1) (10 pts) The cipher text "PAPCIJGXCV" was encrypted using the shift cipher with an encryption key of 15. What is the corresponding plaintext?

Solution

<table>
<thead>
<tr>
<th>Cipher</th>
<th>P(15)</th>
<th>A(0)</th>
<th>P(15)</th>
<th>C(2)</th>
<th>I(8)</th>
<th>J(9)</th>
<th>G(6)</th>
<th>X(23)</th>
<th>C(2)</th>
<th>V(21)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key</td>
<td>15</td>
<td>15</td>
<td>15</td>
<td>15</td>
<td>15</td>
<td>15</td>
<td>15</td>
<td>15</td>
<td>15</td>
<td>15</td>
</tr>
<tr>
<td>Plain</td>
<td>0</td>
<td>-15</td>
<td>0</td>
<td>-13</td>
<td>-7</td>
<td>-6</td>
<td>-9</td>
<td>9</td>
<td>-13</td>
<td>6</td>
</tr>
<tr>
<td>mod 26</td>
<td>0(A)</td>
<td>11(L)</td>
<td>0(A)</td>
<td>13(N)</td>
<td>19(T)</td>
<td>20(U)</td>
<td>17(R)</td>
<td>9(I)</td>
<td>13(N)</td>
<td>6(G)</td>
</tr>
</tbody>
</table>

Grading: 1 pt per letter, 4/10 if they encrypted instead of decrypting.

ALANTURING

2) (10 pts) The set of letters S consists of 5 As, 10 Bs, 15 Cs, 10 Ds, and 10 Es. The set of letters T consists of 15 As, 25 Bs, 30 Cs, 15 Ds and 15 Es. What is the mutual index of coincidence between sets S and T? Leave your answer as a fraction in lowest terms.

Solution

\[ MIC = \frac{5 \times 15 + 10 \times 25 + 15 \times 30 + 10 \times 15 + 10 \times 15}{(5 + 10 + 15 + 10 + 10)(15 + 25 + 30 + 15 + 15)} \]

\[ MIC = \frac{25(3 + 10 + 18 + 6 + 6)}{50 \times 100} = \frac{43}{200} \]

Grading: 6 pts plugging into formula, 2 pts getting unreduced fraction, 2 pts simplifying to lowest terms, 3/10 if they calculated some sort of Index of Coincidence instead.
3) (20 pts) Consider an affine cipher for a language with 61 letters. If an encryption function for this alphabet is \( g(x) = (36x + 29) \mod 61 \), what is the corresponding decryption function? (Your function must be of the form \( g^{-1}(x) = (ax + b) \mod 61 \), where \( a \) and \( b \) are in between 0 and 60, inclusive.)

**Solution**

We ultimately will need to find \( 36^{-1} \mod 61 \), so let's do this first, via the Extended Euclidean Algorithm:

\[
egin{align*}
61 & = 1 \times 36 + 25 \\
36 & = 1 \times 25 + 11 \\
25 & = 2 \times 11 + 3 \\
11 & = 3 \times 3 + 2 \\
3 & = 1 \times 2 + 1 \\
3 - 1 \times 2 & = 1 \\
3 - (11 - 3 \times 3) & = 1 \\
4 \times 3 - 1 \times 11 & = 1 \\
4(25 - 2 \times 11) - 1 \times 11 & = 1 \\
4 \times 25 - 9 \times 11 & = 1 \\
4 \times 25 - 9(36 - 25) & = 1 \\
13 \times 25 - 9 \times 36 & = 1 \\
13(61 - 36) - 9 \times 36 & = 1 \\
13 \times 61 - 22 \times 36 & = 1 
\end{align*}
\]

Taking this equation \( \mod 61 \) we find that \( 36^{-1} \equiv -22 \equiv 39 \) (mod 61)

Now, to find \( g^{-1}(x) \):

\[
\begin{align*}
x & = (36 \cdot g^{-1}(x) + 29) \mod 61 \\
x - 29 & = 36 \cdot g^{-1}(x) \mod 61 \\
39(x - 29) & = 39 \times 36 \cdot g^{-1}(x) \mod 61 \\
g^{-1}(x) & = (39x - 39 \times 29) \mod 61 \\
g^{-1}(x) & = (39x - 1131) \mod 61 \\
g^{-1}(x) & = (39x - 1131) \mod 61 \\
g^{-1}(x) & = (39x + 28) \mod 61 
\end{align*}
\]

**Grading:** Work for \( 36^{-1} \mod 61 \) is 10 pts, work for inverse function is 10 pts. (Only 1 pt off if last term isn't multiplied and modded.)
4) (15 pts) Consider a Hill cipher for an alphabet of size 45. What is the corresponding decryption key for the encryption key \( \begin{pmatrix} 2 & 17 \\ 3 & 11 \end{pmatrix} \)?

**Solution**
The determinant is \( 2 \times 11 - 3 \times 17 = -29 \equiv 16 \mod 45 \). We must find \( 16^{-1} \mod 45 \):

\[
\begin{align*}
45 &= 2 \times 16 + 13 \\
16 &= 1 \times 13 + 3 \\
13 &= 4 \times 3 + 1 \\
13 - 4 \times 3 &= 1 \\
13 - 4(16 - 13) &= 1 \\
13 - 4 \times 16 + 4 \times 13 &= 1 \\
5 \times 13 - 4 \times 16 &= 1 \\
5(45 - 2 \times 16) - 4 \times 16 &= 1 \\
5 \times 45 - 14 \times 16 &= 1 \\
\end{align*}
\]

Thus, \( 16^{-1} \equiv -14 \equiv 31 \mod 45 \).

The decryption key is \( 31 \begin{pmatrix} 11 & -17 \\ -3 & 2 \end{pmatrix} = \begin{pmatrix} 341 \mod 45 & -527 \mod 45 \\ -93 \mod 45 & 62 \mod 45 \end{pmatrix} = \begin{pmatrix} 26 & 13 \\ 42 & 17 \end{pmatrix} \)

**Grading:** Work for inverse is 9 pts, 5 pts for plugging into formula for inversion, 1 pt for modding everything.
5) (12 pts) Encrypt the plaintext "WEAREWORKING" using the Vigenere cipher and the keyword "HOUSE".

Solution

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Key</td>
<td>7</td>
<td>14</td>
<td>20</td>
<td>18</td>
<td>4</td>
<td>7</td>
<td>14</td>
<td>20</td>
<td>18</td>
<td>4</td>
<td>7</td>
<td>14</td>
</tr>
<tr>
<td>Plain</td>
<td>29</td>
<td>18</td>
<td>20</td>
<td>35</td>
<td>8</td>
<td>29</td>
<td>28</td>
<td>37</td>
<td>28</td>
<td>12</td>
<td>20</td>
<td>20</td>
</tr>
<tr>
<td>mod26</td>
<td>3</td>
<td>18</td>
<td>20</td>
<td>9</td>
<td>8</td>
<td>3</td>
<td>2</td>
<td>11</td>
<td>2</td>
<td>12</td>
<td>20</td>
<td>20</td>
</tr>
<tr>
<td>Res</td>
<td>D</td>
<td>S</td>
<td>U</td>
<td>J</td>
<td>I</td>
<td>D</td>
<td>C</td>
<td>L</td>
<td>C</td>
<td>M</td>
<td>U</td>
<td>U</td>
</tr>
</tbody>
</table>

DSUJIDCLCMUU

Grading: 1 pt per letter, 6/12 if decrypted

6) (14 pts) Decrypt the message, “ABEPCLCFWNAMNX”, which was enciphered using the Playfair cipher with the key “TURTLES”. Note: The padding character used was “Q”.

Solution

Here is the Playfair square:

<table>
<thead>
<tr>
<th>T</th>
<th>U</th>
<th>R</th>
<th>L</th>
<th>E</th>
</tr>
</thead>
<tbody>
<tr>
<td>S</td>
<td>A</td>
<td>B</td>
<td>C</td>
<td>D</td>
</tr>
<tr>
<td>F</td>
<td>G</td>
<td>H</td>
<td>I</td>
<td>J</td>
</tr>
<tr>
<td>M</td>
<td>N</td>
<td>O</td>
<td>P</td>
<td>Q</td>
</tr>
<tr>
<td>V</td>
<td>W</td>
<td>X</td>
<td>Y</td>
<td>Z</td>
</tr>
</tbody>
</table>

AB → SA
EP → LQ
CL → LY
CF → SI
WN → NG
AM → SN
NX → OW

Plaintext with padding 'Q' removed: SALLYSINGSNOW

Grading: 3 pts Playfair square, 7 pts total for encrypting, Alternate 2 pts, 1 pt off per incorrect pair (total 11 pts)
7) (15 pts) Determine $59^{-1} \mod 107$

**Solution**

\[
107 = 1 \times 59 + 48 \\
59 = 1 \times 48 + 11 \\
48 = 4 \times 11 + 4 \\
11 = 2 \times 4 + 3 \\
4 = 1 \times 3 + 1
\]

\[
4 - 1 \times 3 = 1 \\
4 - (11 - 2 \times 4) = 1 \\
3 \times 4 - 1 \times 11 = 1 \\
3(48 - 4 \times 11) - 1 \times 11 = 1 \\
3 \times 48 - 13 \times 11 = 1 \\
3 \times 48 - 13(59 - 48) = 1 \\
16 \times 48 - 13 \times 59 = 1 \\
16(107 - 59) - 13 \times 59 = 1 \\
16 \times 107 - 29 \times 59 = 1
\]

Thus, $59^{-1} \equiv -29 \equiv 78 \mod 107$.

Grading: 6 pts Euclidean, 9 pts Extended, total 5/15 if they gave an answer of 2 (happens if the first step of the Euclidean is $107 = 1 \times 59 + 58$)

---

8) (4 pts) In which Swiss town is Gruyere cheese made? **Gruyere** (Give to all)