2,3)	(1,8)	(9,6)	(12,11)	\mathcal{O}	(12,2)	(1,5)	(2,10)	(9,7)
(2,10)	(2,10)	(9,7)	(1,5)	\mathcal{O}	(12,2)	(1,8)	(12,11)	(9,6)	(2,3)
(9,6)	(9,6)	(2,3)	(12,11)	(12,2)	(1,8)	(9,7)	\mathcal{O}	(1,5)	(2,10)
(9,7)	(9,7)	(12,2)	(2,10)	(1,5)	(12,11)	\mathcal{O}	(9,6)	(2,3)	(1,8)
(12,2)	(12,2)	(12,11)	(9,7)	(2,10)	(9,6)	(1,5)	(2,3)	(1,8)	\mathcal{O}
(12,11)	(12,11)	(9,6)	(12,2)	(9,7)	(2,3)	(2,10)	(1,8)	\mathcal{O}	(1,5)

- Pairing table is as follows

Point	(1,5)	(1,8)	(2,3)	(2,10)	(9,6)	(9,7)	(12,2)	(12,11)
Word	RAM	SAW	CUT	MET	SIR	YOU	CUP	DOT

- Let $a = 2; b = 3; k = 5, d = 4, B = (1,5)$ and $h(m)$ could be computed from $m = 00111011101$ using Initialization vector, IV = 101

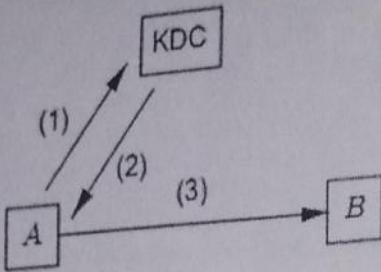
- Encrypt and decrypt the word CUP
- Establish the digital signature of the word RAM

(6+6 marks)

(13 marks)

QUESTION 2 (25 marks)

- A) Kerberos is an authentication service designed to allow clients to access application servers in a secure manner over a network. The diagram below depicts the Kerberos authentication service where A is the client, B is the application server and KDC is the key distribution centre.



- Briefly explain (1), (2) and (3)
- State the contents of the Kerberos ticket from the key distribution centre (KDC)
- State the contents of the Kerberos authenticator from the client to the application server.
- Use the information below to explain how the application server uses the contents of the ticket and authenticator to authenticate the client

- Let private keys $K_A = \{3, 2, 0, 1, 7, 6, 5, 4\}$ and $K_B = \{7, 6, 5, 4, 3, 2, 1, 0\}$
- Let the session key, $K = \{6, 3, 4, 0, 1, 2, 7, 5\}$
- Keys are mapped to decimal equivalents in the keyspace. Let the mapping of the session key, K correspond to decimal 2 which is 010.
- Let the entities identities be $A = 011$ and $B = 101$

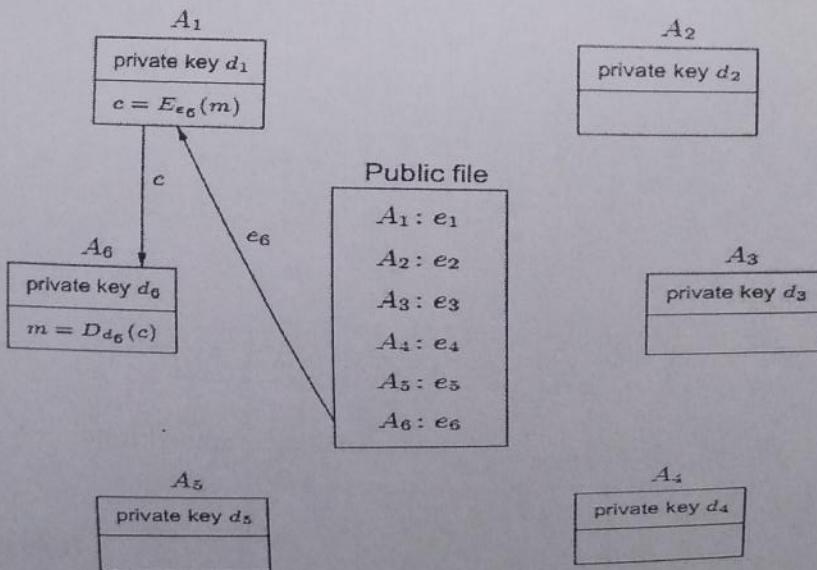
(13 marks)

- B) Suppose node A_1 wishes to send the plaintext PETER with its decimal equivalent equal to 21 to node A_6 using the RSA algorithm. Use figure below and the following data

primes $p = 11$; $q = 5$ and $e_6 = 27$

to answer the following questions

- Compute the ciphertext received by A_6
- Show how A_6 decrypts message PETER
- Assume an active attacker eavesdrop on A_6 public key. Implement a countermeasure to circumvent the attack.



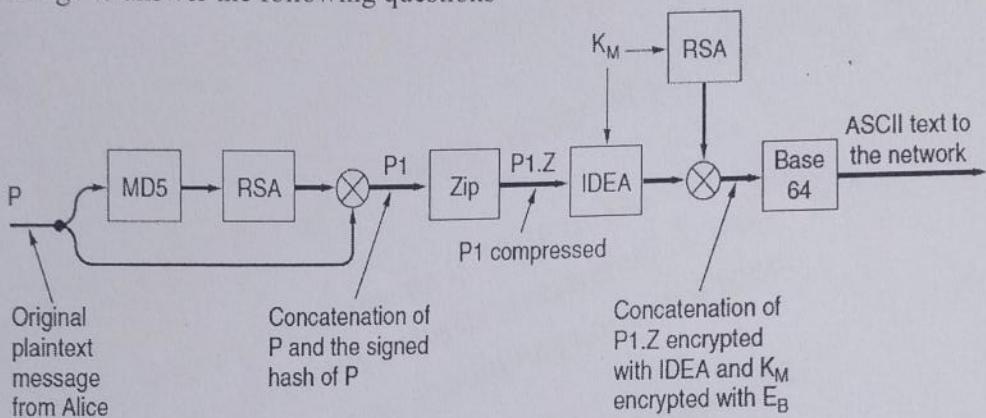
(12 marks)

QUESTION 3 (25 marks)

A) Use a block diagram to briefly explain the fixed DES-encrypted password algorithm. (4 marks)

B) The strength of a password could be estimated from its entropy. Assuming that all the passwords are equally probable, show that the password formed using 6 lowercase characters is weaker compared to a password formed using 5 mixed (lowercase & uppercase) alphanumeric characters (5 marks)

C) Use the block diagram of the PGP (Pretty Good Privacy) which is a complete email security package to answer the following questions



- i) State two advantages to hash the plaintext using MD5 algorithm before RSA signing?
ii) Use the following values to implement the two RSA schemes shown in figure above

- Alice private parameters: $p = 5$; $q = 11$; $d = 7$
- Bob private parameters: $p = 13$; $q = 7$; $d = 3$
- Output of MD5 algorithm, hash of plaintext, $h = 10$
- Session key, $K_M = 23$

(8 marks)

D) Distinguish between entity authentication and message authentication code

Use the following artificial parameters to implement the Hashed Message Authentication Code (HMAC)

- Message to be hashed, $m = 10010100110100011010$
- Message is divided into blocks of 8 bits
- Shared secret key, K is a 4-bit word: $K = 0101$
- Initialization vector, $IV = 01010011$
- First pass key, i_pad key. Final key, $K1$ is obtained with two repetitions of 0111.
- Second pass key, o_pad key. Final key, $K2$ is obtained with two repetitions of 1101.

(8 marks)

9. Provide a word that best qualifies each statement below. (7 mks)

- v. The aspect of paragraphs that deals with ouvert connection of ideas Cohesive Coherence
- vi. A term used for the relationship of ideas in paragraphs Cohesion

10. Indicate if each of the following statements is TRUE or FALSE

- xi. A good introductory paragraph needs a thesis statement. True
- xii. Each paragraph in an expository essay should not contain a topic sentence. False
- xiii. Cohesion in paragraphs relates the use of observable elements that allow for unity. False
- xiv. Coherence in paragraphs deals with logical arrangements of thought. False
- xv. The use of the passive voice in report writing is more important than the active. True

11. Indicate if each of the sentences below is active, passive, or neither active nor passive.

XI. This car was produced six years ago. Passive

XII. Ndop cultivates rice.

..... Active

XIII. This car was produced six years ago.

..... Passive

XIV. The students are writing a CA test.... Active

XV. My shoes are clean. Active

XVI. The test will be graded based on some criteria.

..... Passive

12. List the three cohesive elements in the sentence below.

My students applaud when they understand lectures. It is a good habit.

1. When

2. They

3. It

1. 0+0 null
2. 3.3 ABC

Part 1: Attempt all questions for a maximum of 15 marks

Question 1: MCQs (7 marks)

In the grid provided on the right, mark an X on the letter that corresponds to the best answer from the list of options given for the questions. (Note: Check one option only, and mark your answer clearly)

- a) A Java bytecode file has the following extension:
 (A) .class (B) .o (C) .byte (D) .java
- b) A literal can be of which of these data types?
 (A) float (B) int (C) boolean (D) All of the above
- c) When you compile a Java source code, you generate:
 (A) Object code that is different for different platforms
 (B) Bytecode code that is the same irrespective of the platform
 (C) Bytecode that is different for different platforms
 (D) Object code that is the same irrespective of the platform
- d) Which of the following is a valid declaration of an object of class Box?
 (A) Box obj = new Box(); (B) Box obj = new Box; (C) obj = new Box(); (D) new Box obj;
- e) What is the output from the program in Figure 1?
 (A) The code does not compile (B) true true (C) true false (D) false true

```
public class Ex2 {
    public static void main(String[] args) {
        int []a = {1,2,053,4};
        int [][]b = {{1,2,4}, {2,2,1}, {0,43,2}};
        System.out.print(a[3]==b[0][2]);
        System.out.println(" " + (a[2]==b[2][1]));
    }
}
```

Figure 1

```
public class Ex1 {
    public static void main(String[] args) {
        int x = 10;
        int y = new Ex1().change(x);
        System.out.print(x + " " + y + "***");
        int i, a = 1, b = 0;
        for (i = 0; i < 5; i++) { a = a * 2; b++; }
        System.out.println(i + " " + a + " " + b);
    }
    int change(int x) { x = 5; return x; }
}
```

Figure 2

- f) What is the output from the program in Figure 2?
 (A) 5**5 32 5 (B) 10 5**4 16 4 (C) 10 5**4 32 4 (D) 10 5**5 32 5
- g) What is the output from the program in Figure 3?
 (A) 7 10 20 (B) 7 8 9 (C) 5 10 15 (D) The program will not compile

```
public class Spindle {
    public static void main(String[] args) {
        int[] a = new int[]{5, 10, 15, 20};
        int b = 10, c = 20;      Fold.mutilate(a, b, c);      System.out.printf("%d %d %d\n", a[0], b, c);
    }
}
class Fold {
    static void mutilate(int[] a, int b, int c) { a[0] = 7; b = 8; c = 9; }
}
```

Figure 3

Question 2: (1+2 = 3 marks)

Consider the code in Figure 4. Write the name(s) of the file(s) in which the code must be stored. Also write the output you would get when the code is executed. (3 marks)

File name(s) ValueHolder.java (B)
 1 2 3 F
 ABC 1 2 3 F
 ABC
 ValueHolder.java
 ValueHolderDisplay.java
 0 0 null
 1 2 3 ABC

```
public class ValueHolder {
    public int anInt;
    public float aFloat;
    public String sString;
}

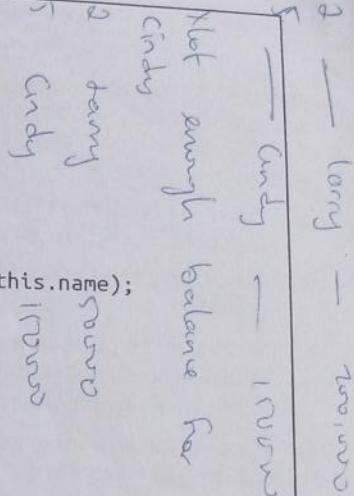
public class ValueHolderDisplay {
    public static void main(String[] args) {
        ValueHolder aValueHolder = new ValueHolder();
        System.out.print(aValueHolder.anInt + " ");
        System.out.print(aValueHolder.aFloat + " ");
        System.out.println(aValueHolder.sString);
        aValueHolder.anInt = 1;
        aValueHolder.aFloat = 2.3f;
        aValueHolder.sString = "ABC";
        System.out.print(aValueHolder.anInt + " ");
        System.out.print(aValueHolder.aFloat + " ");
        System.out.println(aValueHolder.sString);
    }
}
```

Figure 4

3: Question 3: (1.5 + 1.5 + 2 = 5 marks)

```
public class BankAccount {  
    private int balance, id;  
    String name;  
    public BankAccount(int id, String name, int balance) {  
        //A: Write appropriate code here  
    }  
    public void deposit(double amount) {  
        balance += amount;  
    }  
    public void withdrawal(double amount) {  
        if (!overdraft(amount)) balance -= amount;  
        else System.out.println("Not enough balance for " + this.name);  
    }  
    public boolean overdraft(double amount) {  
        //B: Write appropriate code here  
    }  
    public String toString() {  
        return id + "\t" + name + "\t" + balance;  
    }  
    public static void main(String[] args) {  
        BankAccount larry = new BankAccount(2, "Larry", 100000);  
        BankAccount cindy = new BankAccount(5, "Cindy", 150000);  
        System.out.println(larry.toString()); System.out.println(cindy.toString());  
        larry.withdrawal(50000); cindy.withdrawal(200000);  
        System.out.println(larry.toString()); System.out.println(cindy.toString());  
    }  
}
```

Figure 5



appropriate code to replace Comment A

~~BankAccount.int = id;~~
~~BankAccount.string = name;~~
~~BankAccount.balance = balance;~~

Public ~~BankAccount (int, name, balance)~~

Comments are not allowed, i.e., an account holder cannot withdraw more funds than the current account balance. Write appropriate code to replace Comment B so that the overdraft policy is implemented.

~~if (withdrawal > balance)~~

~~System.out.print("Insufficient funds for withdrawal");~~

The output of the program, assuming that you have correctly done (a) and (b) above

~~BankAccount larry = new BankAccount(2, "Larry", 100000);~~
~~BankAccount cindy = new BankAccount(5, "Cindy", 150000);~~
~~cindy.balance = 50000;~~
~~cindy.balance = "Insufficient funds for withdrawal";~~

(b) ~~if (balance > amount)~~:

b) public boolean overdraft (double amount) {

~~if (return balance < amount)~~

This document is available on

1. Define: Base: A base is a number system with its own digits and operands. 3marks

Number system: A number system is a collection of digits in a type of base.

Bit: A bit is a single digit character in a number system.

2. Give the base and symbols of the following number systems: 2marks

Decimal: base: 10

Symbols: ()₁₀ DEC = {0, 1, 2, 3, 4, 5, 6, 7, 8, 9}

Binary: base: 2

Symbols: ()₂ BIN = {0, 1}

Octal: base: 8

Symbols: ()₈ OCT = {0, 1, 2, 3, 4, 5, 6, 7}

Hexadecimal: base: 16

Symbols: ()₁₆ HEX = {0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F}

3. What is the two's complement of: 2marks

0101 = 0011

10110100 = 010110

4. Perform the following operations A+B; A-B; A×B on the given numbers (110110)₂; (101001)₂ 3marks

$$\begin{array}{r} A+B: 110110 \\ + 101001 \\ \hline 1011111 \end{array}$$

$$A+B = 101111_2$$

$$\begin{array}{r} A-B: 110110 \\ - 101001 \\ \hline 1101 \end{array}$$

$$A-B = 1101_2$$

$$\begin{array}{r} A\times B: 110110 \\ \times 101001 \\ \hline 110110 \\ 0000000 \\ 0000000 \\ 110110000 \\ + 100000000 \\ \hline 100101001100_2 \end{array}$$

$$A\times B = 100101001100_2$$

5. Perform the following conversion

a) $(567)_{10} = (?)_{16} = (?)_8$

To hexadecimal:

$$\begin{array}{r} 16 | 567 \\ 16 | 35 \\ 16 | 2 \\ 0 | 2 \end{array} \therefore (567)_{10} = (237)_{16}$$

c) $(B.2C)_{16} = (?)_8 = (?)_{10}$

$(B.2C)_{16}$ to binary from binary

$$16 = 2^4$$

to octal

$$\begin{array}{r} B \cdot 2^3 + C \cdot 2^2 \\ 1011 \cdot 0010 = 1100 \\ 1100 = 14 \end{array}$$

$$1 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^0 = 15$$

$$1 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 = 15$$

$$= (B.2C)_{16}$$

$$= (15.214)_8$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

$$= (11.1787)_{10}$$

6. Simplify the following functions using K-map. 6marks

a) $f(A,B,C,D) = \Sigma m(3,4,6,8,9,12,14)$

b) $f(A,B,C,D) = \Sigma m(1,2,7,12,15) + d(5,9,10,11,13)$

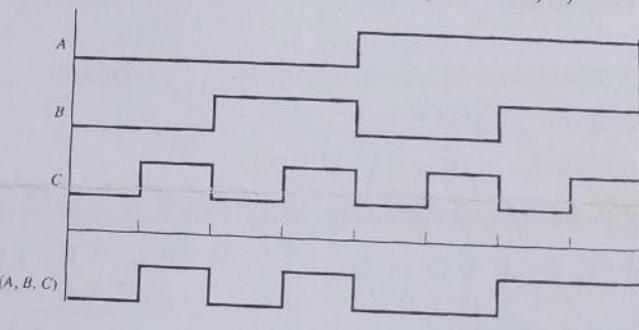
c) $f(A,B,C,D) = \Pi M(1,2,5,11,13,15)$

7. Given the timing diagram of a combinatory circuit represented in the figure below where the inputs are A, B, C and the output is $f(A,B,C)$.

a) Derive the truth table of the output $f(A,B,C)$. 3marks

b) Give the simplified expression of $f(A,B,C)$ using minterms. 2marks

c) Draw the logic network that realizes this function 3marks



a)

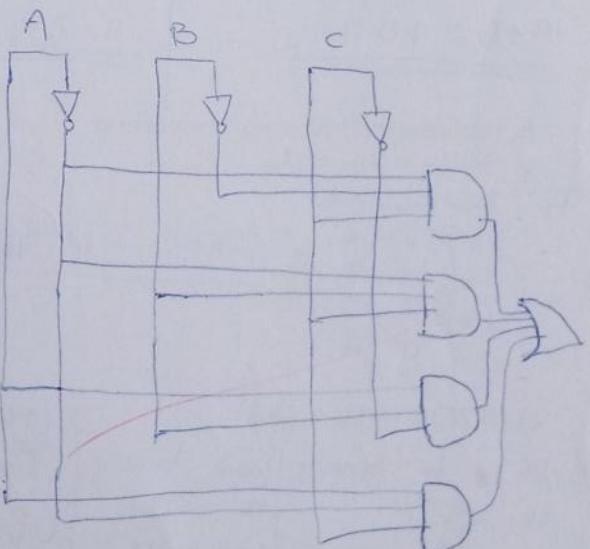
A	B	C	F
0	0	0	0
0	0	1	1
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	0
1	1	0	1
1	1	1	1

3

$(\bar{B} + \bar{B})$

c)

a



b)

$F = \bar{A}\bar{B}C + \bar{A}BC + ABC\bar{C} + ABC$

UNIVERSITY OF BUEA
COLLEGE OF TECHNOLOGY
SECOND SEMESTER EXAMINATION 2021/2022

DEPARTMENT: COMPUTER ENGINEERING	COURSE INSTRUCTOR(S): Dr Denis Nkweteyim
MONTH/YEAR: June 2022	COURSE CODE: CEC302
DATE: 15/06/2022	COURSE TITLE: Object-oriented Programming
TIME ALLOWED: 2 Hours (13:00-15:00)	
CREDIT VALUE: 4	Hall: U-Block E

INSTRUCTIONS: Answer Questions 1 and 2, and either Question 3 or Question 4. All code in Java. Indicate the questions you have answered in the spaces provided on the front cover of your answer booklet. **Start each question on a NEW page!**

Question 1 (15 + 7 = 22 marks)

- a) Write the letter that corresponds to the correct answer for each of the following questions.
- i) Assume `int[][] x = {{1,2},{3,4},{5,6},{4,3,6}}`, what are `x.length` and `x[3].length`?
 A 1 and 3 B 9 and 1 C 4 and 3 D 4 and 2
- ii) What is the connection between public classes and .java file names? (Assume the file contains no inner classes.)
 A The file can have at most one public class; if present, it must have the same name as the file
 B The file must have at least one public class and none of them can have the same name as the file
 C It is common practice to name a file after one of the public classes in it, but Java does not require it
 D If the file does not contain a public class, its name must not match the names of any of the classes in it.
- iii) _____ is invoked to create an object.
 A A constructor B The main method C A method with a return type D A method with no return type
- iv) What modifier should you use on a class so that any class in the same package can access it but a class in a different package cannot access it?
 A public B private C protected D Use the default modifier
- v) The default value for data field of a boolean type and numeric type is _____, respectively are
 A true, 1 B true, 0 C false, 1 D false, 0
- vi) Variables that are shared by every instance of a class are _____.
 A public variables B private variables C instance variables D class variables
- vii) Object-oriented programming allows you to derive new classes from existing classes. This is called _____.
 A encapsulation B inheritance C abstraction D composition
- viii) Choose the best answer from the options given below.
 A A subclass is a subset of a superclass.
 B A subclass is usually extended to contain more functions and more detailed information than its superclass.
 C "class A extends B" means B is a subclass of A D B and C are correct
- ix) Because of polymorphism, _____.
 A data fields should be declared private
 B a variable of supertype can refer to a subtype object
 C a class can extend another class
 D a class can contain another class
- x) What is the output of the code in Figure 1?
 A Same B SameEquals
 C Equals D Nothing displayed; code cannot compile
- xi) What is the output of the program in Figure 2?
 A 0 B 1 C 4 D 5

```
public class S {
    int x = 4;
    S() { x++; }
    public static void main (String args[]) {
        S s = new S(); System.out.println(s.x);
    }
}
```

Figure 2

```
String s1 = new String("My String");
String s2 = new String("My String");
if (s1 == s2)
    System.out.print("Same");
if (s1.equals(s2))
    System.out.print("Equals");
```

Figure 1

- xii) What is the output of the code in Figure 3?
 A 1 2 3 4 B 4 5 6 7
 C 2 5 9 13 D 3 6 10 14

```
public class Test {
    public static void main(String[] args) {
        int[][] matrix = {{1, 2, 3, 4},
                          {4, 5, 6, 7},
                          {8, 9, 10, 11},
                          {12, 13, 14, 15}};
        for (int i = 0; i < 4; i++)
            System.out.print(matrix[i][1] + " ");
    }
}
```

Figure 3

- Analyze the code in Figure 4, and answer the following three questions
- xiii) What will be displayed by the first `println` statement in the main method?
 A f2.i is 1 f2.s is 1 B f2.i is 1 f2.s is 2 C f2.i is 2 f2.s is 2
- xiv) What will be displayed by the second `println` statement in the main method?
 A f2.i is 1 f2.s is 1 B f2.i is 1 f2.s is 2 C f2.i is 2 f2.s is 2
- xv) What will be displayed by the third `println` statement in the main method?
 A f2.i is 1 f2.s is 1 B f2.i is 1 f2.s is 2 C f2.i is 2 f2.s is 2

- D f2.i is 2 f2.s is 1
 D f2.i is 2 f2.s is 1
 D f2.i is 2 f2.s is 1

```
public class Foo {
    int i;
    static int s;
    public static void main(String[] args) {
        Foo f1 = new Foo(); System.out.println("f1.i is " + f1.i + " f1.s is " + f1.s);
        Foo f2 = new Foo(); System.out.println("f2.i is " + f2.i + " f2.s is " + f2.s);
        Foo f3 = new Foo(); System.out.println("f3.i is " + f3.i + " f3.s is " + f3.s);
    }
    public Foo() {
        i++; s++;
    }
}
```

Figure 4

- b) Indicate which of the following statements are True or False. Write only the question number, followed by the word True or False
- A class in Java can implement multiple interfaces
 - A class constructor never executes its parent class constructor.
 - Private members of an object can be accessed by methods of another object if the two objects have “Is-A” relationship.
 - Given that `o1` and `o2` are two declared and initialised references to objects of the same class, the true value of the expression `o1.equals(o2)` always implies that `o1 == o2` also evaluates to true.
A class Animal has a subclass Mammal. Which of the following is/are true and which is/are false?
 - Because of single inheritance, Mammal can have no subclasses.
 - Because of single inheritance, Mammal can have no other parent than Animal.
 - Because of single inheritance, Animal can have only one subclass.

Question 2 (6 + 3 + 6 + 9 = 24 marks)

```
1 int N = arr.length;
2 double min = 0;
3 int minLocation=0;
4 for(int i = 1; i <= N; i++) {
5     if (arr[i] < min)
6         min = arr[i];
7     minLocation = i;
8 }
9 System.out.print("The minimal value is arr[");
10 System.out.println(minLocation + "] = " + min);
```

Figure 5

```
public class Test {
    public static void main(String[] args){
        A a = new A();
        a.print();
    }
}
class A {
    String s;
    A(String newS) {
        s = newS;
    }
    void print() {
        System.out.println(s);
    }
}
```

Figure 6

```
public class Mystery {
    public static void main(String[] args) {
        // Part 1
        int[] a = {0, 1, 2, 3, 4, 5};
        for (int i = 0; i < 6; i++)
            System.out.print(a[i/2] + " ");
        System.out.println();
        // Part 2
        for (int i = 5; i >= 0; i--)
            System.out.print(5 - a[a[i]] + " ");
        System.out.println();
        // Part 3
        for (int i = 0; i < 3; i++) {
            int t = a[i];
            a[i] = a[5-i];a[5-i] = t;
            System.out.print(a[i] + " ");
        }
        System.out.println(a[3]+ " " +a[4]+ " "+a[5]);
    }
}
```

Figure 7

	Expression	Type	Value
(i)	$(11/2) * 2.0$		
(ii)	$(11/2.0) * 2.0$		
(iii)	<code>!(false !true)</code>		
(iv)	<code>"2.1" + "2.4"</code>		
(v)	<code>1 + 2.2 + "1.1" + "(a)"</code>		
(vi)	<code>Float.parseFloat("123.5")</code>		

Figure 8

- a) Consider the code fragment in Figure 5 (with line numbers provided for convenience). The code is intended to examine an array of double values and print out the minimum value in the array and its location. You may assume that arr[] is an array of double values that has been properly declared and initialized. With the help of the line numbers provided in the code, identify the location, and in less than ten words in each case, state THREE bugs that are in the code. In each case, state whether the error will lead to compilation error, runtime error, or the error may only be noticed from the wrong results that the code produces.
- b) Analyze the code in Figure 6 and explain in not more than three lines, the problem with it.
- c) Examine the code fragment in Figure 7. How many lines of output will the code generate? Write the output
- d) Complete the table in Figure 8 with the type and value of each of the given expressions (6 marks)

Answer EITHER Question 3 or Question 4. If you answer both, only Question 3 will be graded

Question 3 ($[2+2+2+4+4+4] + 6 = 24$ marks)

- a) Write code to create class **Point**. Class **Point** represents a point in 3-dimensional space, with the following variables, constructors, and methods:
- Variables **x**, **y**, **z** to represent the coordinates of a point in space
 - A constructor that takes three parameters and uses them to initialize instance variables
 - A constructor that takes no parameter, and calls the 3-parameter constructor in (ii) with a value of 0 for each of the parameters
 - A method called **absVal()** that takes a single **Point** object and returns its absolute value
 - A method called **distance()** that takes one **Point** object, and computes and returns the distance from the origin using them using the formula $\sqrt{x^2 + y^2 + z^2}$
 - A method called **volume()** that computes and returns the volume of a box. The method takes the variables **x**, **y**, **z** as arguments, and returns the product of the **absolute values** of these three parameters
- b) Write a code fragment that:
- Creates two **Point** objects **p1** and **p2** with coordinates (2, 4, 3) and (-3, 3, 4) respectively
 - Calls the distance method and assigns the distance between **p1** and **p2** to an appropriately declared variable, **d**.

Notes:

- You should also apply the principle of code re-usability, i.e., do not write new code if there is existing code to do the same thing
- Make use of the **sqrt()** and **abs()** static methods of the **Math** class

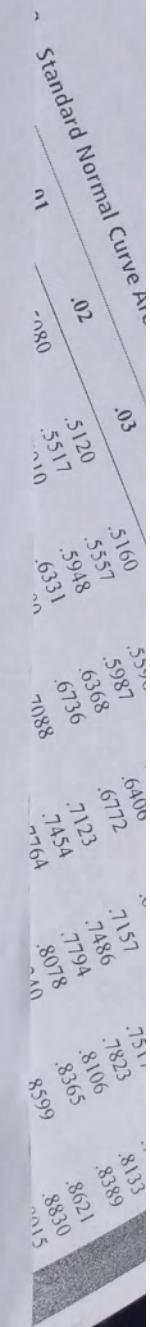
Question 4: (6 x 4 = 24 marks)

Figure 9 shows a number of classes and their properties.

- (a) Write code for to create class **Date**, including the following:
- One constructor to initialize instance variables
 - A **toString** method to print the date of the form d/m/y
- (b) Write code for class **Student** as follows:
- One constructor with 8 parameters: the first six to instantiate **bDate** and **aDate**, and the last two to initialize **stName** and **progName**
 - A **toString** method to return information on the instance variables. This method should get its Date information from Class Date.
- (c) Write code for class **UGStudent** as follows:
- One constructor with 9 parameters: the first eight as in (b), and the last one for the **minor**.
 - A **toString** method to return all information (including **minor**) about an UG student. This method should get its Student information from Class Student.
- (d) Write code for class **PGStudent** as follows:
- One constructor with 10 parameters: the first eight as in (b), and the last two for the **level** and **supervisor**
 - A **toString** method to return all information (including **level** and **supervisor**) about a PG student. This method should get its Student information from Class Student.
- (e) Write a code fragment to create an undergraduate student: Name: John Doe, programme: Computer Science, minor: Physics, birth date: 30 July 1995, admission date: 10 October 2015. Include in your code, a display of all we know about the student
- (f) Write a code fragment to create a graduate student: Name: Mary Doe, programme: Physics, level: MSc, supervisor: John Cox, birth date: 30 April 1993, admission date: 20 August 2014. Include in your code, a display of all we know about the student

Class	Properties
Date	d,m,y (all int)
Student	bDate and aDate (Date objects), stName and progName (String)
UGStudent	minor (String) plus all properties of class Student
PGStudent	level (String), supervisor (String) plus all properties of class Student

Figure 9



UNIVERSITY OF BUEA

COLLEGE OF TECHNOLOGY

DEPARTMENT:

COURSE INSTRUCTOR: Moses Minang

MONTH: JUNE

COURSE CODE & NUMBER: COT308

YEAR: 2021

COURSE TITLE: Technical writing

TIME ALLOWED: 2 Hours

CREDIT VALUE:

INSTRUCTION: Answer ALL questions

1. Study the following passage and answer the questions that follow.

1. Marrying while still teenagers can be a bad decision, creating many problems for young couples. 2. First when teens marry in or just out of high school, their relations often change drastically. 3. Instead of spending time with their individual former friends, newly weds often find that their spouse does not like some or all of the other's friends, so the husband or wife has to choose --- "them or me." 4. Even when the old friends are accepted, many times friendships die out because a married couple's interests can be so different from a single person's. 5. While some young couples continue to go to the same parties, concerts and vacation spots, many more find themselves having to try to have fun with each other's in-laws instead. 6. As years pass, another problem begins as young couple's often find themselves becoming increasingly cut off from the rest of life and dependent on one another. 7. They have already been seeing less of old friends, many of whom are off at college or trade school, or simply doing other things, but after that first baby arrives, the young couple's life become really hard.

- Which sentence in the above writing do you think would be the thesis sentence? (2 mks)
- What do you think is the main idea in this passage? (2 mks)
- What one thing makes life quite challenging for couples to associate with friends. (2 mks)
- What age range gives one qualification as a teenager. (1) (2 mks)
- What is likely to end relationships between the married and their unmarried friends? (2 mks)
- List five words in the text that shows cohesion. (5 mks)
- What words do *their* in Sentence 2, *their*, *them*, *me* in sentence 3, themselves in sentence 6, they and whom in sentence 7 refer to? Use a simple table to represent

Pronouns	Antecedent
Their	Name of the word referred to e.g. school children

vi. Summarize this passage in at most 30 words. (10 mks)

2. Say whether each of the following statements is true or false. (10 mks)

- If you quote from a book or article, you must include the date of publication and page.
- If you summarize material from an article, you need to include the reference.
- If you can't get the source of information to reference it, it is generally preferable to leave the information out.
- Using an author's ideas without referencing is plagiarism.
- Peer editing is a useful way to make your report better before submission.
- The topic sentence should appear at the beginning of a paragraph.
- Transitional expressions are not important in achieving paragraph unity.
- Transitional expressions help a writer in achieving cohesion.
- A conclusion must only be a summary of an essay.
- The thesis sentence is best placed in the first paragraph of an essay.
- The passive voice could also be used in technical writing.

3. Provide a word that best represents each statement below.

- The least number of meeting members required for a binding decision to be taken.
- A final decision taken at meeting sessions.
- The process that involves regularizing minutes of a precious meeting.
- The technical word used for the list of issues to be handled during a meeting.
- A strongly worded statement that is used to counter a discussion or a point of view.

Write on any of the following: (20 mks)

- You have completed a project in your area of specialization. Write a technical report to the sponsors of the project. (20 mks)
- Your company has just ended a meeting held to discuss the construction of a Village Solar Energy Station. Develop the minutes of that meeting. (20 mks)

Department of Electrical & Electronics Engineering
Second Semester Examination 2021/2022

Course: Probability & Statistics

Course code: EEC 338

Credit Value: 3 Duration: 2 h

Instructors: TAKEMBO (L)/ NANA (AP)

Instruction: Answer All Questions

1. In a communication system the signal sent from point X to point Y arrives by two paths in parallel. Over each path the signal passes through two repeaters (in series). Each repeater in one path has a probability of failing (becoming an open circuit) of 0.005. This probability is 0.008 for each repeater on the other path. All repeaters fail independently of each other.
 - (a) Make a sketch of the communication network **1mk**
 - (b) State the condition necessary for the signal not to arrive at point Y. **1mk**
 - (c) Hence find the probability that the signal will not arrive at point Y. **2mks**

2. A random variable X can have values -4, -1, 2, 3, and 4, each with probability $\frac{1}{5}$
 - (a) Is the random variable X discrete, continuous or mixed? Justify your answer **2mks**
 - (b) Find: the density function f_Y , the distribution function F_Y , the mean μ_Y , and the variance σ_Y^2 , of the random $Y=3X^3$ **7mks**

3. The lifetime of a system expressed in weeks is a Rayleigh random variable with probability density function given by:

$$f(x) = \begin{cases} kxe^{-\frac{x^2}{400}} & x \geq 0 \\ 0 & x < 0, \end{cases}$$
 - (a) Show that $k = \frac{1}{200}$, given that $f(x)$ is legitimate. **2mks**
 - (b) What is the probability that the system will not last a full week? What is the corresponding probability that the system lifetime will exceed a full week? **3mks**

4. Suppose the current measurements in a strip of wire are assumed to follow a normal distribution with a mean of 10 milliamperes and a variance of 4 (milliamperes)².
 - (a) What is the probability that a measurement will exceed 13 milliamperes? **2mks**
 - (b) What is the probability that a measurement will between 9 and 11 milliamperes? **2mks**

5. A bank operates both a drive-up facility and a walk-up window. On a randomly selected day, let X = the proportion of time that the drive-up facility is in use (at least one customer is being served or waiting to be served) and Y = the proportion of the time that the walk-up window is in use. Then the set of possible values for (X, Y) is the rectangle

$$D = \{(x, y): 0 \leq x \leq 1, 0 \leq y \leq 1\}.$$
 Suppose the joint probability density function of (X, Y) is given by : $f_{X,Y} = \begin{cases} \frac{6}{5}(x + y^2) & 0 \leq x \leq 1, 0 \leq y \leq 1 \\ 0 & \text{Otherwise} \end{cases}$
 - (a) Show that $f_{X,Y}$ is legitimate **2mks**
 - (b) Find the probability that neither facility is busy more than one-quarter of the time. **2mks**
 - (c) Find f_X and f_Y , the marginal probability density function of X and Y respectively. **2mks**
 - (d) Construct the conditional probability density function of Y given that X=0.8. **2mks**
 - (e) Evaluate the probability that the walk-up facility is busy at most half of the time given that X=0.8 **2mks**
 - (f) Calculate the expected proportion of the time that the walk-up facility is busy given that X=0.8 **2mks**

UNIVERSITY OF BUEA**COLLEGE OF TECHNOLOGY****SECOND-SEMESTER EXAM**

MONTH: June

YEAR: 2022

TIME ALLOWED: 2 hours

INSTRUCTION: Answer All questions

COURSE INSTRUCTORS: Dr TCHAGNA / Dr. MELINGUI

COURSE TITLE: Introduction to Mobile App Dev

COURSE CODE: CEC318

CREDIT VALUE: 4

Part I: Comprehensive Questions (40pts)**Exercise 1: MCQ (10pts)**

1. Android Architecture is made up of how many key components?
a. 3 b. 4 c. 5 d. 6
2. What is AAPT?
a) Android Asset Packaging Terminal
b) Android Asset Packaging Tool
c) Android Actif Packaging Terminal.
d) Android Actif Packaging Tool.
3. What is the use of an *activityCreator*?
a) is the first step towards the creation of a new Android project.
b) It is made up of a shell script that will be used to create new file system
c) a and b is true
d) a and b is false
4. What are the four essential states of an activity?
a) Active-Paused-Stopped-Destroyed
b) Active-paused-Sleeped-Destroyed
c) Active-Stopped-Sleeped-Destroyed
d) Active-paused-Sleeped-Stopped
5. What items are not important in every Android project?
a) AndroidManifest.xml
b) build.xml
c) assets/
d) lib/

Exercise 2: STRUCTURED QUESTIONS (30pts)

1. What are the types of flags to run an application in android? (3pts)
2. What language is supported by Android for application development? (3pts)
3. How do you create a widget that looks different in iOS and Android in flutter? (5pts)
4. How do you make HTTP requests in Flutter? (4pts)
5. Explain the rule of each these method in the lifecycle of a 'StatefulWidget' in flutter.
(15pts)

Methods	rule
createState()	

initState()	
didChangeDependencies()	
build()	
didUpdateWidget()	
deactivate()	
dispose()	

Part II: Practical part (30pts)

Choose one of these projects and briefly describe how you can build a native mobile application by using flutter

1. Trip Planner Application (custom itinerary)

Common tourist trails are of little interest to many people nowadays. At the same time, many travelers who have had fascinating travel experiences will be eager to share them with others. The idea for this mobile app is to create a database featuring travel itineraries, or just walks, that are explained by the users themselves.

2. City Guide

It is no problem at all to find a good city guide app for megacities. However, for smaller cities and towns, it can become a real challenge. You can easily create such a product by finding and systemizing the necessary reference data and making a dedicated mobile app out of it. Many users will surely take advantage of this app to access all the necessary data about their city in one place.

3. Brand Identifier Application

This brand identifier app will allow users to learn more about a specific brand or product. By scanning the logo or tag of the item, the mobile app will list articles, information, and news about the manufacturer as well as about the product. In the case of clothing items, it will also tell the users whether it is authentic or not.

4. AR for School Application

This app facilitates the illustration of complex materials taught in classes such as Chemistry or Biology. By applying Augmented Reality technology, the app aims to help students visualize and better understand complex subjects.

5. Smart Cooking Application

The idea behind this application is that the users enter the ingredients they have in their kitchen. Then, the mobile app will give them a list of recipes they can use to make food from the available resources. This app could help its users to come up with some great cooking ideas that they mightn't have done before.

6. Scientific calculator app

A scientific calculator is a type of electronic calculator, usually but not always handheld, designed to calculate problems in science, engineering, and mathematics. They have completely replaced slide rules in traditional applications, and are widely used in both education and professional settings.

COLLEGE OF TECHNOLOGY
CONTINOUS ASSESSMENT

DEPARTMENT: Computer Engineering Technology

COURSE INSTRUCTOR: Mr. Nyanga B.

MONTH: APRIL

COURSE CODE & NUMBER: CEC306

YEAR: 2022

COURSE TITLE: SYSTEM ANALYSIS AND DESIGN

DATE: 22/04/2022 TIME: 07:30-08:15

CREDIT VALUE: 4

TIME ALLOWED: 45 MINS

INSTRUCTIONS: Read through EACH question before you answer it. Follow instructions for EACH Section. Time is allocated for a MAXIMUM POSSIBLE MARK of 22. DIAGRAMS assumed to be in Standard UML/VP. State any assumptions made. Penalty for poor English or poor presentation of work.

Q. 1 is an important factor of management information system.

- A) System B) Data C) Process D) All

Q.2 Which are the following is / are the level(s) of documentation?

- A) Documentation for management B) Documentation for user
C) Documentation for data processing department D) All of the above

Q.3 level supply information to strategic tier for the use of top management.

- A) Operational B) Environmental C) Competitive D) Tactical

Q.4 In a DFD external entities are represented by a

- A) Rectangle B) Ellipse C) Diamond shaped box D) Circle

Q.5 can be defined as data that has been processed into a form that is meaningful to the recipient and is of real or perceived value in current or prospective decisions.

- A) System B) Information C) Technology D) Service

Q.6 Use the new system at the same time as the old system to compare the results. This is known as ...

- A) Procedure Writing B) Simultaneous processing C) Parallel Operation D) File Conversion

Q.7 A data flow can

- A) Only emanate from an external entity B) Only terminate in an external entity

C) May emanate and terminate in an external entity

D) May either emanate or terminate in an external entity but not both

Q.8 can be defined as most recent and perhaps the most comprehensive technique for solving computer problems.

- A) System Analysis B) System Data C) System Procedure D) System Record

Q.9 SDLC stands for

- A) System Development Life Cycle B) Structure Design Life Cycle

C) System Design Life Cycle D) Structure development Life Cycle

Q.10 includes review of the existing procedures and information flow.

- A) Feasibility Study B) Feasibility report C) System Design D) System analysis

Q.11 A rectangle in a DFD represents

- A) a process B) a data store C) an external entity D) an input unit

Q.12 refers to the collection of information pertinent to systems Project.

- A) Data transfer B) Data gathering C) Data Embedding D) Data Request

Q.13 means coordinated effort, to communicate the information of the system written

- A) System documentation B) Resource required C) Development schedule D) User Document

Q.14 External Entities may be a

- A) Source of input data only B) Source of input data or destination of results

C) Destination of results only D) Repository of data

Q.15 is a group of interested components working together towards a common goal by accepting inputs and producing outputs in an organized transformation process.

- A) System B) Network C) Team D) System Unit

Q.16 To create vehicle of information to provide evidence in the development process and to monitor the process. This is one of the objectives of

- A) Analysis B) Design C) Development D) Documentation

Q.17 A System is no more than idea

- A) Conceptual B) Logical C) Physical D) All of the above

Q.18 By an external entity we mean a

A) Unit outside the system being designed which can be controlled by an analyst.

B) Unit outside the system whose behavior is independent of the system being designed

C) A unit external to the system being designed D) A unit which is not part of a DFD

Q. 19 Data store in a DFD represents.

A) a sequential file B) a disk store C) a repository of data D) a random access memory

Q.20 is a good example of deterministic system.

A) Life cycle B) Computer Program C) Software Program D) None of the above

Q.21 The main ingredient of the report documenting the is the cost benefit analysis.

A) System Analysis B) Feasibility Study C) System Analyst D) System Design

Q.22 A data flow can

A) Only a data store B) Only leaves a data store

C) Enter or leave a data Store D) Either enter or leave a data store but not both

LEVELS: 3
MONTH: April
OPTIONS: Software Engineering & Networking
DATE: 30/04/2022
TIME: 10:00 a.m. – 11:00 a.m.

UNIVERSITY OF BUEA
COLLEGE OF TECHNOLOGY
DEPARTMENT OF COMPUTER
ENGINEERING
SECOND SEMESTER CA

COURSE FACILITATOR:
Kometa Denis
COURSE CODE: CEC320
COURSE TITLE:
Embedded Systems I
TIME ALLOWED: 1 Hour;

Instructions:

- This is a **CLOSED BOOK CA** (No document or device is authorised)
- Answer All questions. Be certain to read the questions carefully before responding
- Important: Unless explicitly stated otherwise, justify your answer carefully!! Answers without justification do not give any credits. The questions are weighted differently
- Any form of fraud will be penalised accordingly. Should you copy, quote your sources-Academic Integrity

Question I: 5 Points

- i. Differentiate among embedded systems, real-time embedded systems and desktop computers.
- ii. Give the characteristics of a real time embedded system.
- iii. Using a diagram, explain the architecture of an embedded system.

Question II: 5 Points

- i. Differentiate between the specification of a typical memory and the memory of a real time embedded system.
- ii. Using the specifications of the memory of a real time embedded system, discuss the following memories: OTP ROM, EEPROM, EPROM, Flash Memory.
- iii. Differentiate between SRAM and DRAM; which one is mostly used in embedded systems?

Question III: 5 Points

- i. Briefly describe signal processing.
- ii. Differentiate between microprocessor and microcontrollers.
- iii. Discuss the different types of microcontrollers looking at the following elements: Memory Architecture, Instruction Set, Bus Width, Memory.

Good Luck!
(Lăوش)

UNIVERSITY OF BUEA
COLLEGE OF TECHNOLOGY
DEPARTMENT OF COMPUTER ENGINEERING
SECOND SEMESTER EXAMINATION

LEVELS: 300
DATE: 06/06/2022
TIME: 10:00 - 12:00
TIME ALLOWED: 2 Hours

OPTIONS CONCERNED:
 Networking, Software Engineering
ACADEMIC YEAR: 2021/2022

COURSE FACILITATORS:
 Dr Njitacke Zelic/Kometa Denis
COURSE CODE: CEC320
COURSE TITLE:
 Embedded Systems I
DEGREE LEVEL: Bachelor

Instructions:

- * This is a **CLOSED BOOK** Examination (No document or device is authorised)
- * Answer All questions. Be certain to read the questions carefully before responding.
- * Important: Unless explicitly stated otherwise, justify your answer carefully!! Answers without justification do not give any credits. The questions are weighted differently
- * Any form of fraud will be penalised accordingly. Should you copy, quote your sources-Academic Integrity

Question I: Course Work - 30 Points

1. Using a diagram, explain the architecture of an RTES by discussing the function of the various blocks.
2. Write 5 advantages and 5 disadvantages of embodiment.
3. Give at least 5 examples of embedded systems you are using/watching in your day-to-day life.
4. Enumerate the similarities and differences between the μ C and DSP.
5. List at least 4 differences between the I/O devices for a RTES and a Desktop PC.
6. Highlight on different modes of DMA data transfer; which mode consumes the least power and; which mode is the fastest?
7. Elaborate on interrupts and interrupts priorities.
8. Discuss the importance of interfacing in embedded systems, looking at: addressing, arbitration and protocol.
9. Discuss about the HDD housed in your PC; is it an RTES and why?
10. Briefly discuss signal processing and the different types of cache mappings.

Question II: Semi-Applied Knowledge - 20 Points

1. Discuss 5 types of microcontrollers looking at the following elements: Memory Architecture, Instruction Set, Bus Width, Memory.
2. Using two architectural diagrams, explain how the Priority and the Daisy Chain Arbitration work.
3. Using diagrams distinguish between Recipient Type A and B of the USB and using a table, present the pins, signals and colours of the wires.
4. A computer system has three devices whose characteristics are summarized in the following table:

Device	Service Time	Interrupt Frequency	Allowable Latency
D1	150 μ s	1/(800 μ s)	50 μ s
D2	50 μ s	1/(1000 μ s)	50 μ s
D3	100 μ s	1/(800 μ s)	100 μ s

Service time indicates how long it takes to run the interrupt handler for each device. The maximum time allowed to elapse between an interrupt request and the start of the interrupt handler is indicated by allowable latency. If a program P takes 100 seconds to execute when interrupts are disabled, how long will P take to run when interrupts are enabled?

Question III: Applied Knowledge - 20 Points

Problem: Topic-Design of a Water Level Detector

The system provided in Figure 2 is a tested Arduino project that uses 3 sensor probes as a water level indicator with 3 LEDs and one LCD display and a simple controller that turns off a motor when the water has reached the desired level (the highest in our case). The green LED is associated with the high level, the yellow one with the average level, and the red LED with the low level. When the water in the tank is empty, or at an average level, the motor provided to pump the water in the tank is ON. When the water level in the tank is at its highest level, the motor is off.

1. Identify the Arduino pins configured as INPUT (1 Point).
2. Write a short program which enables one to configure these pins as INPUT (3 Points).
3. Apart from the screen pins, identify the Arduino pins configured as OUTPUT (1 Point).
4. Write the program which enables us to configure these pins as OUTPUT (3 Points).
5. Give the role of resistors R7, R8, R9 (1 Point).
6. Propose values for resistors: R7, R8, R9 which will enable the LEDS to shine (3 Points).
7. Identify the type of screen used in the circuit shown in Figure 2 (1 Point).
8. Complete the program below in order to enable the circuit of shown in Figure 2 to work (7 Points).

```
#include <LiquidCrystal.h>
LiquidCrystal lcd(7, 6, 5, 4, 3, 2);
void setup() {
}
void loop() {
```

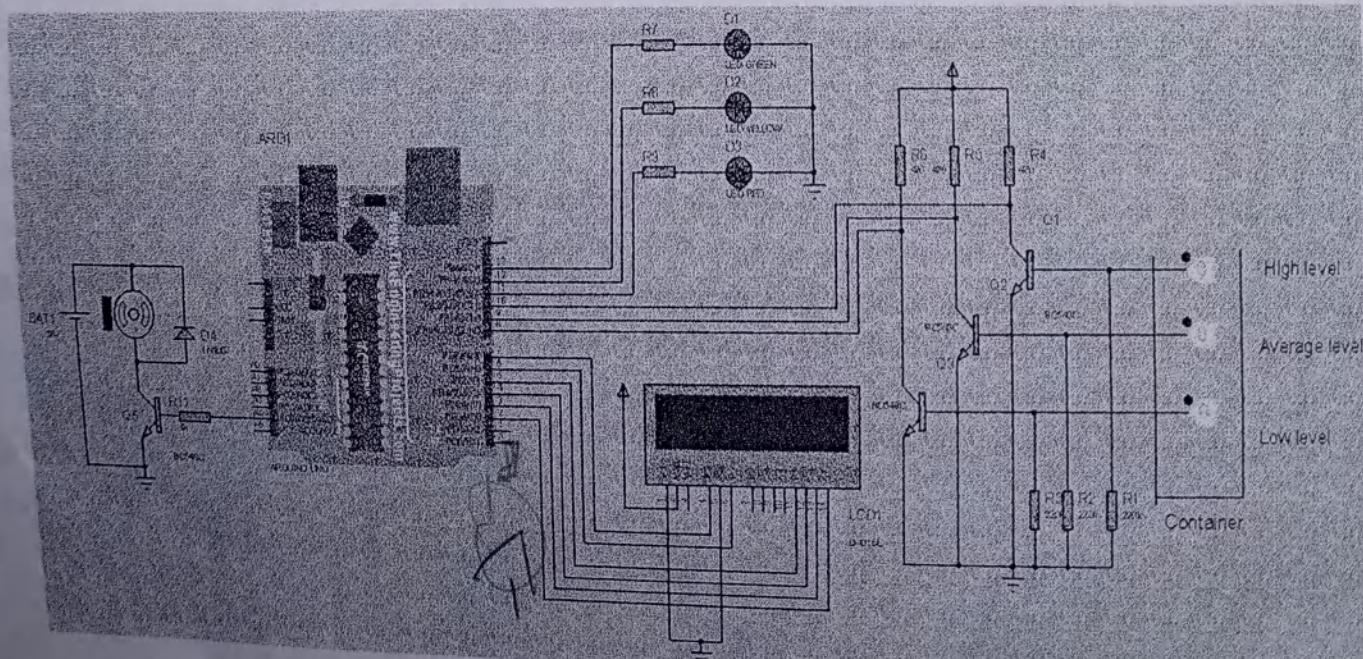


Figure 2: Water Level Detector Circuit.

Good Luck!

QUESTION 1 (25 marks)

ECDH

- Public/ private key pairs:
 $(a; P_A = a.B)$
 $(b; P_B = b.B)$
 where $B = \text{basis point}$
- Shared secret
 $K_{ab} = abB$
- Encryption
 $P_c = [kB], (P_M + kK_{ab})]$
 where $k = \text{integer}$ and P_M is
 point on curve
- Decryption
 $(P_M + kK_{ab}) - [b.(kB)]$

ECDSA

- KEY GENERATION
 A selects a random integer d as the private key, and publishes $Q = dB$ as the public key
- SIGNING
 - Select a random integer k ;
 Compute $kB = (x_1, y_1)$ and $r = x_1 \bmod n$;
 - Compute $k^{-1} \bmod n$;
 - Compute $h(m)$, where h is a hash function of m ;
 - Compute $s = k^{-1}\{h(m) + dr\} \bmod n$.
 (r, s) is A 's signature of message m .

Use the algorithms above and the following parameters to answer the questions below:

- elliptic curve $y^2 = x^3 + 3x + 8 \bmod 13$ with the following complete addition table

	\mathcal{O}	(1, 5)	(1, 8)	(2, 3)	(2, 10)	(9, 6)	(9, 7)	(12, 2)	(12, 11)
\mathcal{O}	\mathcal{O}	(1, 5)	(1, 8)	(2, 3)	(2, 10)	(9, 6)	(9, 7)	(12, 2)	(12, 11)
(1, 5)	(1, 5)	(2, 10)	\mathcal{O}	(1, 8)	(9, 7)	(2, 3)	(12, 2)	(12, 11)	(9, 6)
(1, 8)	(1, 8)	\mathcal{O}	(2, 3)	(9, 6)	(1, 5)	(12, 11)	(2, 10)	(9, 7)	(12, 2)
(2, 3)	(2, 3)	(1, 8)	(9, 6)	(12, 11)	\mathcal{O}	(12, 2)	(1, 5)	(2, 10)	(9, 7)
(2, 10)	(2, 10)	(9, 7)	(1, 5)	\mathcal{O}	(12, 2)	(1, 8)	(12, 11)	(9, 6)	(2, 3)
(9, 6)	(9, 6)	(2, 3)	(12, 11)	(12, 2)	(1, 8)	(9, 7)	\mathcal{O}	(1, 5)	(2, 10)
(9, 7)	(9, 7)	(12, 2)	(2, 10)	(1, 5)	(12, 11)	\mathcal{O}	(9, 6)	(2, 3)	(1, 8)
(12, 2)	(12, 2)	(12, 11)	(9, 7)	(2, 10)	(9, 6)	(1, 5)	(2, 3)	(1, 8)	\mathcal{O}
(12, 11)	(12, 11)	(9, 6)	(12, 2)	(9, 7)	(2, 3)	(2, 10)	(1, 8)	\mathcal{O}	(1, 5)

- Pairing table is as follows

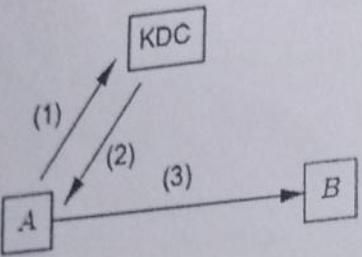
Point	(1,5)	(1,8)	(2,3)	(2,10)	(9,6)	(9,7)	(12,2)	(12,11)
Word	RAM	SAW	CUT	MET	SIR	YOU	CUP	DOT

- Let $a = 2$; $b = 3$; $k = 5$, $d = 4$, $B = (1,5)$ and $h(m)$ could be computed from $m = 00111011101$ using Initialization vector, $IV = 101$

- Encrypt and decrypt the word CUP (6+6 marks)
- Establish the digital signature of the word RAM (13 marks)

QUESTION 2 (25 marks)

- A) Kerberos is an authentication service designed to allow clients to access application servers in a secure manner over a network. The diagram below depicts the Kerberos authentication service where A is the client, B is the application server and KDC is the key distribution centre.



- Briefly explain (1), (2) and (3)
 - State the contents of the Kerberos ticket from the key distribution centre (KDC)
 - State the contents of the Kerberos authenticator from the client to the application server.
 - Use the information below to explain how the application server uses the contents of the ticket and authenticator to authenticate the client
- Let private keys $K_A = \{3, 2, 0, 1, 7, 6, 5, 4\}$ and $K_B = \{7, 6, 5, 4, 3, 2, 1, 0\}$
 - Let the session key, $K = \{6, 3, 4, 0, 1, 2, 7, 5\}$
 - Keys are mapped to decimal equivalents in the keyspace. Let the mapping of the session key, K correspond to decimal 2 which is 010.
 - Let the entities identities be $A = 011$ and $B = 101$

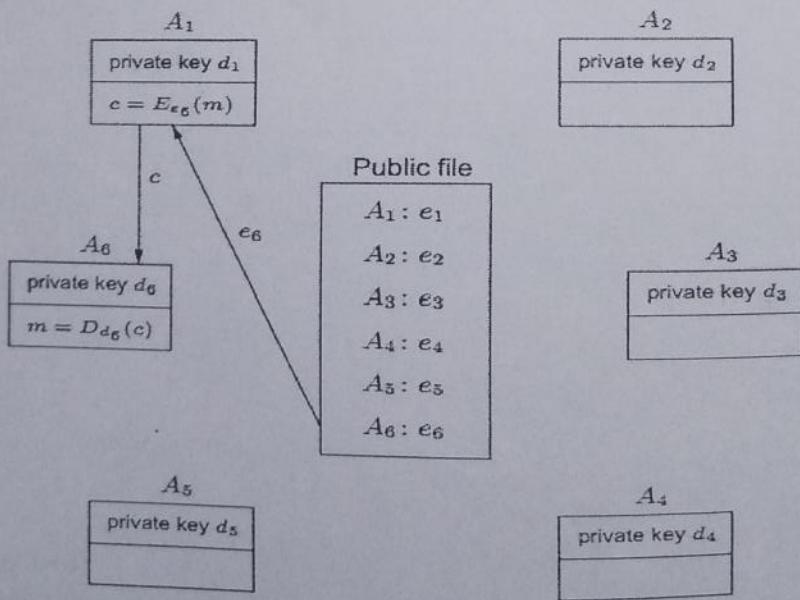
(13 marks)

- B) Suppose node A_1 wishes to send the plaintext PETER with its decimal equivalent equal to 21 to node A_6 using the RSA algorithm. Use figure below and the following data

primes $p = 11$; $q = 5$ and $e_6 = 27$

to answer the following questions

- Compute the ciphertext received by A_6
- Show how A_6 decrypts message PETER
- Assume an active attacker eavesdrop on A_6 public key. Implement a countermeasure to circumvent the attack.



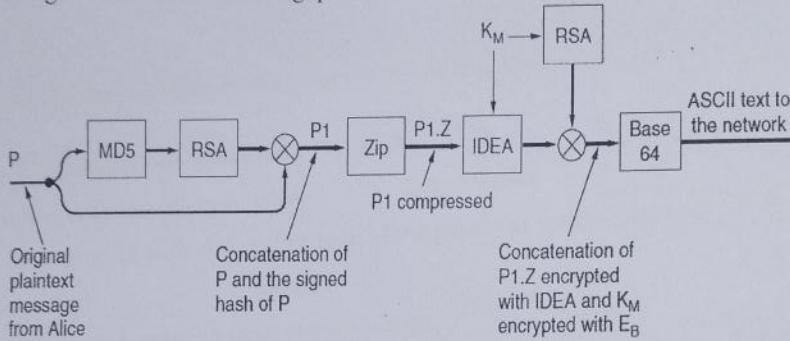
(12 marks)

QUESTION 3 (25 marks)

A) Use a block diagram to briefly explain the fixed DES-encrypted password algorithm. (4 marks)

B) The strength of a password could be estimated from its entropy. Assuming that all the passwords are equally probable, show that the password formed using 6 lowercase characters is weaker compared to a password formed using 5 mixed (lowercase & uppercase) alphanumeric characters (5 marks)

C) Use the block diagram of the PGP (Pretty Good Privacy) which is a complete email security package to answer the following questions



i) State two advantages to hash the plaintext using MD5 algorithm before RSA signing?

ii) Use the following values to implement the two RSA schemes shown in figure above

- Alice private parameters: p = 5; q = 11; d = 7
- Bob private parameters: p = 13; q = 7; d = 3
- Output of MD5 algorithm, hash of plaintext, h = 10
- Session key, K_M = 23

(8 marks)

D) Distinguish between entity authentication and message authentication code

Use the following artificial parameters to implement the Hashed Message Authentication Code (HMAC)

- Message to be hashed, m = 10010100110100011010
- Message is divided into blocks of 8 bits
- Shared secret key, K is a 4-bit word: K = 0101
- Initialization vector, IV = 01010011
- First pass key, i_pad key. Final key, K1 is obtained with two repetitions of 0111.
- Second pass key, o_pad key. Final key, K2 is obtained with two repetitions of 1101.

(8 marks)

MONTH: June	UNIVERSITY OF BUEA
YEAR: 2022	COLLEGE OF TECHNOLOGY
DATE: 10/06/2022	SECOND SEMESTER EXAMINATIONS
TIME ALLOWED: 2H	COURSE INSTRUCTOR: FEUDJIO
	COURSE CODE & NUMBER: EEC330
	COURSE TITLE: Basics of Digital Electronic
	TIME: 15:30 – 17:30

SECTION I: Comprehensive questions 15 marks

1. Define: Base, Number system, truth table. 1x3=3marks
2. Name four logic gates of your choice. For each of them draw its symbol, the truth table, and give its output equation. 8marks
3. What is the difference between a latch and a flip-flop. 2marks
4. Draw the logic symbol and the truth table of a flip-flop of your choice. 2marks

SECTION II: Number Systems 10 marks

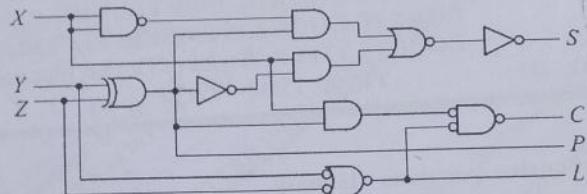
1. Calculate A+B; A-B; A×B for the following pair of binary numbers 1101011 and 1010 4marks
2. Convert each of the following hexadecimal numbers to binary, octal and decimal using the most appropriate conversion method. a) 4F b) F8.A7 c) ABC d) 201.4 4marks
3. Give the two's complement of the following binary numbers 2marks

00100011; 00010010

SECTION III: Switching functions and simplification 25 marks

- 1) Prove the following equalities by using Boolean algebra 2x2marks=4marks
 - a) $A + BC = (A + B)(A + C)$
 - b) $(AB + C)B = ABC + \bar{A}BC + ABC$
- 2) Using Boolean algebra, simplify the following expressions as much as possible. 3x2mars=6marks
 - a) $F = AB + AC + \bar{A}B + B\bar{C}$
 - b) $F = A\bar{B} + \overline{\bar{A}C + \bar{B}C}$
- 3) Find the minimized SOP form for the following functions using K-map 5marks
 - a) $f_1(A,B,C) = \sum m(3, 6, 7)$,
 - b) $f_2(A,B,C,D) = \sum m(1, 3, 6, 7) + d(4, 9, 11)$
 - c) $f_3(A,B,C,D) = \prod M(1, 2, 5, 11, 13, 15)$

4) Given the circuit diagram shown in the figure below



a) Write the logic expressions of S, C, P, and L. **4x2marks=8marks**

b) What is the function of this circuit if S and C are treated as outputs? **2marks**

SECTION IV: Problem analysis: 20 marks

1. We want to design a decimal-to-BCD encoder. Assume that each decimal digit (0 through 9) is represented by a switch which when closed is interpreted as logic 1 and when open is interpreted as logic 0.

a) How many inputs and outputs are necessary for the design of this encoder? **1mark**

b) Draw the truth table for each of the output **3marks**

c) Determine the minterm list for each output. **3marks**

d) Draw the logic network for this encoder. **3marks**

2. Design of a full adder logic circuit that takes at its inputs two bits A, B plus a carry bit C_{n-1} and produces at its output a sum bit S_n and a carry bit C_n

a) Draw the truth table **3marks**

b) Use K-map to express in POS form the output functions **3marks**

c) Draw the logic circuit of this full adder **4marks**

INSTRUCTIONS: Read through EACH questions before you start answering. Attempt ALL questions. Time allocated for a MAXIMUM POSSIBLE MARK of 70 (= 19 + 40). Penalty for poor English or poor presentation of work.

For Question SECTION WRITE DOWN THE LETTER WITH THE CORRECT ANSWER.

1. What are the four principles of Object-Orientation?
 - a. Abstraction, encapsulation, polymorphism, modularity
 - b. Abstraction, polymorphism, modularity, hierarchy
 - c. Encapsulation, polymorphism, hierarchy, modularity
 - d. Abstraction, encapsulation, modularity, hierarchy
2. The UML is a language for ...
 - a. Visualizing, specifying, constructing, documenting the artefacts of a software system
 - b. Visualizing, modeling, constructing, documenting the artefacts of a software system
 - c. Visualizing, documenting, modeling, encapsulating the artefacts of a software system
 - d. Visualizing, modeling, constructing, encapsulating the artefacts of a software system
3. Which of the following is NOT a characteristic of an object?
 - a. Identity
 - b. Behaviour
 - c. Action
 - d. State
4. Encapsulation is also known as ...
 - a. Information hiding
 - b. Interface management
 - c. Polymorphism
 - d. Aggregation
5. A class is a description of a set of objects that share the same ...
 - a. Attributes, behaviour and operations
 - b. Identity, behaviour and state
 - c. Attributes, operations and relationships
 - d. Relationships, operations and multiplicity
6. Data by itself is not useful unless
 - (a) It is massive
 - (b) It is processed to obtain information
 - (c) It is collected from diverse sources
 - (d) It is properly stated
7. In motor car manufacturing the following type of information is operational
 - (a) Decision on introducing a new model
 - (b) Scheduling production
 - (c) Assessing competitor car
 - (d) Computing sales tax collected
8. Operational information is
 - (a) Haphazard
 - (b) Well organized
 - (c) Unstructured
 - (d) Partly structured
9. Data mining is used to aid in
 - (a) operational management
 - (b) analyzing past decision made by managers
 - (c) detecting patterns in operational data
 - (d) retrieving archival data
10. Decision support systems are essential for
 - (a) day-to-day operation of an organization.
 - (b) providing statutory information.
 - (c) top level strategic decision making.
 - (d) ensuring that organizations are profitable.
11. It is necessary to consult the following while drawing up requirement specification
 - a) only top managers
 - b) only top and middle management
 - c) only top, middle and operational managers
 - d) top, middle and operational managers and also all who will use the system
12. Feasibility study is carried out by
 - a) managers of the organization
 - b) system analyst in consultation with managers of the organization
 - c) users of the proposed system
 - d) systems designers in consultation with the prospective users of the system
13. Hardware study is carried out
 - a) after the final system is specified
 - b) at the requirements specification stage
 - c) before the requirements are specified
 - d) whenever management decides it is necessary
14. Systems are modified whenever
 - a) user's requirements change
 - b) new computers are introduced in the market
 - c) new software tools become available in the market
 - d) other similar organization modify these system
15. The main objective of system modification is

- a) to use the latest software tools b) to meet the user's new/changed needs
c) to use the latest hardware d) to have the most modern system
16. Information is gathered by a system analyst in order to
a) find out whether a computer based system is required b) find out how the organization works
c) find out how the current system works and what is expected from a new computer based system
d) find out who will use the system
17. Gathering information in large and complex organizations is difficult and takes time because
i) it is necessary to consult a large number of persons at various levels of hierarchy in the organization
ii) one has to examine the current system in detail iii) a clear strategy has to be evolved to gather information
iv) it is necessary to use an information flow model of an organization
a) i and iii b) iii and iv c) i and ii d) ii and iv
18. A strategy to gather information consists of
i) identifying information sources ii) using information flow model of organization
iii) examining systems of other organizations iv) rely on ones experience
a) i and ii b) i and iii c) ii and iv d) ii and iii
19. In order to get fast response when questionnaires are sent
i) the questionnaire must be simple to answer ii) the questionnaire should be comprehensive
iii) the questionnaire should be short iv) the questionnaire should be long
a) i, ii b) ii, iv c) i, iii d) i, iv
20. The purpose of designing an information system is to
a) modernize the functioning of an organization b) reduce the number of people employed by an organization
c) provide operational, tactical and strategic information to efficiently manage an organization
d) improve the day-to-day working of an organization
21. The expansion of SRS is
a) System Requirements Specification (b) System Resources Statement
(c) Statement of Reliability of System (d) Standard Requirements Statement
22. Graphical tools used to arrive at SRS are:
(i) Data Flow Diagrams (ii) Program Flow Charts (iii) System Flow Charts (iv) Document Flow Diagrams
(a) i and ii (b) ii and iii (c) i and iv (d) ii and iv
23. A cost-benefit analysis is performed to assess
(a) economic feasibility (b) operational feasibility (c) technical feasibility (d) all of the above
24. At the end of the feasibility study the systems analyst
(a) meets the user's for a discussion (b) gives a summary feasibility report to the management
(c) gives a systems proposal to management (d) tells the top management if the system is not feasible
25. By technical feasibility of a solution we mean that
(a) technology is available to implement it (b) persons are available to implement it
(c) persons have technical ability to implement it (d) funds are available to implement it
26. By economic feasibility of a system we mean that
(a) it is economical to operate (b) it is expensive to operate (c) it will be cost-effective if implemented
(d) finances are available to implement the system and it will be cost-effective
27. The primary objective of cost-benefit analysis is
(a) to find out direct and indirect cost of developing the information system
(b) to determine the tangible benefits of the information system
(c) to determine if it is economically worthwhile to invest in developing the information system
(d) to determine the intangible benefits of the information system
28. A cost-benefit analysis is performed as a part of
(a) system design (b) system specification (c) system performance assessment (d) feasibility analysis
29. In payback method one finds out
(a) the period necessary to invest the cost of the system (b) the time required for the full benefits to accrue
(c) the time at which benefits exceed cost (d) whether the system is able to payback amount invested
30. The main objectives of a detailed system proposal are to
(i) convince management about the benefits of the proposed system (ii) explain in detail to the management what to expect from the system and at what cost (iii) have a detailed plan on what the system will do and how it will be implemented (iv) make sure that it is possible to implement the system
(a) i and ii (b) ii and iii (c) i and iv (d) ii and iv

31. A data flow can
(a) only emanate from an external entity (b) only terminate in an external entity
(c) may emanate and terminate in an external entity
(d) may either emanate or terminate in an external entity but not both
32. External Entities may be a
(a) source of input data only (b) source of input data or destination of results
(c) destination of results only (d) repository of data
33. Data cannot flow between two data stores because
(a) it is not allowed in a DFD (b) a data store is a passive repository of data
(c) data can get corrupted (d) they will get merged
34. By levelling a DFD we mean
(a) splitting it into different levels (b) make its structure uniform
(c) expanding a process into one with more sub-processes giving more detail
(d) summarizing a DFD to specify only the essentials
35. Before developing a logical DFD it is a good idea to
a) develop a physical DFD b) develop a system flow chart c) determine the contents of all data stores
d) find out user's preferences
36. A physical DFD
(a) has no means of showing material flow (b) does not concern itself with material flow
(c) can show only stored material (d) can show the flow of material
37. Structured English is a
(a) structured programming language (b) description of processes in simple English
(c) method of describing computational procedures reasonably precisely in English
(d) natural language based algorithmic language
38. A decision table
(a) has a structured English equivalent representation (b) cannot be represented using structured English
(c) does not have an equivalent algorithmic representation (d) cannot be used to represent processes in a DFD
39. Select statements from the following list which may be used in structured English
(i) if marks are too low fail student (ii) if marks >=60 enter first class
(iii) if average height select candidate (iv) if weight < 40 kg. reject candidate
(a) i and ii (b) ii and iii (c) iii and iv (d) ii and iv
40. The conditions in the condition stub of a limited entry decision table
(a) must be in sequential order (b) must be in the order in which they are to be tested
(c) may be in any order (d) must be in the order in which they are to be executed
41. The actions in the action stub of a limited entry decision table
(a) must be in sequential order (b) must be in the order in which they are to be tested
(c) may be in any order (d) must be in the order in which they are to be executed
42. A data dictionary is useful as
(i) it is a documentation aid (ii) it assists in designing input forms
(iii) it contains all data in an application including temporary data used in processes
(iv) it is a good idea in system design
(a) (i) and (ii) (b) (i) and (iv) (c) (i),(ii) and (iii) (d) (i) and (iv)
43. Good system design prevents data entry errors by
(i) Designing good forms with plenty of space to write in block capitals
(ii) By giving clear instructions to a user on how to fill a form
(iii) Reducing keystrokes of an operator (v)Designing good keyboard
(a) i, ii, iii (b) i, ii, iv (c) i, ii (d) iii and iv
44. In interactive data input a menu is used to
(a) enter new data (b) add/delete data (c) select one out of many alternatives often by a mouse click
(d) detect errors in data input
45. A code is useful to represent a key field because
(a) it is a concise representation of the field (b) it is usually done by all
(c) it is generally a good idea (d) it is needed in database design
46. Pick the meaningful relationship between entities
(a) vendor supplies goods (b) vendor talks with customers (c) vendor complains to vendor (d) vendor asks

prices

47. The entity set is a

- (a) set of entities (b) collection of different entities
- (c) collection of related entities (d) collection of similar entities

48. Relationships are identified from the word statement of a problem by

- (a) picking words which are adjectives (b) picking words which are nouns
- (c) picking words which are verbs (d) picking words which are pronouns

49. Normalization is a process of restructuring a relation to

- (a) minimize duplication of data in a database (b) maximize duplication of data to ensure reliability
- (c) make it of uniform size (d) allow addition of data

SECTION B: Answer all questions for (15 +15=30 marks).

a. Starting with a context diagram, draw as many nested DFDs as you consider necessary to represent all of the details of the engineering document management system described in the following narrative. You must draw at least a context diagram and a level-0 diagram. In drawing these diagrams, if you discover that the narrative is incomplete, make up reasonable explanations to complete the story. Provide these extra explanations along with the diagrams.

Projects, Inc. is an engineering firm with approximately 500 engineers that provide mechanical engineering assistance to organizations, which requires managing many documents. Projects, Inc. is known for its strong emphasis on change management and quality assurance procedures. The customer provides detailed information when requesting a document through a web portal. The company liaison (a position within Projects, Inc.) assigns an engineer to write the first draft of the requested document. Upon completion, two peer engineers review the document to ensure that it is correct and meets the requirements. These reviewers may require changes or may approve the document as is. The original engineer updates the document until the reviewers are satisfied with the quality of the document. The document is then sent to the company liaison, who performs a final quality check and ensures that the document meets the requirements specified by the customer. Finally, the customer liaison sends the document to the customer for approval. The customer can require changes or accept the document. When the customer requires changes, the company liaison assigns an engineer to make the changes to the document. When those changes are made, two other engineers must review them. When those reviewers are satisfied with the changes, the document is sent back to the company liaison, who sends the document back to the customer. This may happen through several iterations until the customer is satisfied with the document.

b. Analyze the DFDs you created in part a. What recommendations for improvements can you make based on this analysis? Draw new logical DFDs that represent the requirements you would suggest for an improved document management system. Remember, these are to be logical DFDs, so consider improvements independent of technology that can be used to support the management of these documents.