King Fahd University of Petroleum and Minerals
College of Computer Sciences and Engineering
Information and Computer Science Department

ICS 254: Discrete Structures II
Second semester 2016-2017 (162)
Major Exam #2, Thursday April 20, 2017
Time: **120** Minutes

Name: ____

ID#: ____________________

Section: ___________________

Instructions:
1. The exam consists of 9 pages, including this page, containing 6 questions.
2. Answer all questions. **Show all the steps.**
3. Make sure your answers are **clear** and **readable**.
4. The exam is closed book and closed notes. **No calculators** or any helping aides are allowed. Make sure you turn off your mobile phone and keep it in your pocket.
5. If there is no space on the front of the page, use the back of the page.

Question	**Maximum Points**	**Earned Points**
1	10	
2	15	
3	15	
4	10	
5	25	
6	25	
Total	**100**	

A 00	*B* 01	*C* 02	*D* 03	*E* 04	*F* 05	*G* 06	*H* 07	*I* 08	*J* 09
K 10	*L* 11	*M* 12	*N* 13	*O* 14	*P* 15	*Q* 16	*R* 17	*S* 18	*T* 19
U 20	*V* 21	*W* 22	*X* 23	*Y* 24	*Z* 25				

Q1: [10 points] Answer the following questions.

The check digit a_{13} for an ISBN-13 number with initial digits $a_1 a_2 a_3 \ldots a_{12}$ is determined by the congruence $(a_1 + a_3 + \cdots + a_{11} + a_{13}) + 3(a_2 + a_4 + \cdots + a_{10} + a_{12}) \equiv 0 \pmod{10}$.

(a) [5 points] Determine whether 978-0-201-10179-9 is a valid ISBN-13 number.

$$(9+8+2+1+0+7+9) + 3(7+0+0+1+1+9) \pmod{10}$$

$$= 6 + 3(8) \pmod{10} = 0 \pmod{10}$$

Therefore, it is a valid ISBN-13 number

(b) [5 points] Show that there are transpositions of two digits that are not detected by an ISBN-13 number.

Swapping the location (index) of any two digits in $\{a_1, a_3, a_5, a_7, a_9, a_{11}, a_{13}\}$ or in $\{a_2, a_4, a_6, a_8, a_{10}, a_{12}\}$ will not change the value of the summation. Hence transpositions of such digits may go undetected as the number is still a valid ISBN-13 number but may not be the original one.

Q2: [15 points] Classical Cryptography.

(a) [8 points] Encrypt the plaintext message *READ A LOT* using the shift cipher with shift $k = 18$.

$R = 17, f(R) = 17 + 18\ (mod\ 26) = 9\ (J)$

$E = 4, f(E) = 4 + 18\ (mod\ 26) = 22\ (W)$

$A = 0, f(A) = 0 + 18\ (mod\ 26) = 18\ (S)$

$D = 3, f(D) = 3 + 18\ (mod\ 26) = 21\ (V)$

$L = 11, f(L) = 11 + 18\ (mod\ 26) = 3\ (D)$

$O = 14, f(O) = 14 + 18\ (mod\ 26) = 6\ (G)$

$T = 19, f(T) = 19 + 18\ (mod\ 26) = 11\ (L)$

$JWSV\ S\ DGL$

(b) [7 points] Decrypt the message *FUPK ISGM EATR* which is the ciphertext produced by encrypting a plaintext message using the transposition cipher with blocks of four letters and the permutation σ of {1, 2, 3, 4} defined by $\sigma(1) = 4$, $\sigma(2) = 1$, $\sigma(3) = 2$, and $\sigma(4) = 3$.

We first compute σ^{-1}.

$\sigma^{-1}(1) = 2, \quad \sigma^{-1}(2) = 3, \quad \sigma^{-1}(3) = 4, \quad \sigma^{-1}(4) = 1$

$FUPK \rightarrow KFUP$

$ISGM \rightarrow MISG$

$EATR \rightarrow REAT$

$KFUPM\ IS\ GREAT$

Q3: [15 points] The RSA Cryptosystem.

(a) [5 points] Propose an RSA public key encryption method based on the two prime numbers $p = 5$ and $q = 11$.

In order to apply RSA, we first need a number that is relatively prime to $(p-1)(q-1)$ $(4)(10) = 40$ in order to use as an exponent e. Possible values include 3, 7, 9, etc. Depending on the choice, the encryption method for message M becomes $M^e\ (mod\ 55)$.

Hence, possible answers are:

$$C = M^3\ (mod\ 55)$$

$$C = M^7\ (mod\ 55)$$

$$C = M^9\ (mod\ 55)$$

(b) [5 points] Based on your encryption method in part (a), encrypt the letter H.

Since the value of H is 7, we have the following possibilities:

$$7^3\ (mod\ 55) = 49 * 7\ (mod\ 55) = -6 * 7\ (mod\ 55) = -42\ (mod\ 55) = 13$$

Other possible answers include:

$$7^7\ (mod\ 55) = 28$$

$$7^9\ (mod\ 55) = 52$$

(c) [5 points]] Based on your encryption method in part (a), find the decryption method and show how to decrypt the encrypted message 24. No need to carry out the calculations. Just CLEARLY show what needs to be computed.

1- Use the Euclidean Algorithm to find d which is the inverse of e mod 40.

2- If $e = 3$ then

$$40 = 3(13) + 1$$

$$40 - 3(13) = 1$$

$$40 + 3(-13) = 1$$

$$\therefore d = -13\ (mod\ 40) = 27\ (mod\ 40)$$

$$M = 24^{27}(\text{mod } 55)$$

2. If $e = 7$ then $d = 23,\ and\ M = 24^{23}\ (\text{mod } 55)$

2. If $e = 9$ then $d = 9,\ \ and\ M = 24^{9}\ (\text{mod } 55)$

Q4: [10 points] Suppose that *R* and *S* are reflexive relations on a set *A*.

(a) (5 points) Prove or disprove that $R \cap S$ is a reflexive relation

Let R and S be reflexive relations. Then, $\forall a \in A\ [\ (a,a) \in R \wedge (a,a) \in S]$, i.e., $(a,a) \in R \cap S$.

Therefore, $R \cap S$ is indeed reflexive.

OR

Since R and S are reflexive, their matrix representations have 1's in the diagonal. Since the intersection is represented as a Boolean *and* operation, The resulting matrix will also have 1's on the diagonal ($r_{ii} \wedge s_{ii} = 1 \wedge 1 = 1\ \forall i$), and hence $R \cap S$ is also reflexive.

(b) (5 points) Prove or disprove that $S \circ R$ is a reflexive relation

Let R and S be two reflexive relations. Then, $\forall a \in A\ \ (a,a) \in R \wedge (a,a) \in S$

Since by the definition of the composition function, there is an element (viz. $\boldsymbol{a}$) such that $(a,\boldsymbol{a}) \in R$ and $(\boldsymbol{a},a) \in S$. Hence, $(a,a) \in S \circ R$ and therefore it is reflexive.

OR

Since R and S are reflexive, their matrix representations have 1's in the diagonal. Since the composition is represented as a Boolean product operation, $\odot$, the resulting matrix will also have 1's on the diagonal ($r_{ii} * s_{ii} = 1 * 1 = 1 \forall i$), and hence $S \circ R$ is also reflexive.

Q5: [25 points] Solve the following questions

(a) [15 points] Let R be the relation on the set of ordered pairs of positive integers such that $((a, b), (c, d)) \in R$ if and only if $a + d = b + c$.

i. (10 points) Show that R is an equivalence relation.

a. R is reflexive: To show that $\big((a,b),(a,b)\big) \in R\ \forall a,b \in Z^+$

Since $a + b = b + a \quad \forall a,b \in Z^+$, R is reflexive.

b. R is symmetric: if $\big((a,b),(c,d)\big) \in R$, we need to show that $\big((c,d),(a,b)\big) \in R$.

Since $\big((a,b),(c,d)\big) \in R$, we know that $a + d = b + c = c + b = d + a$. Hence, R is Symmetric.

c. R is Transitive: if $\big((a,b),(c,d)\big) \in R$ and $\big((c,d),(e,f)\big) \in R$, we need to show that $\big((a,b),(e,f)\big) \in R$,

if $\big((a,b),(c,d)\big) \in R$ then, $a + d = b + c, i.e., c - d = a - b$

if $\big((c,d),(e,f)\big) \in R$ then, $c + f = d + e, i.e., c - d = e - f$

From both equations above, it is obvious that $a - b = e - f, i.e., a + f = b + e$

$i.e., \big((a,b),(e,f)\big) \in R$, which is what we want to prove.

ii. [5 points] list 5 distinct elements that belong to the class containing (3,1).

$\{(3,1),(4,2),(5,3),(6,4),(7,5),\ldots\}$

(b) [10 points] Using Warshall's algorithm, find the transitive closure of the relation

$$R = \{(a,b),(a,c),(a,e),(b,a),(b,c),(c,a),(c,b),(d,a),(e,d)\}$$

on $\{a,b,c,d,e\}$

$$R = R_0 = \begin{bmatrix} 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

$$R_1 = \begin{bmatrix} 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

$$R_2 = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

$$R_3 = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

$$R_4 = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

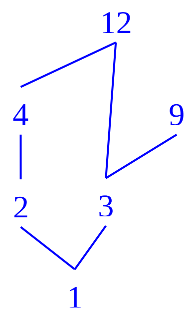
$$R_5 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \end{bmatrix} = R^*$$

$\therefore$ Letting $A = \{a,b,c,d,e\}, R^* = A \times A$

Q6: [25 points]

(a) [10 points] Consider the following partial order $\{(a, b) | a \text{ divides } b\}$ on $\{1,2,3,4,9,12\}$.

i. (4 points) Draw the Hasse diagram corresponding to the above poset.



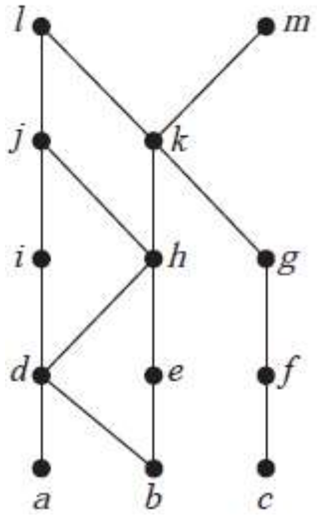
ii. (3 points) What is the covering relation of the above poset?

Covering Relation = {(1,2), (1,3), (2,4), (3,9), (3,12), (4,12)}

iii. (3 points) Is the above poset a total order? Justify your answer.

No. Since neither (4,9) nor (9,4) belong to the poset, not all elements are comparable, and hence it is not a total order.

(b) [15 points] Answer the following questions for the partial order represented by this Hasse diagram.



i. (3 points) Find the maximal elements.

$\{l, m\}$

ii. (2 points) Is there a greatest element? If yes, write it.

No.

iii. (3 points) Find all upper bounds of $\{a, b, c\}$.

$\{k, l, m\}$

iv. (2 points) Find the least upper bound of $\{a, b, c\}$, if it exists.

k

v. (3 points) Find all lower bounds of $\{j, k, m\}$.

$\{a, b, d, e, h\}$

vi. (2 points) Find the greatest lower bound of $\{j, k, m\}$, if it exists.

h