Name: _______________________

Math 181 – Practice Exam 3
Spring 2018
100 points possible

• Make sure to put your name on your exam!

• There are a total of 11 questions.

• Do not the exam booklet until you are told to start.

• Please write clearly and justify your answers.

• No materials other than a pen, pencil, and eraser.

• Stop working and close the exam when time is called.

• Please note that the questions are not necessarily in order of difficulty.

• Good luck. You have 50 minutes to complete the exam.
1. (20 points) True or false. Circle your answer.

(a) If you are using a decimation cipher with key 3, then all Cs in the plaintext will be replaced by Ms in the ciphertext.

True or False

(b) If you are using a Caesar cipher with a shift of 6 then all Ys in the plaintext will be replaced by Es in the ciphertext.

True or False

(c) The most common letter in the English language is a.

True or False

(d) The Last Diminisher method is envy-free.

True or False

(e) Divide and choose is Pareto optimal.

True or False

(f) When deciding who will get an organ that becomes available, the amount of time on the waiting list is one of the factors considered.

True or False

(g) The Adjusted Winner Procedure is equitable.

True or False

(h) The data encoding scheme $A \rightarrow 0$, $B \rightarrow 1$, $C \rightarrow 01$ is unambiguous.

True or False

(i) The numbers 15 and 32 are coprime.

True or False

(j) The RSA encryption algorithm is impossible to break.

True or False
2. (10 points) In a substitution cipher, each letter in the top row is replaced by the corresponding letter in the bottom row:

\[
\begin{align*}
&\text{ABCDEFGHIJKLMNOPQRSTUVWXYZ} \\
&\text{XVUQMCBPSWLDIHGONATYERFKZJ}
\end{align*}
\]

(a) Encrypt the following message:

ROSEBUD

(b) Decrypt the following message:

USYSJ MHLXH M
3. (12 points) Data Compression
   (a) Find the Huffman tree representing the following symbols and probabilities.

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Probability</th>
</tr>
</thead>
<tbody>
<tr>
<td>K</td>
<td>0.03</td>
</tr>
<tr>
<td>L</td>
<td>0.20</td>
</tr>
<tr>
<td>M</td>
<td>0.07</td>
</tr>
<tr>
<td>N</td>
<td>0.31</td>
</tr>
<tr>
<td>O</td>
<td>0.34</td>
</tr>
<tr>
<td>P</td>
<td>0.05</td>
</tr>
</tbody>
</table>

   (b) Use the Huffman code that you constructed in part (b) to encode the text below:

   POMP
4. (10 points) Answer the following using modular arithmetic.

(a) (2 points) Hannah was born on a Tuesday. On what day of the week was her first birthday? (Assume that there were no leap days in her first year of life.)

(b) (2 points) Today is Friday. What day of the week will it be in 100 days?

(c) (2 points) What day of the week was it 49 days ago?

(d) (4 points) Find the smallest positive integer that evaluates the following expressions.

45 (mod 12) =

5 (mod 17) =

30 (mod 7) =

18 (mod 6) =
5. (9 points) Solve the following equations (your answer should be of the form \( x = k \) (mod \( n \)) where \( 0 \leq k \leq n - 1 \)).

(a) \( x - 4 = 3 \) (mod 9)

(b) \( 5 + x = 4 \) (mod 7)

(c) \( 3x = 2 \) (mod 5)
6. (5 points) Convert the following number written in binary (base 2) to decimal (base 10).

1100111

7. (5 points) Convert the following number written in decimal (base 10) to base 5.

132
8. (8 points) You are planning to use the RSA with

\[ N = 33. \]

Does the pair \( e = 3, \ d = 17 \) form a valid public/private key pair?
9. (10 points) Alice, Bob, and Carol are trying to divide two cakes, Cake 1 and Cake 2. Suppose that Alice divides the cake as follows for the Lone Divider Procedure.

(a) For Cake 1, if Bob and Carol both only approve of slices X and Y, then what is a final allocation of the cake using the Lone Divider Procedure?

(b) For Cake 2, if Bob and Carol both only approve of slice X, then what is the final allocation of the cake using the Lone Divider Procedure?
10. (5 points) Alice and Bob inherit a cabin. Use the Knaster inheritance procedure to determine a fair division of the cabin.

<table>
<thead>
<tr>
<th>Item</th>
<th>Alice</th>
<th>Bob</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cabin</td>
<td>$40,000</td>
<td>$80,000</td>
</tr>
</tbody>
</table>

11. (6 points) I used a Caesar cipher with a shift of 6 and got the following encrypted message. Decrypt the message.

UYQKK CUC CUC