Kafrelsheikh University
Faculty of Computers and Information
Department of Computer Science

SE

Final Exam of
Intro. to Computer Security (**CS471**)
2019/2020 (First Term)
Date: 29/12/2019
Time: 3 hrs

Question (1) **(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 *Vigenere Cipher* with key word "math" , then the encrypted text is .....

(a) ZADL TU AHBPXU **(b)** YACL 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) dnwewuwrtrfznsdokvl **(b)** dvmwuwjphyyrfznydokvl **(c)** dvmuwwjhypyrfzndoykvl **(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

Kafrelsheikh University
Faculty of Computers and Information
Department of Computer Science

SE

Final Exam of
Intro. to Computer Security (**CS471**)
2019/2020 (First Term)
Date: 29/12/2019
Time: 3 hrs

Question (1) **(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 *Vigenere Cipher* with key word "math" , then the encrypted text is .....

(a) ZADL TU AHBPXU **(b)** YACL 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) dnwewuwrtrfznsdokvl **(b)** dvmwuwjphyyrfznydokvl **(c)** dvmuwwjhypyrfzndoykvl **(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

Kafrelsheikh University
Faculty of Computers and Information
Department of Computer Science

SE

Final Exam of
Intro. to Computer Security (CS471)
2019/2020 (First Term)
Date: 29/12/2019
Time: 3 hrs

(9) In RC5, the initialization operations makes use of magic constants defined as follows: Pw=Odd((e-2) 2^w) and Qw=Odd((φ-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) MTTOOEMORWEEMR (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

Kafrelsheikh University
Faculty of Computers and Information
Department of Computer Science

Department : *CS*

Final Exam of
Parallel Computations (**CS431**)
2019/2020 (First term)
Date: 12/1/2020
Time: 3 hrs

Questions **(28 Marks)**

(I) ***Chose*** **the correct answer for the following sentences,** ***write only the choice*****: (18 Marks)**

(1) Execution of several activities at the same time is ..... .
(a) processing (b) parallel processing (c) serial processing (d) multitasking

(2) A term for simultaneous access to a resource, physical or logical is ..... .
(a) Multiprogramming (b) Multitasking (c) Threads (d) Concurrency

(3) ..... leads to concurrency.
(a) Serialization (b) Parallelism (c) Serial processing (d) Distribution

(4) The measure of the "effort" needed to maintain efficiency while adding processors.
(a) Maintainability (b) Efficiency (c) Scalability (d) Effectiveness

(5) In ..... , instructions are executed sequentially one after another, and Executed on a single processor.
(a) Parallel Computing (b) Serial Computing (c) MISD (d) MIMD

(6) ... is the simultaneous use of multiple compute resources to solve a computational problem.
(a) Parallel Computing (b) Serial Computing (c) MIMD (d) Nothing of them

(7) The following is one from *Flynn's Classical Taxonomy*.
(a) SIDM (b) SIDD (c) MISD (d) Nothing of them

(8) ..... is the amount of data that can be communicated per unit of time. Commonly expressed as megabytes/sec or gigabytes/sec
(a) Concurrency (b) Latency (c) Bandwidth (d) Nothing of them

(9) ..... is one of the main reasons of "Why Use Parallel Computing?".
(a) Provide Synchronous (b) Provide Concurrency (c) Engineering (d) Nothing of them

(10) In ..... , changes in a memory location affected by one processor are visible to all other processors.
(a) Shared Memory (b) Distributed Memory (c) SISD (d) Nothing of them

(11) ..... is one from Von Neumann Architecture .
(a) SISD (b) MISD (c) (a) and (b) together (d) Nothing of them

(12) In ..... , changes it makes to its local memory have no effect on the memory of other processors.
(a) Shared Memory (b) Distributed Memory (c) MIMD (d) Nothing of them

(13) A serial (non-parallel) computer is represented by ..... Architecture.
(a) SIMD (b) SISD (c) MIMD (d) Nothing of them

(14) ..... is the simultaneous use of multiple compute resources to solve a computational problem.
(a) Serial Computing (b) MIMD (c) MISD (d) Nothing of them

(15) ..... is one from Flynn's Classical Taxonomy.
(a) SIDM (b) MISD (c) (a) and (b) together (d) Nothing of them

(16) ..... are often referred to as blocking communications since other work must wait until the communications have completed.

(a) Asynchronous Communications (b) Collective (c) Latency (d) Nothing of them

(17) ..... is a qualitative measure of the ratio of computation to communication.

(a) Debugging (b) Granularity (c) Collective (d) Nothing of them

(18) ..... is a parallel computing platform and application programming interface (API) model created by Nvidia. It allows software developers and software engineers to use GPU.

(a) CUDA (b) MPMD (c) SPMD (d) CDUA

(II) Put sign(√) at correct and sign(×) at wrong with *correction* the wrong: (12 Marks)

(1) Parallel processing has single execution flow.

(2) Many MIMD architectures also include SIMD execution sub-components.

(3) Latency is the time it takes to send a minimal (0 byte) message from point A to point B. Commonly expressed as microseconds.

(4) In MIMD, every processor may be working with a different data stream.

(5) In MIMD, each processing unit operates on the data independently via separate instruction streams.

(6) Collective involves two tasks with one task acting as the sender/producer of data, and the other acting as the receiver/consumer.

(7) MPMD is actually a "high level" programming model, where all tasks execute their copy of the same program simultaneously, this program can be threads, message passing, data parallel or hybrid.

(8) In Data Parallel Model, tasks exchange data through communications by sending and receiving messages.

(9) Distributed Memory Machines have been classified as UMA and NUMA, based upon memory access times.

(10) Factors that contribute to scalability include particularly memory-CPU bandwidths and network.

Question (3) Answer following *sub-questions* as required at each of them: (32 Marks)

(1) List the *Risks* of *fully automatic* for compiler's parallelizing.

(2) Compare between "*Fine-grain Parallelism*" and "*Coarse-grain Parallelism*", and Which of them is *the best ?*

(3) Write about *Limits and Costs of Parallel Programming.*

(4) Write the List of a *Several Parallel Programming Models* in common use. Also, Explain the details of *Threads Model* with drawing, and Write about the two different implementations of *Threads.*

(5) Write about *Amdahl's Law* with its *equations* for all its different cases.

With best wishes with success;

Dr. Osama M. Abu Zaid

Kafrelsheikh University
Faculty of Computers and Information
Department of Computer Science

SE and CS

Final Exam of
Intro. to Computer Security (CS471)
2019/2020 (First Term)
Date: 1/1/2020
Time: 3 hrs

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) YACL 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) dnwewuwrtrfznsdokvl (b) dvmwuwjphyyrfznydokvl (c) dvmuwwjhypyrfzndoykvl (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=Odd((e-2) 2^w) and Qw=Odd((φ-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) MTTOOEMORWEEMR (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

Kafrelsheikh University
Faculty of Computers and Information
Department of Computer Science

[redacted] CS

Final Exam of
Intro. to Computer Security (**CS471**)
2019/2020 (First Term)
Date: 1/1/2020
Time: 3 hrs

(B) 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) Active 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+8 in its key expansion algorithm, but t = 2r+4 in RC6 cipher.

(5) MAC 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, RC5 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) RC5 encryption uses Right shift and RC6 decryption uses Left shift.

(9) If the correlation coefficient measuring factor (C.C) equals -1, 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.

Question (2) 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 *Diagram* of its *Key Expansion Technique* .

(b) Compare between *ACLs* and *Capability Lists*, with illustration by example and drawing figures.

(c) Encrypt " *Welcome to Kfs University* " by using " *Playfair cipher* " with keyword *"monarchy"*.

Question (3) 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

With best wishes with success;

Dr. Osama M. Abu Zaid

Kafrelsheikh University

Faculty of Computers and Information

Department of Information systems

Final Exam of
Advanced Database (IS411)
2020/2019 (First Term)
Date: 29/ 12 / 2019 – Time:3 hrs

Q1) Define the following terms: *superclass of a subclass, superclass/subclass relationship, specialization, generalization, data warehouse, Temporal databases, spatial database and category.* (8 point)

Q2) Draw an EER schema diagram for this art museum. Assume that the following requirements were collected: (12 points)

- The museum has a collection of ART_OBJECTS. Each ART_OBJECT has a unique Id_no, an Artist (if known), a Year (when it was created, if known), a Title, and a Description. The art objects are categorized in several ways, as discussed below.
- ART_OBJECTS are categorized based on their type. There are three main types—PAINTING, SCULPTURE, and STATUE—plus another type called OTHER to accommodate objects that do not fall into one of the three main types.
- A PAINTING has a Paint_type (oil, watercolor, etc.), material on which it is Drawn_on (paper, canvas, wood, etc.), and Style (modern, abstract, etc.).
- A SCULPTURE or A STATUE has a Material from which it was created (wood, stone, etc.), Height, Weight, and Style.
- An art object in the OTHER category has a Type (print, photo, etc.) and Style.
- ART_OBJECTs are categorized as either PERMANENT_COLLECTION (objects that are owned by the museum) and BORROWED. Information captured about objects in the PERMANENT_COLLECTION includes Date_acquired, Status (on display, on loan, or stored), and Cost. Informationcaptured about BORROWED objects includes the Collection from which it was borrowed, Date_borrowed, and Date_returned.
- Information describing the country or culture of Origin (Italian, Egyptian, American, Indian, and so forth) and Epoch (Renaissance, Modern, Ancient, and so forth) is captured for each ART_OBJECT.
- The museum keeps track of ARTIST information, if known: Name, DateBorn (if known), Date_died (if not living), Country_of_origin, Epoch, Main_style, and Description. The Name is assumed to be unique.
- Different EXHIBITIONS occur, each having a Name, Start_date, and End_date. EXHIBITIONS are related to all the art objects that were on display during the exhibition.
- Information is kept on other COLLECTIONS with which the museum interacts; this information includes Name (unique), Type (museum, personal, etc.), Description, Address, Phone, and current Contact_person.

Q3) (20 points)

A) Consider the following bank database schema:

branch (*branch name, branch city, assets*)
customer (*customer name, customer street, customer city*)
loan (*loan number, branch name, amount*)
borrower (*customer name, loan number*)
account (*account number, branch name, balance*)
depositor (*customer name, account number*)

Write an SQL trigger to carry out the following action: On delete of an account, for each owner of the account, check if the owner has any remaining accounts, and if she does not, delete her from the *depositor* relation. (5 points)

B) Consider an employee database with two relations

employee (employee name, street, city)

works (employee name, company name, salary)

where the primary keys are underlined. Write a query to find companies whose employees earn a higher salary, on average, than the average salary at "First Bank Corporation". (5 points)

C) Consider the relational schema

part(part id, name, cost)

subpart(part id, subpart id, count)

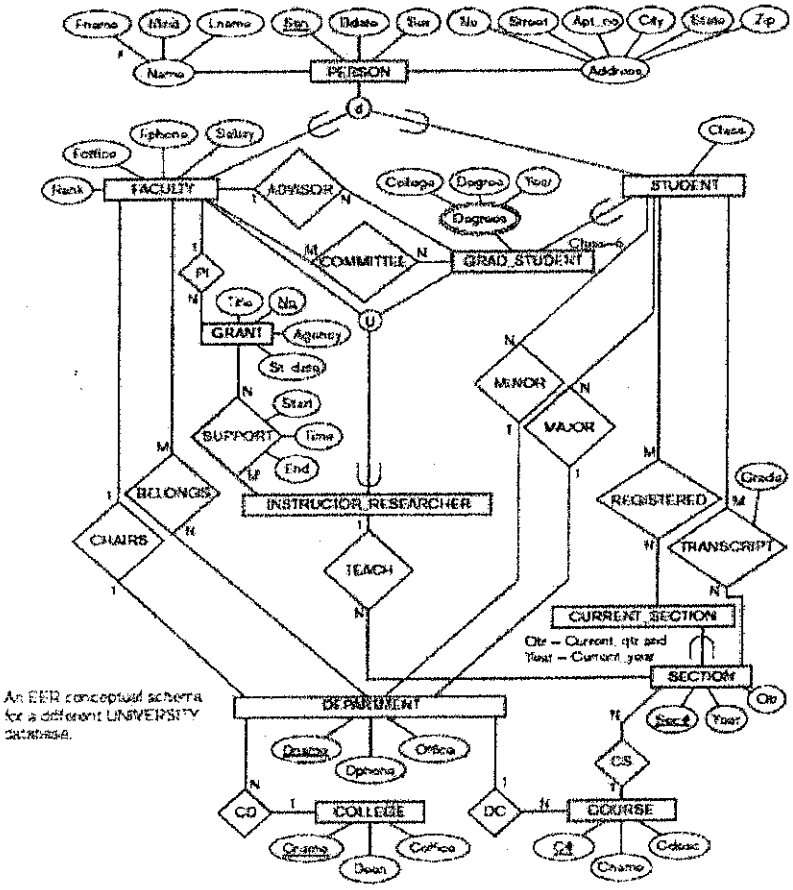
A tuple (p1, p2, 3) in the subpart relation denotes that the part with part-id p_2 is a direct subpart of the part with part-id p_1, and p_1 has 3 copies of p_2. Note that p_2 may itself have further subparts. Write a recursive SQL query that outputs the names of all subparts of the part with part-id "P-100". (5 points)

D) Consider the relational schema:

Instructor(Instructor_name, address, city, dept_name)

Create a SQL function that, given the name of a department, returns the count of the number of instructors in that department. And then use that function in a query that returns names of all departments with more than 12 instructors. (5 points)

Q5) Map the EER diagrams in the following figures into relational schemas: (20 points)



An EER conceptual schema for a different UNIVERSITY database.

With My Best wishes
Dr. Ahmed Elashry

Kafrelsheikh University
Faculty of Computers and Information
Department of Information systems

Final Exam of
Embedded Systems (CS423)
2019/2020 (First Term)
Date: 8/ 1 / 2020 – Time:3 hrs

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)***

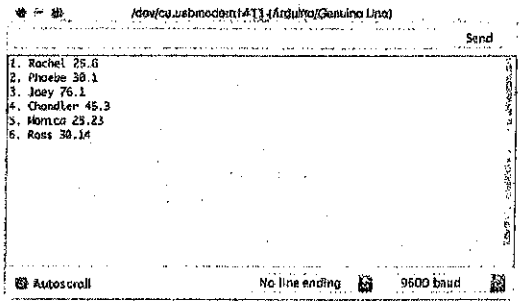
(B) write the appropriate code to send SMS using the GSM module? And the appropriate code to receive that SMS? ***(6 points)***

(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("DIGTAL 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 16×2 LCD Display, Arduino UNO, Jumper wires) ***(10 points)***

With my Best Wishes

Dr. Ahmed Elashry

Kafrelsheikh University
Faculty of Computers and Information
Department of Computer Science

[redacted] CS

Final Exam of
Intro. to Computer Security (**CS471**)
2019/2020 (First Term)
Date: 1/1/2020
Time: 3 hrs

(B) 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) Active 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+8 in its key expansion algorithm, but t = 2r+4 in RC6 cipher.

(5) MAC 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, RC5 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) RC5 encryption uses Right shift and RC6 decryption uses Left shift.

(9) If the correlation coefficient measuring factor (C.C) equals -1, 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.

Question (2) 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 *Diagram* of its *Key Expansion Technique* .**

(b) **Compare between *ACLs* and *Capability Lists*, with illustration by example and drawing figures.**

(c) **Encrypt " *Welcome to Kfs University* " by using " *Playfair cipher* " with keyword *"monarchy"*.**

Question (3) 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

With best wishes with success;

Dr. Osama M. Abu Zaid