CS1800 Discrete Structures Midterm
Version B

Instructions:

1. The exam is closed book and closed notes. You may not use a calculator or any other electronic device.

2. The exam is worth 100 total points. The points for each problem are given in the problem statement and in the table below.

3. You should write your answers in the space provided; use the back sides of these sheets, if necessary.

4. You have two hours to complete the exam.

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Section 1[18 points]</td>
<td>Binary, Octal, and Hexadecimal</td>
<td></td>
</tr>
<tr>
<td>Section 2 [18 points]</td>
<td>Logic</td>
<td></td>
</tr>
<tr>
<td>Section 3 [18 points]</td>
<td>Modular Arithmetic and Algorithms</td>
<td></td>
</tr>
<tr>
<td>Section 4 [8 points]</td>
<td>Modular Cryptosystems</td>
<td></td>
</tr>
<tr>
<td>Section 5 [20 points]</td>
<td>Sets</td>
<td></td>
</tr>
<tr>
<td>Section 6 [18 points]</td>
<td>Counting</td>
<td></td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Name: _________________________ NU ID#: _________________________

Recitation Time/Loc: _______________ Recitation TA: _______________
Section 1 [18 pts (5,4,4,5)]: Binary, Octal, and Hexadecimal

1. What is the result of subtracting 0x2222 from 0xFFEA? (The 0x indicates the number is in hexadecimal.)
   \[ \text{Sol: } 0xFFEA - 0x2222 = 0xDDC8 \]

2. How many zeros are in the binary representation of \(2^{10}\)?
   \[ \text{Sol: } 10 \]

3. How many ones are in the 16-bit two’s complement representation of \(-2^n\), if \(0 \leq n \leq 15\)?
   \[ \text{Sol: } 16 - n \]

4. Convert \(71_8\) from octal to binary.
   \[ \text{Sol: } 111001 \]
Section 2 [18 pts (4, 4, 4, 6)]: Logic

1. Draw a circuit that is true if and only if at least one of the inputs $a$, $b$, or $c$ is 1 and (in addition) input $d$ is 0.
   
   **Sol:** Should be an AND connecting an OR gate with 3 inputs $a, b, c$ on the one hand, and a NOT gate in front of $d$ on the other.

2. Write a logical formula in disjunctive normal form (clauses containing and’s, joined by or’s) that is equivalent to the circuit in the preceding problem. (The variable names should remain $a, b, c, d$.)
   
   **Sol:** $(a \land \neg d) \lor (b \land \neg d) \lor (c \land \neg d)$

3. Write a formula in conjunctive normal form (clauses containing or’s, joined by and’s) that is equivalent to $\neg(\neg a \land b) \land \neg(c \land \neg d)$.
   
   **Sol:** $(a \lor \neg b) \land (\neg c \lor d)$

4. Give a logical formula for a two-bit multiplexer that takes inputs $x_0, x_1, y$, and produces the value of $x_0$ if $y = 0$ and produces the value of $x_1$ if $y = 1$. (You can figure this out; it’s not meant to be memorized.)
   
   **Sol:** $(x_0 \land \neg y) \lor (x_1 \land y)$
Section 3 [18 pts (5,5,2,6)]: Modular Arithmetic and Algorithms

1. Use fast exponentiation (repeated squaring) to find $2^{65}$ (mod 5).
   \[2; \text{squaring up to } 2^4 \text{ gives 1, so further powers will also give 1, and thus } 2^{65} = 2^{64} \times 2 = 1 \times 2 = 2\]

2. Use Euclid’s algorithm to find the gcd of 63000 and 90000. Show your work.
   \[\text{Sol: } 9000 \text{ – the numbers in the Euclid calls are 90000, 63000, 27000, 9000}\]

3. Use the gcd from the preceding problem to find the lcm of 63000 and 90000. Show your work.
   \[\text{Sol: } 63000 \times 90000 / 9000 = 630000\]

4. Use Extended Euclid to find the multiplicative inverse of 9 (mod 31).
   \[\text{Sol: } 7\]
Section 4 [8 pts (2,2,4)]: Modular Cryptosystems

1. Suppose you receive a message that purports to be from Alice, along with a garbled message as an attachment. The message says that the garbled attachment is the same message as the very message you are reading, but encrypted with Alice’s private key to prove both came from her. If you know Alice’s public key \((e, n)\), what should you do to verify that the attachment was encrypted with the private key? (You can assume the message is short enough to be encoded as one number.)

**Sol:** “Encrypting” the attachment with the public key by converting the message to a number and raising it to the power of \(e \mod n\) should produce the original message. If it doesn’t, this isn’t from Alice.

2. Suppose I “double-encrypt” an RSA message by computing \(M' = M^e \mod n\), then \(M'' = (M')^e \mod n\). If \(d\) was the original private key, what effectively is the new private key?

**Sol:** \(d^2\), or \(d^2 \mod \phi(n)\), but not \(d^2 \mod n\)

3. How many different linear ciphers are there, modulo 26? (A valid linear cipher is a pair \((a, b)\) encoding an encryption formula \(y = ax + b \mod 26\) that can be inverted to decrypt. Omit the “identity” encryption \((1, 0)\).)

**Sol:** There are 12 numbers relatively prime to 26 for the coefficients \(a\), and 26 possible addends \(b\), so \(12 \times 26 = 312\), -1 for the identity = 311.
Section 5 [20 pts (1,2,2,2,3,3,5)]: Sets

Assume for the following questions that \( A = \{1, 2, 3\}, B = \{2, 3, 4, 5\}, C = \{4, 5, 6\} \), and the universe \( U = \{x : x \in \mathbb{N}, 0 \leq x \leq 10\} \).

1. What is \( A \cup B \cup C \)?
   \[ \text{Sol: } \{1, 2, 3, 4, 5, 6\} \]

2. What is \( A \cap C \)?
   \[ \text{Sol: } \emptyset \]

3. What is \( B - C \)?
   \[ \text{Sol: } \{2, 3\} \]

4. What is \( B - A \)?
   \[ \text{Sol: } \{4, 5\} \]

5. What is \( \overline{A \cap C} \)?
   \[ \text{Sol: } U \text{ or } \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\} \]

6. What is \( A \times (C - B) \)?
   \[ \text{Sol: } \{(1, 6), (2, 6), (3, 6)\} \]

7. What is the power set \( \mathcal{P}(C) \)?
   \[ \text{Sol: } \{\emptyset, \{4\}, \{5\}, \{6\}, \{4, 5\}, \{4, 6\}, \{5, 6\}, \{4, 5, 6\}\} \]

8. Suppose \(|P| = 10, |Q| = 20, |R| = 30, |P \cap Q| = 5, |P \cap R| = 2, |Q \cap R| = 5, |P \cap Q \cap R| = 1\).
   Find (a) \(|P \cup Q|\), (b) \(|P \cup Q \cup R|\).
   \[ \text{Sol: } (a) \ 10 + 20 - 5 = 25, \ (b) \ 10 + 20 + 30 - 2 \cdot 5 - 5 + 1 = 49 \]
Section 6 [18 pts (5, 6, 7)]: Counting

1. If I distributed 30 pieces of candy among 7 children on Halloween, what is the largest number of candies I can say for certain that some child must have received (by the generalized pigeonhole principle)?

   Sol: 5

2. A free email service requires users to have usernames that are exactly 8 characters long. These characters must be lowercase letters, except up to two of them can be periods instead. How many different usernames are possible under this scheme? (You can leave your answer unsimplified.)

   Sol: $26^8 + 8(26)^7 + \binom{8}{2}(26)^6$. \(\binom{8}{2}\) may appear as 28.

3. How many possible outcomes could a costume contest with 10 contestants have if there are first, second, and third place prizes and an arbitrary subset of the remaining contestants (as few as zero or as many as all that remain) designated as “honorable mention”? You need not simplify your answer.

   Sol: $10 \times 9 \times 8 \times 2^7 = 90 \times 2^{10} = 92160$