This exam has 6 problems and 7 numbered pages.

Name: ________________________________  Instructor: ______Michael Kozdron_____

You have 75 minutes to complete this exam. Show all work neatly and in order, and clearly indicate your final answers. Answers must be justified whenever possible in order to earn full credit.

Unless otherwise specified, no credit will be given for unsupported answers, even if your final answer is correct. Points will be deducted for incoherent, incorrect, and/or irrelevant statements. A formula page will be provided, and calculators are permitted, but no other aids are allowed.

You are allowed to use standard notation. However, any new notation or abbreviations that you introduce must be clearly defined.

This examination consists of 6 problems and is worth 100 total points. You must answer all of the questions in the space provided.

Good luck!

<table>
<thead>
<tr>
<th>Problem</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
</tr>
</tbody>
</table>

TOTAL: _________
The numerical equivalents of the letters are as follows:

<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>
<tr>
<td>N</td>
<td>O</td>
<td>P</td>
<td>Q</td>
<td>R</td>
<td>S</td>
<td>T</td>
<td>U</td>
<td>V</td>
<td>W</td>
<td>X</td>
<td>Y</td>
<td>Z</td>
</tr>
<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>

\[ A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \]

\[ \text{det}(A) = ad - bc \]

\[ A^{-1} = \text{det}(A)^{-1} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \]

\[ I = \frac{n_0(n_0 - 1) + \cdots + n_{25}(n_{25} - 1)}{n(n - 1)} \]

\[ k = \frac{0.0265n}{(0.065 - I) + n(I - 0.0385)} \]

\# digits in binary representation of \( x = \left\lfloor \frac{\ln x}{\ln 2} \right\rfloor + 1 \)
1. (16 points) Suppose that $A = \begin{bmatrix} -2 & 1 \\ -3 & 2 \end{bmatrix}$ and $B = \begin{bmatrix} -1 & 2 \\ 3 & 3 \end{bmatrix}$.

(a) Compute $AB \pmod{26}$.

(b) Let $C = AB \pmod{26}$ be the matrix that you computed in (a). Determine $C^{-1} \pmod{26}$.

(continued)
2. (16 points)

(a) Convert the number with base twenty-six representation ELVES to decimal (base ten).

(b) Convert the number with binary (base two) representation 11011001 to decimal.

(c) Convert the number with decimal representation 123 to octal (base eight).

(d) Let $a = 110110$ and $b = 10101$ be two binary numbers. Compute the binary numbers $a + b$ and $a - b$. 

(continued)
3. (16 points)

(a) Encipher the message GANDALF THE GREY using the Vigenère method with the keyword BILBO.

(b) Suppose that the Vigenère encipherment produced the ciphertext PKSFIH QDNB when the three-letter key string XV_ was used. (The last letter of the key string is not yet known.) Decipher as much of the plaintext as possible, and based on the plaintext you obtain, determine the missing plaintext letters and the third letter of the key string.
4. (16 points)

(a) The ciphertext ELPF resulted from a Hill encipherment with the key matrix \( A = \begin{bmatrix} 4 & 3 \\ 3 & 1 \end{bmatrix} \).
Decipher the message.

(b) The ciphertext BAOI resulted from a Hill encipherment of the plaintext BASE. Based on this information, determine the key matrix \( A \).
5. (20 points) A message was enciphered using the Vigenère method with a keyword of a certain length. The ciphertext is shown below, and certain repeated letter groups are underlined.

YYFHS WZBJG KFFWV JVZYS SBWQU XLBGS WKVHG PPGHJ
JETRF YYSGK FITOC WUGLB YYSLF MRZOG TWGWC SVBLB
JWCUA TIHDZ RVGBC TDSGH TUWHC SVTRF YYSGO WBZRF
IFBKW XUOUY YYFRB JZBFW JCQQR TWARF IFFZV JISWV
JJVDR TNGOW JFBHF NEUWC WLZHJ MVAZD QFBHF NEUWC
KZBGH MVARB JIQWU YFPWU SXHKS RRZOO SUXWH MVRF
PESVG GBGKH MVALB YYSOO SUCIA TIRRF BYSUS YYSVV
FUCZG QZS

(a) From the spacing between the repeated letter groups, use Kasiski’s test to estimate the length of the keyword.
The distribution (i.e., letter counts) of the 288 characters in the ciphertext is as follows.

<table>
<thead>
<tr>
<th></th>
<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></td>
<td>6</td>
<td>18</td>
<td>10</td>
<td>5</td>
<td>4</td>
<td>21</td>
<td>17</td>
<td>14</td>
<td>8</td>
<td>12</td>
<td>6</td>
<td>6</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<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></td>
<td>3</td>
<td>10</td>
<td>4</td>
<td>6</td>
<td>15</td>
<td>21</td>
<td>10</td>
<td>14</td>
<td>17</td>
<td>21</td>
<td>3</td>
<td>18</td>
<td>14</td>
</tr>
</tbody>
</table>

(b) Suppose that 4 letters from this ciphertext are picked at random. Write down (but do not evaluate) an expression to represent the probability that these 4 letters are identical.

(c) Suppose that 4 letters from this ciphertext are picked at random. Write down (but do not evaluate) an expression to represent the probability that either “a pair of A’s and a pair of B’s” is drawn or “three J’s and one K” is drawn.
6. (16 points) Consider the 5-bit linear feedback shift register given by

\[
\begin{align*}
  b_1' &\leftarrow b_2 \\
  b_2' &\leftarrow b_3 \\
  b_3' &\leftarrow b_4 \\
  b_4' &\leftarrow b_5 \\
  b_5' &\leftarrow b_3 + b_2 + b_1 
\end{align*}
\]

with initial values \( b_5 = 1, b_4 = 0, b_3 = 0, b_2 = 1, b_1 = 0. \) Compute the first 8 values of \( b_1, \)
and use them to do a binary Vigenère encipherment of the plaintext 11101101.

(The End.)