

Q1) (25 points)

A) Design and Develop an android application that contain 3 radio options (Red, Green, Blue), when the user chooses one of them the app Background should change to the corresponding color. And also, include a reset button that clear radio buttons selection and return the background color back to the default. (Note: write the required code for the activity_main.xml and MainActivity.java. (10 Points)

B) When you go with friends to a restaurant and wish to divide the check and tip, you can get into a lot of manual calculations and disagreements. Instead, develop an android application based on the following design that lets you simply add the tip percentage to the total and divide by the number of diners. (Note: write the required code for the activity_main.xml and MainActivity.java. (15 Points)

A screenshot of an Android application interface. The interface is dark-themed and contains the following elements:

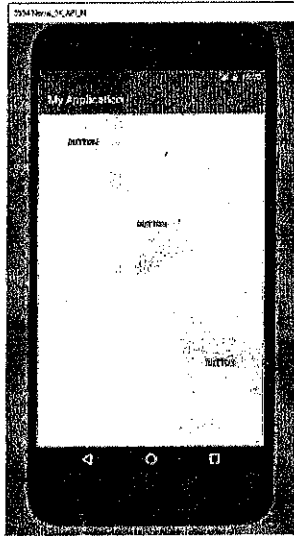
- Total Amount:** A text label followed by an empty text input field.
- No. of people:** A text label followed by an empty text input field.
- Tip Percentage:** A text label followed by three radio button options: "15%", "20%", and "Other". The "20%" option is selected.
- Buttons:** Two buttons labeled "Reset" and "Calculate" are positioned below the radio buttons.
- Output Fields:** Below a horizontal separator line, there are three text labels: "Tip Amount:", "Total to Pay:", and "Total per Person:", each followed by an empty text input field.

Q2) (25 points)

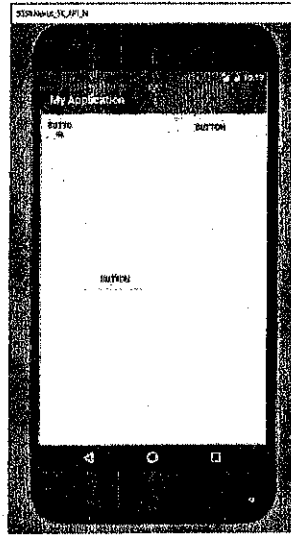
A) Write the required code to set up the required permissions to use sensors, reading acceleration and magnetic field data in an android App? And where you should place that code? (4 points)

B) write the corresponding activity_main.xml code for each of the following design: (6 points)

(1)



(2)

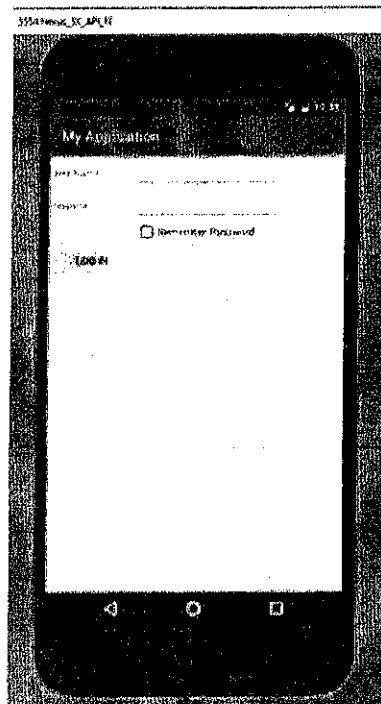


C) Write the required code that should be added to MainActivity.java to develop a simple compass app that will utilize the internal accelerometer and magnetometer sensors of the Android device? (15 points)

Q3) (10 points)

A) Write code that you need to know the device's current orientation (portrait or landscape)? and where should you place that code? (5 points)

B) write the corresponding activity_main.xml code for each of the following design: (5 points)



With My Best Wishes
Dr. Ahmed Elashry



Q1) (15 points)

(A) Explain how to connect a GSM shield to Arduino UNO? write the appropriate code to make a call using GSM module? (5 points)

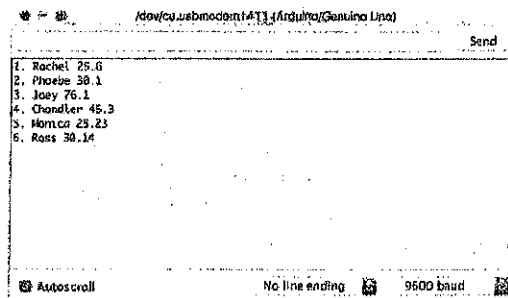
(B) write the appropriate code to send SMS using the GSM module? And the appropriate code to receive that SMS? (6 points)

(C) Discuss and Explain what the following code do? (4 points)

```
#include <LiquidCrystal.h>
LiquidCrystal lcd(13, 12, 11, 10, 9, 8);// initialize the LCD
Library w.r t. RS,E,D4,D5,D6,D7
int BUTTON_LOW=5;
int RED_LED=3;
int BLUE_LED=2;
void setup()
{
  pinMode(BUTTON_LOW, INPUT_PULLUP);
  pinMode(RED_LED,OUTPUT);
  pinMode(BLUE_LED,OUTPUT);
  lcd.begin(20, 4);
  lcd.setCursor(0, 0);
  lcd.print("DIGITAL LOW BUTTON ");
  lcd.setCursor(0, 1);
  lcd.print("READ SYSTEM.....");
  delay(1000);
}
void loop()
{
  int BUTTON_LOW_READ =
    digitalRead(BUTTON_LOW);
  if (BUTTON_LOW_READ == LOW)
  {
    lcd.clear();
    lcd.setCursor(0, 2);
    lcd.print("BUTTON_PRESSED ");
    digitalWrite(RED_LED, HIGH);
    digitalWrite(BLUE_LED, LOW);
    delay(20);
  }
  else //otherwise
  {
    lcd.clear();
    lcd.setCursor(0, 2);
    lcd.print("BUTTON_NOT_PRESSED ");
    digitalWrite(BLUE_LED, HIGH);
    digitalWrite(RED_LED,LOW);
    delay(20);
  }
}
```

Q2) write the following programs in Arduino IDE and C: (15 points)

(A) Suppose you have two files stored on an SD card. One file has five players' names and another file has their scores. Now make another file, containing both the names and scores side by side with the serial number. Look at the following screenshot for clarification: (7 points)



(B) Make a list of the following food items, with the prices next to them. If a customer buys a number of food pieces from the list. calculate the total money he would need to buy the food pieces: (8 points)

1. Sandwiches (\$2.90), 2. Burgers (\$4.90), 3. Pizzas (\$9.99), 4. Soft Drinks (\$1.50), 5. Beer (\$4.99)

Your output should look as follows:

****The customer receipt****

Food Name	Quantity	Price	Total
Sandwiches	0	2.90	0
Burgers	0	4.90	0
Pizzas	5	9.99	49.95
Soft Drinks	0	1.50	0
Beer	5	4.99	24.95
Total:		\$ 74.90	

Q3) Design, develop and write the appropriate code for fire and motion detection home security system with a 2.4 GHz RF Modem that will sense any fire or any unusual motion in your home and then makes a sound and displays a text on LCD screen if that happened. (note: The system should be designed in two sections: (1) sensor node and (2) server.) use the following components in your system: (20 points)

Components List for a Transmitter Section		Components List for a Receiver Section	
Component/Specification	Quantity	Component/Specification	Quantity
Power supply/+12 V/1 A	1	Power supply/+12 V/1 A	1
Arduino Uno	1	Arduino Uno	1
PIR sensor	1	LCD (20 * 4)	1
PIR sensor patch	1	LCD patch	1
Flame sensor	1	2.4 GHz RF modem	1
Flame sensor patch	1	2.4 GHz RF modem patch	1
LCD (20 * 4)	1	Connecting wires (M-M, M-F, F-F)	20 each
LCD patch	1	bread board	1
2.4 GHz RF modem	1		
2.4 GHz RF modem patch	1		
Connecting wires (M-M, M-F, F-F)	20 each		
bread board	1		

Q4) Design, develop and write the appropriate code for a Smart Weather System that will measure air temperature, air pressure, and air humidity. Use the following components: (Humidity and Temperature Sensor (DHT11), Pressure Sensor, a 16x2 LCD Display, Arduino UNO, Jumper wires) (10 points)

With my Best Wishes
Dr. Ahmed Elashry



Question 1

(25 Marks)

(A) Chose the correct answer for each one of the following Sentences: (15 Marks)

- (1) Use Caesar's Cipher to decipher the text "HQFUBSWHG WHAW" produce

 - (a) ABANDONED LOCK
 - (b) ENCRYPTED TEXT
 - (c) ABANDONED TEXT
 - (d) Nothing

- (2) If the text "Make It Happen" is encrypted by using *Vigenere Cipher* with key word "math" , then the encrypted text is

 - (a) ZADL TU AHBPXU
 - (b) YA CL VT AHBQXU
 - (c) YADL UT AHBPXU
 - (d) Nothing

- (3) It is a technique, in which the letters of plaintext are replaced by other letters or numbers or symbols .

 - (a) RC5 Cipher
 - (b) Substitution Cipher
 - (c) Transposition Cipher
 - (d) Nothing

- (4) The cipher which handle (4^2) registers of 32 bits in its encryption or decryption process.

 - (a) RC5 Cipher
 - (b) Playfair Cipher
 - (c) Transposition Cipher
 - (d) MRC6

- (5) Caesar Cipher represents an example of

 - (a) Poly-alphabetic Cipher
 - (b) Mono-alphabetic Cipher
 - (c) Transposition Cipher
 - (d) Nothing

- (6) Encrypting "pepsiisrefrigerator" using *Vignere Cipher* using the keyword "HUMOR" we get cipher text

 - (a) dnwewwtrfznsdokvl
 - (b) dvmwuwjphyrfzndokvl
 - (c) dvmuwjhyrfzndoykvl
 - (d) Nothing

- (7) Which of the following is true for the RC5 algorithm?

 - (a) Has variable number of rounds
 - (b) Has fixed Key length
 - (c) High memory Requirements
 - (d) Nothing

- (8) The number of sub-keys required in both RC5 and MRC6 at $r = 18$ of computation are....

 - (a) 40 and 160
 - (b) 38 and 159
 - (c) 37 and 159
 - (d) 38 and 160

- (9) In RC5, the initialization operations makes use of magic constants defined as follows: $Pw = \text{Odd}((e-2) 2^m)$ and $Qw = \text{Odd}((\phi-1) 2^m)$, What is the hexadecimal value of Qw for word size of 32 bits?, Is

 - (a) 9D3779B4
 - (b) 9E3779B9
 - (c) 9E36D9B2
 - (d) Nothing

- (10) If the message "meet me tomorrow" encrypted by *rail fence* of depth 3, the result of encrypted message is...

 - (a) MTTOMOEORWEMER
 - (b) MTTOEMORWEEMR
 - (c) MEMTMROETEOORW
 - (d) Nothing

- (11) Assures that systems work promptly and service is not denied to authorized users

 - (a) Availability
 - (b) Integrity
 - (c) Confidentiality
 - (d) Nothing

- (12) This is an attack on confidentiality, and an unauthorized party gains access to an asset, the unauthorized party could be a person, a program or a computer.

 - (a) Interruption
 - (b) Interception
 - (c) Modification
 - (d) Nothing

- (13) This is an attack on integrity, and an unauthorized party not only gains access to but also tampers with an asset.

 - (a) Interruption
 - (b) Interception
 - (c) Fabrication
 - (d) Nothing

- (14) This is an attack on authenticity, and an unauthorized party inserts counterfeit objects into the system.

 - (a) Modification
 - (b) Fabrication
 - (c) Interception
 - (d) Nothing

- (15) The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner.

 - (a) Security policy
 - (b) Risk assessment
 - (c) Access control
 - (d) Nothing



SE

(25 Marks)

(A) Put sign (✓) at correct and sign (×) at wrong with correction the wrong: (10 Marks)

- (1) If the sender and receiver use different keys, the system is conventional cipher system.
- (2) Passive attack is an attempt to learn or make use of information from the system that does not affect system resources.
- (3) Integrity is preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
- (4) In MRC6 Cipher use $t = 4r + 16$ in its key expansion algorithm, but $t = 2r + 2$ in RC5 cipher.
- (5) DAC is policy where an entity might have access rights that permit the entity, by its own volition, to enable another entity to access some resource.
- (6) RC6 and MRC6 Ciphers uses a function " $x * (2x^2 + 1)$ " in their encryption algorithms.
- (7) A protection domain is a set of objects together with access rights to those objects. In terms of the access matrix, a row defines it.
- (8) RC6 encryption uses Right shift and RC5 decryption uses Left shift.
- (9) If the correlation coefficient measuring factor (C.C) equals 0, this means the encrypted image is the same of the original image.
- (10) Substitution Cipher is the technique in which, the letters/symbols in the message are reordered but are not disguised.

(B) Chose the correct answer for each one of the following Sentences: (15 Marks)

- (1) Use Caesar's Cipher to decipher the text "HQFUBSWHG WHAW" produce
(a) ABANDONED LOCK (b) ENCRYPTED TEXT (c) ABANDONED TEXT (d) Nothing
- (2) If the text "Make It Happen" is encrypted by using *Vignere Cipher* with key word "math", then the encrypted text is
(a) ZADL TU AHBPXU (b) YAQL VT AHBQXU (c) YADL UT AHBPXU (d) Nothing
- (3) It is a technique, in which the letters of plaintext are replaced by other letters or numbers or symbols .
(a) RC5 Cipher (b) Substitution Cipher (c) Transposition Cipher (d) Nothing
- (4) The cipher which handle (4^2) registers of 32 bits in its encryption or decryption process.
(a) RC5 Cipher (b) Playfair Cipher (c) Transposition Cipher (d) MRC6
- (5) Caesar Cipher represents an example of
(a) Poly-alphabetic Cipher (b) Mono-alphabetic Cipher (c) Transposition Cipher (d) Nothing
- (6) Encrypting "pepsiisinrefrigerator" using *Vignere Cipher* using the keyword "HUMOR" we get cipher text
(a) dnwewuwrtfznsdokvl (b) dvmuwujphyrfzndokvl (c) dvmuwujhyprfzndoykvl (d) Nothing
- (7) Which of the following is true for the RC5 algorithm?
(a) Has variable number of rounds (b) Has fixed Key length (c) High memory Requirements (d) Nothing
- (8) The number of sub-keys required in both RC5 and MRC6 at $r = 18$ of computation are....
(a) 40 and 160 (b) 38 and 159 (c) 37 and 159 (d) Nothing



SE

- (9) In RC5, the initialization operations makes use of magic constants defined as follows: $Pw = \text{Odd}((e-2) 2^w)$ and $Qw = \text{Odd}((\phi-1) 2^w)$, What is the hexadecimal value of Qw for word size of 32 bits?, Is
- (a) 9D3779B4 (b) 9E3779B9 (c) 9E36D9B2 (d) Nothing
- (10) If the message "meet me tomorrow" encrypted by rail fence of depth 3, the result of encrypted message is...
- (a) MTTOMOEORWEMER (b) MTTOEMORWEEMR (c) MEMTMROETEOORW (d) Nothing
- (11) Assures that systems work promptly and service is not denied to authorized users
- (a) Availability (b) Integrity (c) Confidentiality (d) Nothing
- (12) This is an attack on confidentiality, and an unauthorized party gains access to an asset, the unauthorized party could be a person, a program or a computer.
- (a) Interruption (b) Interception (c) Modification (d) Nothing
- (13) This is an attack on integrity, and an unauthorized party not only gains access to but also tampers with an asset.
- (a) Interruption (b) Interception (c) Fabrication (d) Nothing
- (14) This is an attack on authenticity, and an unauthorized party inserts counterfeit objects into the system.
- (a) Modification (b) Fabrication (c) Interception (d) Nothing
- (15) The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner.
- (a) Security policy (b) Risk assessment (c) Access control (d) Nothing

Question (2) Answer the following sub-questions as required at each of them: (20 Marks)

- (1) **Define:** (a) Access Right, and What is included? (b) Subject, and its three classes.
(c) Throughput.
- (2) Write the Equation of Maximum Deviation Measuring Factor (D).

Also use this factor (D) to measure, Which is of the two algorithms (X) or (Y) gives More Encryption Quality? Assume we have the following information:

X encrypt the plain-image (im) and produce encrypted image (im_x), and Y encrypt the same image (im) and produce encrypted image (im_y). these images have the following histogram.

image	Pixel value	0	10	15	70	125	170	200	225	240	255
im	frequency	13	16	13	23	18	33	23	15	13	33
im_x	frequency	10	12	22	17	14	12	32	32	27	22
im_y	frequency	18	13	33	16	18	15	33	23	18	13

Question (3) Answer the following questions as required in each of them: (15 Marks)

- (a) Write the Encryption Algorithm for "MRC6 Block Cipher Algorithm", and draw The Flowchart of its Key Expansion Technique.
- (b) Compare between ACLs and Capability Lists, with illustration by example and drawing figures.
- (c) Encrypt "Welcome to computers college" by using "Playfair cipher" with keyword "monarchy".

With best wishes with success;
22/12/2019
Dr. Osama M. Abu Zaid