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 IJKLMEN
OBPKQGB AB NBF DJC.
AB NBF DJC OBPKQGB AB
GF DI IJKLMEN
–OBTEKTC GUKA

Solution: The letter frequency table of the cipher text is

<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>5</td>
<td>10</td>
<td>4</td>
<td>7</td>
<td>4</td>
<td>5</td>
<td>4</td>
<td>0</td>
<td>4</td>
<td>4</td>
<td>6</td>
<td>2</td>
<td>2</td>
<td>2</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>
<td></td>
</tr>
<tr>
<td>2</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

The correct plaintext is “We do not stop playing because we get old. We get old because we stop playing. -Bernard Shaw”

2. What are the two last digits of of $9^{9^9}$?

Solution: The last two digits can be obtained by taking modulo 100. Hence, we need to find $9^{9^9} \pmod{100}$. First, note that

$$9^{40} = 1 \pmod{100}$$  \hspace{1cm} (1)

from the Euler’s theorem. Therefore, $9^{81} = 9 \pmod{100}$. We have

$$9^{9^2} = 9 \pmod{100}.$$ Now,

$$9^{9^9} = (9^{9^2})^{9^7} = 9^{9^7} \pmod{100}$$  \hspace{1cm} (2)
We can continue this process with $9^7$ until we have

$$9^9 = 9^9 \pmod{100} \quad (3)$$

From the hint, the last two digits are 89.

3. Solve for $x$ such that $17x \equiv 1 \pmod{53}$.
   **Solution:** We can use the extended Euclidean algorithm to find the inverse of 17 over modulo 53.

   $$\begin{align*}
   53 &= 17 \cdot 3 + 2 \\
   17 &= 2 \cdot 8 + 1
   \end{align*} \quad (4)$$

At this point, we have

$$1 = 17 - 2 \cdot 8 = 17 - (53 - 17 \cdot 3) \cdot 8 = 25 \cdot 17 - 8 \cdot 53 \quad (6)$$

Therefore, the inverse of 17 is given as $25 \pmod{53}$.

4. Given that a plaintext comp was encrypted to ciphertext SANB using a Hill cipher with a $2 \times 2$ matrix as the key, $K$, find $K$.
   **Solution:** We have the plaintext comp mapping to $[2,14,12,15]$ and ciphertext SANB mapping to $[18,0,13,1]$. In Hill cipher, the encryption is given as $y = xK$. Therefore, we need to solve the system of equations given as

   $$\begin{align*}
   2k_{11} + 14k_{21} &= 18 \pmod{26} \\
   12k_{11} + 15k_{21} &= 13 \pmod{26} \\
   2k_{12} + 14k_{22} &= 0 \pmod{26} \\
   12k_{12} + 15k_{22} &= 1 \pmod{26}
   \end{align*} \quad (7-10)$$

Solving these system of equations, we obtain

$$k_{11} = 2, k_{12} = 5, k_{21} = 1, k_{22} = 3 \quad (11)$$

which is a well-defined key since the determinant of $K$ is given as

$$\text{det}(K) = k_{11}k_{22} - k_{12}k_{21} = 6 - 5 = 1 \quad (12)$$

which is relatively prime to 26.

5. What are the number of integers that are smaller than 515 and are relatively prime to 515?
   **Solution:** This is the definition of the totient function $\phi$. Hence we need to find $\phi(515)$.

   $$\phi(515) = \phi(5 \cdot 103) = \phi(5) \cdot \phi(103) = 4 \cdot 102 = 408 \quad (13)$$
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 \( 10 \equiv 1 \pmod{3} \).)

Solution: Let \( m = a_1a_2a_3 \cdots a_n \) be the \( n \)-th digit number with \( a_i \) as the \( i \)-th digit. The number \( m \) can be written as

\[
m = \sum_{i=1}^{n} a_i10^{n-i}.
\]

The goal is to show that \( m \) is divisible by 3 if and only if \( \sum_{i=1}^{n} a_i \) is divisible by 3. By definition of the modulus operator, this is equivalent to

\[
m \equiv 0 \pmod{3} \iff \sum_{i=1}^{n} a_i \equiv 0 \pmod{3}.
\]

To prove this, it suffices to show that

\[
m \equiv \sum_{i=1}^{n} a_i \pmod{3}.
\]

We have

\[
m \equiv \sum_{i=1}^{n} a_i10^{n-i} \equiv \sum_{i=1}^{n} a_i1^{n-i} \equiv \sum_{i=1}^{n} a_i \pmod{3},
\]

where the second congruence relation follows from the fact that \( 10 \equiv 1 \pmod{3} \).

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 \( x \neq y \pmod{n} \) but \( x^2 = y^2 \pmod{n} \) 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.

Solution: The goal is to find an integer \( y \) satisfying \( y^2 \equiv 6^2 \equiv 36 \mod{11413} \), which is equivalent to \( y^2 \equiv 36 + 11413\mu \) for some integer \( \mu \). First, we try \( \mu = 1 \), and find that \( y = 107 \) satisfies 1072 = 11449 = 11413+36 = 36 mod 11413. Thus \( 6^2 \equiv 107^2 \mod{11413} \), i.e., \( 107^2 - 6^2 \equiv 0 \mod{11413} \).

We now have that \( (107 - 6)(107 + 6) \equiv 0 \mod{11413} \), and so \( 101)(113) = k11413 \) for some integer \( k \). In fact, \( (101)(113) = 11413 \), which implies that the factors of \( n \) are \( 101 \) and \( 113 \).

8. Solve the following linear congruence equations.

\[
X = 1 \pmod{3} \quad (14)
\]
\[
X = 2 \pmod{5} \quad (15)
\]
\[
X = 4 \pmod{7} \quad (16)
\]
Solution: The problem can be solved using the Chinese Remainder Theorem, which gives

\[ X = \sum_{i=1}^{r} a_i M_i y_i \mod M, \]

where \( m_i \)'s are the moduli, \( a_i \) are the right-hand sides of the above equations, \( M_i = M/m_i \), and \( y_i = M_i^{-1} \mod m_i \). We have that \( m_1 = 3 \), \( m_2 = 5 \), and \( m_3 = 7 \). Hence \( M = 105 \), \( M_1 = 35 \), \( M_2 = 21 \), and \( M_3 = 15 \). Furthermore, \( y_1 = 35^{-1} \mod 3 = 2^{-1} \mod 3 = 2 \), \( y_2 = 21^{-1} \mod 5 = 1^{-1} \mod 5 = 1 \), and \( y_3 = 15^{-1} \mod 7 = 1 \). This implies

\[ X = 1(35)(2) + 2(21)(1) + 4(15)(1) = 172 = 67 \mod 105. \]

Thus \( X = 67 \).

9. The encryption method in the modified affine cipher is given as

\[ y = ax + b \quad \text{(mod 28)} \]  

Since the most frequent plainletter is now blank, which corresponds to \( x = 26 \), maps to J, which corresponds to \( y = 9 \), we can find one equation

\[ 9 = 26a + b \quad \text{(mod 28)} \]  

and the next frequent plainletter is e, which corresponds to \( x = 4 \), maps to L, which corresponds to \( y = 11 \), we find another equation

\[ 11 = 4a + b \quad \text{(mod 28)} \]  

Subtracting the second equation from the first, we obtain

\[ -2 = 22a \quad \text{(mod 28)} \]  

At this point, \( a \), cannot be found directly, since inverse of 22 is ill-defined in modulo 28. However, this equation can be reduced to

\[ -1 = 11a \quad \text{(mod 14)} \]  

It can be seen that \( a = 5 \), and \( b = -9 = 19 \quad \text{(mod 28)} \).

10. If \( \gcd(a, b) = 2 \), then without loss of generality, we can write

\[ a = 2^m z_1, b = 2 z_2 \]  

where \( z_1 \) and \( z_2 \) are relatively prime. Then

\[ \phi(ab) = \phi(2^{m+1} z_1 z_2) = \phi(2^{m+1})\phi(z_1)\phi(z_2) = 2^m \phi(z_1)\phi(z_2) \]  

but at the same time, we have

\[ \phi(a) = 2^{m-1}\phi(z_1), \phi(b) = 2\phi(z_2) = \phi(z_2) \]  

Therefore, \( \phi(ab) = 2 \cdot \phi(a) \cdot \phi(b) \).
11. (a) We need to show that
\[ m^{ab} = m \pmod{n} \] (25)
From the relation \( ab = 1 \pmod{1000} \), we have \( ab = \lambda 1000 + 1 \) for some integer \( \lambda \). Therefore
\[ m^{ab} = m \cdot (m^{1000})^\lambda = m \pmod{n} \] (26)
since we are restricting the set of messages \( m \) for those that satisfy
\[ m^{1000} = 1 \pmod{n} \] (27)
(b) We know that \( m^{1000} = 1 \pmod{n} \) if and only if \( m^{1000} = 1 \pmod{p} \) and \( m^{1000} = 1 \pmod{q} \). Let \( m_1, m_2 \) be values such that
\[ m_1^{1000} = 1 \pmod{p}, m_2^{1000} = 1 \pmod{q} \] (28)
Let \( X \) be the solution to the system of equations
\[ X = m_1 \pmod{p} \] (29)
\[ X = m_2 \pmod{q} \] (30)
From the Chinese Remainder Theorem, we know that there exists a unique solution \( X \) in modulo \( n = pq \) that satisfies the system of equations. Moreover,
\[ X^{1000} = m_1^{1000} = 1 \pmod{p}, X^{1000} = m_2^{1000} = 1 \pmod{q} \] (31)
Therefore \( X^{1000} = 1 \pmod{pq} \). Therefore, for every pair \((m_1, m_2)\), there exists a unique mapping to \( X \) in modulo \( n \). Hence there are one million solutions.

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

**Answer:** Based on the sequence 1, 1, 0, 2, 2, 0, 1, 1, we have the equations
\[ c_0 \cdot 1 + c_1 \cdot 1 = 0 \pmod{3} \] (32)
\[ c_0 \cdot 1 + c_1 \cdot 0 = 2 \pmod{3} \] (33)
Combining these equations yields \( c_0 = 2, c_1 = 1 \). Hence the next four elements are 0, 2, 2, 0.

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.

\[
\text{BABBBBABBB}
\]
Show that the most likely key length is $m = 2$.

**Answer:** The autocorrelation of the given language is given as $(0.8)^2 + (0.2)^2 = 0.68$. Since the length of the ciphertext is 10, there are two possible key length values $m = 2$ and $m = 5$. (Or as mentioned in the case $m = 1$ is also valid. In this case, however, the cryptosystem reduces down to *shift cipher*). By breaking the ciphertext as blocks of two, and we obtain two cipherblocks.

$$
y_1 = BBBAB \quad (34)
y_2 = ABBBB \quad (35)
$$

We see that for each of the cipherblocks, the autocorrelation matches 0.68. On the other hand, when we break the ciphertext as every 5 letters, we obtain five sub-blocks given as

$$
y_1 = BB \quad (36)
y_2 = AA \quad (37)
y_3 = BB \quad (38)
y_4 = BB \quad (39)
y_5 = BB \quad (40)
$$

For each of the cipherblocks, the frequency distribution is biased, in the sense the autocorrelation value is all 1, which is different from the autocorrelation of the language of 0.68. This leads us to conclude that the most likely key length is $m = 2$. However, also note that as mentioned in the class, because the ciphertext length is small, the frequency test may not be accurate.