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 $a_1a_2a_3 \ldots a_{12}$ 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.

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

Q2: **[15 points] Classical Cryptography.**

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

(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 $\sigma(4) = 3$.

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 $q = 11$.

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

(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.

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

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

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.

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

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

Q6: [25 points]

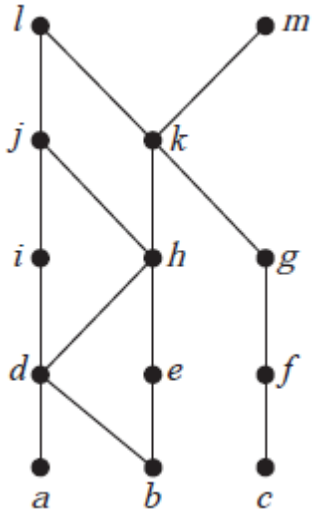
(a) [10 points] Consider the following partial order $\{(a, b) | a \text{ divides } b\}$ on $\{1,2,3,4,9,12\}$.

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

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

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

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



i. (3 points) Find the maximal elements.

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

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

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

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

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