1. You discover a cipher which you know is a shift cipher. However, all of it has faded with time and is unreadable, except a single two letter word. The two letter ciphertext is EZ. Is this enough to determine the shift? Explain. Solution: Looking at all possible shifts of EZ gives us (leaving out the last 3)

E F G H I J K L M N O P Q R S T U V W X Y Z A B C D
Z A B C D E F G H I J K L M N O P Q R S T U V W

We already see two possible words, TO and UP. So we can not determine what the correct shift is.

2. Decipher the ciphertext FALL

using an affine cipher with key $a = 3, b = 6$.

Solution: The decipherment function is $x = (3^{-1})(y - 6) \mod 26 = 9(y - 6) \mod 26$. Since F is 5, the plaintext must be $9 \cdot (5 - 6) \mod 26 = -9 \mod 26 = 17 \mod 26$, or R. Since A = 0, the plaintext must be $9(0 - 6) \mod 26 = -54 \mod 26 = -2 \mod 26 = 24 \mod 26$, or X. Since L = 11 the plaintext must be $9(11 - 6) \mod 26 = 45 \mod 26 = 19$, or T. So the final answer is RXTT.

3. An affine cipher enciphers E as F and enciphers T as G. What letter does it encipher O as?
Solution: E is 4, F is 5, T is 19 and G is 6. So we know that
\[ 5 \equiv 4a + b \mod 26. \]
\[ 6 \equiv 19a + b \mod 26. \]
Subtracting the bottom from the top,
\[ 1 \equiv 15a \mod 26. \]
In other words, \( a \) is the multiplicative inverse of 15 mod 26. By trial and error (only checking numbers relatively prime to 26) we find that \( a = 7 \). To solve for \( b \), we plug in \( a = 7 \) into one of the equations.
\[ 5 \equiv 4 \cdot 7 + b \mod 26. \]
\[ 5 \equiv 28 + b \mod 26. \]
So \( b = 3 \). Finally, as \( O = 14 \) it is enciphered by
\[ y = 7 \cdot 14 + 3 \mod 26 = 101 \mod 26 = 23. \]
Thus the final answer is X.

4. Find the indicated multiplicative inverse, or explain why it is not possible.

(a) \( (5)^{-1} \mod 24 \)
Solution: 5, since \( 5 \cdot 5 = 25 \equiv 1 \mod 24 \).

(b) \( (8)^{-1} \mod 34 \)
Solution: 8 and 34 are not relatively prime, so \( (8)^{-1} \mod 34 \) does not exist.

(c) \( (-3)^{-1} \mod 26 \)
Solution: Since \( (-9) \cdot (-3) = 27 \equiv 1 \mod 26 \),
\[ -9 = 17 \mod 26 \]
is the indicated multiplicative inverse.

5. Use a mixed alphabet keyword substitution cipher with keyword COCACOLA to decrypt the ciphertext ZGERC.

<table>
<thead>
<tr>
<th>plaintext</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>
<th>N</th>
<th>O</th>
<th>P</th>
</tr>
</thead>
<tbody>
<tr>
<td>ciphertext</td>
<td>C</td>
<td>O</td>
<td>A</td>
<td>L</td>
<td>B</td>
<td>D</td>
<td>E</td>
<td>F</td>
<td>G</td>
<td>H</td>
<td>I</td>
<td>J</td>
<td>K</td>
<td>M</td>
<td>N</td>
<td>P</td>
</tr>
</tbody>
</table>

After P all letters encipher as themselves. So ZGERC is deciphered as ZIGRA.

General note: Very short fragments may not be words. But if you find long plaintexts that do not make sense you are probably doing something
wrong. See 2 above.

This fragment was put here by mistake. But it makes a great question! Can you determine the type of cipher and decrypt it?
YUENO NPTUD LEFTA XOHIR
(Answer at the end...)

6. The following ciphertext was produced using a columnar transposition cipher. Decipher it.

TTOEW HTRSE IAIBM PSEE P NSFLO

Solution: There are 25 characters, so naturally you try 5 rows and 5 cols.

| T | H | I | P | N |
| T | T | A | S | S |
| O | R | I | E | F |
| E | S | B | E | L |
| W | E | M | P | O |

which does not seem to work. If you try 4 columns you will also fail. However, with 6 columns, each of length 4 except for the first which must have 5,

| T | H | E | B | E | S |
| T | T | I | M | E | F |
| O | R | A | P | P | L |
| E | S | I | S | N | O |
| W |

Gives THE BEST TIME FOR APPLES IS NOW.

7. Encipher the plaintext WHERE ARE YOU GOING using a keyword columnar transposition with keyword BLUE.

| B | L | U | E |
| W | H | E | R |
| E | A | R | E |
| Y | O | U | G |
| O | I | N | G |

So the answer is WEYOR EGGHA OIERU N
8. Decipher the ciphertext LOGHNQLW using a Vigenère cipher with key WORD.

Solution: Using the Vigenère table to decrypt

<table>
<thead>
<tr>
<th>Ciphertext</th>
<th>L</th>
<th>O</th>
<th>G</th>
<th>H</th>
<th>N</th>
<th>Q</th>
<th>L</th>
<th>W</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key</td>
<td>W</td>
<td>O</td>
<td>R</td>
<td>D</td>
<td>W</td>
<td>O</td>
<td>R</td>
<td>D</td>
</tr>
</tbody>
</table>

the plaintext is PAPERCUT.

9. Two distinct whole numbers from 1 to 7 (inclusive) are chosen at random. What is the probability that their sum is congruent to 3 modulo 8?

Solution: There are $\binom{7}{2}$ possible pairs of distinct numbers we can choose from 1 to 7. The smallest possible sum is 2 and the largest is 14. The only ones in that range which are congruent to 3 modulo 8 are 3 and 11. The only pair which sums to 3 is \{1, 2\}. The pairs which sum to 11 are \{4, 7\}, \{5, 6\}. So there are three pairs, and the probability is

$$\frac{4}{\binom{7}{2}} = \frac{3}{7} \cdot \frac{2}{6} = \frac{6}{42} = \frac{1}{7}.$$

10. Four friends compare what day of the week, Sunday, Monday, etc., their birthday is in 2011. Assuming that for any individual each of the seven days of the week is equally likely, what is the probability that at least two of them will be celebrating their birthday on the same day of the week? (You need only write down an arithmetic expression for your answer - do not compute it exactly.)

The probability that at least two are the same is $1 - p$, where $p$ is the probability that they are all different. We have seen that

$$p = \frac{7 \cdot 6 \cdot 5 \cdot 4}{7 \cdot 7 \cdot 7 \cdot 7}.$$

So the answer is

$$1 - \frac{6 \cdot 5 \cdot 4}{7^3}.$$

Note: You can definitely leave your answer in this form.

11. The following ciphertext was produced using a Vigenère cipher, with a key of length less than ten. Find the length of the key used. (You do not need to recover the plaintext.)

JGJBT QTIJN KXQEI DFIVF PIETI KCAUZ YVWQE HHSXL MQBDY KXPDJ GJBTQ TIJNK XQEIN RVMGX URKRB JD
There is a VERY long repeated sequence: JGJBTQTIJNKXQEI. The two fragments are separated by 49 characters. The Kasiski test tells us that the key should be a factor of 49 and the problem says less than 10. So there only possibility is 7. Note that a single LONG repeated sequence is extremely unlikely to be an accident.

12. Write down a sentence with at least 10 letters and index of coincidence at most 0.02.
Solution: Any 10 letter or longer sentence with no repeated letters or a sentence with 11 or more with exactly one letter that occurs twice would be ok. For instance OWLS FLY RIGHT.

13. You are given a 200 letter cipher and told it is either a simple substitution, columnar transposition or Vigenère. Give a specific method for determining which type of encryption method was used that does NOT involve decrypting the cipher. Vague descriptions will get a vague amount of credit.
Solution: There are many possibilities. Here is one. First compute the index of coincidence of the ciphertext. If it is close to .0385, which is random, then it is a Vigenère. If it is closer to .065 we assume it is simple substitution or transposition. To distinguish between these two, look at the high frequency letters of the ciphertext. If they are among ETAONIRSH, then we would believe it is a transposition, otherwise it must be a simple substitution.

14. YUENO NPTUD LEFTA XOHIT
The only letters which appear 2 or more times are E, O, T, U, N. Four out of five are from the high frequency letters of English, so we assume it is a transposition. There are 20 characters, so we should try 4 or 5 columns. With five columns we discover

\[
\begin{array}{cccc}
Y & O & U & F \\
U & N & D & T \\
E & P & L & A \\
N & T & E & X \\
\end{array}
\]

So the solution is YOU FOUND THE PLAINTEXT.