EE 418 Sample Midterm

Department of Electrical Engineering
University of Washington, Seattle, WA 98195

Posted: Oct. 23th 2017; Due: N/A
Solution will be posted on Oct. 27th (Fri), 2017

This sample exam is for your benefit. You are advised to read lecture notes, quiz and the homework assignments in preparing for the exam. Exam as you were told is open book, open notes and open home works.

Mapping of alphabets to numerals

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
<th>G</th>
<th>H</th>
<th>I</th>
<th>J</th>
<th>K</th>
<th>L</th>
<th>M</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>10</td>
<td>11</td>
<td>12</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>N</th>
<th>O</th>
<th>P</th>
<th>Q</th>
<th>R</th>
<th>S</th>
<th>T</th>
<th>U</th>
<th>V</th>
<th>W</th>
<th>X</th>
<th>Y</th>
<th>Z</th>
</tr>
</thead>
<tbody>
<tr>
<td>13</td>
<td>14</td>
<td>15</td>
<td>16</td>
<td>17</td>
<td>18</td>
<td>19</td>
<td>20</td>
<td>21</td>
<td>22</td>
<td>23</td>
<td>24</td>
<td>25</td>
</tr>
</tbody>
</table>

Probabilities of occurrence of the 26 English letters

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
<th>G</th>
<th>H</th>
<th>I</th>
<th>J</th>
<th>K</th>
<th>L</th>
<th>M</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.082</td>
<td>0.015</td>
<td>0.028</td>
<td>0.043</td>
<td>0.127</td>
<td>0.022</td>
<td>0.020</td>
<td>0.061</td>
<td>0.070</td>
<td>0.002</td>
<td>0.008</td>
<td>0.040</td>
<td>0.024</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>N</th>
<th>O</th>
<th>P</th>
<th>Q</th>
<th>R</th>
<th>S</th>
<th>T</th>
<th>U</th>
<th>V</th>
<th>W</th>
<th>X</th>
<th>Y</th>
<th>Z</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.067</td>
<td>0.075</td>
<td>0.019</td>
<td>0.001</td>
<td>0.060</td>
<td>0.063</td>
<td>0.091</td>
<td>0.028</td>
<td>0.010</td>
<td>0.023</td>
<td>0.001</td>
<td>0.020</td>
<td>0.001</td>
</tr>
</tbody>
</table>

1. The following ciphertext was encrypted using the substitution cipher. Determine the correct plaintext using frequency analysis and additional hints that ciphertext ‘C’ maps to plaintext ‘d,’ ciphertext ‘D’ maps to plaintext ‘o,’ ciphertext ‘I’ maps to plaintext ‘p’ and ciphertext ‘G’ maps to plaintext ‘s.’

AB CD EDF GFDI IJLKMEN
OBPKQGB AB NBF DJC.
AB NBF DJC OBPKQGB AB
GFDI IJLKMEN
–OBTEKTC GUAK

2. What are the two last digits of $9^9$? (You may use the fact that last two digits of $9^9$ is 89)

3. Solve for $x$ such that $17x \equiv 1 \pmod{53}$. 
4. Given that a plaintext comp was encrypted to ciphertext SANB using a Hill cipher with a 2×2 matrix as the key, $K$, find $K$.

5. What are the number of integers that are smaller than 515 and are relatively prime to 515?

6. Let $a_1a_2a_3\cdots a_n$ be an $n$ digit number with $a_i$ on the $i^{th}$ digit $0 \leq a_i < 10$ where $1 \leq i \leq n$. Using your good knowledge gained from the initial weeks of the class, show that the number $a_1a_2a_3\cdots a_n$ is divisible by 3 if the sum of the digits is a multiple of 3. (Hint is note that $10 = 1 \pmod{3}$.)

7. You are given a composite number $n = 11413$. Using the random square method discussed in class, we want to find two integers $x, y$ such that $x \not\equiv y \pmod{n}$ but $x^2 \equiv y^2 \pmod{n}$ and factor the number $n$. IF you are given that the smaller number is given as $x = 6$, what is/are the values of the other integer $y$? What are the factors of $n$? Show steps (Hint: $107^2 = 11449$).

8. Solve the following linear congruent equations.

\[
\begin{align*}
X & \equiv 1 \pmod{3} \\
X & \equiv 2 \pmod{5} \\
X & \equiv 4 \pmod{7}
\end{align*}
\]

9. Homer propose a modification of the Affine Cipher by including two letters (used by Homer often): "" (blank) = 26, "?" = 27. So there are 28 letters, hence mod 28 (i.e. letters A to Z, "", "?"). Homer then broadcasts a ciphertext. Lisa wants to decrypt the ciphertext and hence does a frequency analysis which reveals that most common letter in the ciphertext is "J" and second most common is "L". Lisa also knows that most common letters in english text written with the 28 possible letters are "" (blank) followed by E. Can you show that Lisa is indeed successful in finding the key $K = (a; b)$ used by Homer for obtaining the ciphertext.

10. In the class, it was shown that if gcd$(a, b) = 1$, then $\phi(ab) = \phi(a)\phi(b)$. If instead gcd$(a, b) = 2$, then what is the expression for $\phi(ab)$ in terms of $\phi(a)$ and $\phi(b)$?

11. Suppose you are using RSA with modulus $n = pq$ with public key $b$ and private key $a$. You however, decide to restrict your messages to the numbers $m$ satisfying property $m^{1000} \equiv 1 \pmod{n}$.

(a) Show that if the private key $a$ satisfies the equation $ab = 1 \pmod{1000}$, then $a$ can be used to decrypt these messages.

(b) Assume that both $p$ and $q$ are congruent to 1 under $\pmod{1000}$. Determine how many messages satisfy $m^{1000} \equiv 1 \pmod{n}$. You may assume and use the fact that $m^{1000} \equiv 1 \pmod{r}$ has 1000 solutions when $r$ is a prime and satisfies $r = 1 \pmod{1000}$. 
12. Consider a linear feedback shift register that works mod 3 instead of mod 2, so that the \((i + m)\)-th element of the key stream is given by

\[
z_{i+m} = \sum_{j=0}^{m-1} c_j z_{i+j} \pmod{3}.
\] (4)

Let a recurrence of length \(m = 2\) be used to generate the sequence 1, 1, 0, 2, 2, 0, 1, 1. Compute the next four elements of the key stream.

13. Suppose you have a language with only two letters \(a, b\) and they occur with frequencies 0.8 and 0.2. The following cipher was encrypted using a Vigenere cipher with the shift of mod 2 instead of mod 26.

\[
\text{BABBBBABBBA}
\]

Show that the most likely key length is \(m = 2\).