1) Given encryption function

\[ y = (26x + 42) \mod 45 \]
\[ y - 42 = 26x \mod 45 \]  \hspace{1cm} (1 pt)

We have to find the modular inverse of 26 \mod 45 using the extended Euclidean algorithm

\[ 45 = 1 \times 26 + 19 \Rightarrow 19 = 45 - 1 \times 26 \]
\[ 26 = 1 \times 19 + 7 \Rightarrow 7 = 26 - 1 \times 19 \]
\[ 19 = 2 \times 7 + 5 \Rightarrow 5 = 19 - 2 \times 7 \]
\[ 7 = 1 \times 5 + 2 \Rightarrow 2 = 7 - 1 \times 5 \]
\[ 5 = 2 \times 2 + 1 \]  \hspace{1cm} (2 pts)

Back substituting for the remainder to get a linear combination

\[ 5 - 2(7 - 1 \times 5) = 1 \]
\[ 3 \times 5 - 2 \times 7 = 1 \]
\[ 3 \times (19 - 2 \times 7) - 2 \times 7 = 1 \]
\[ 3 \times 19 - 6 \times 7 - 2 \times 7 = 1 \]
\[ 3 \times 19 - 8 \times 7 = 1 \]
\[ 3 \times 19 - 8(26 - 19) = 1 \]
\[ 3 \times 19 - 8 \times 26 + 8 \times 19 = 1 \]
\[ 11 \times 19 - 8 \times 26 = 1 \]
\[ 11 \times (45 - 26) - 8 \times 26 = 1 \]
\[ 11 \times 46 - 11 \times 26 - 8 \times 26 = 1 \]
\[ 11 \times 45 - 19 \times 26 = 1 \]  \hspace{1cm} (3 pts)

\(-19 \times 26 \equiv 1 \mod 45\) and the modular inverse of 26 \mod 45 is 26 \mod 45.

Hence

\[ 26 \times (y - 42) = x \mod 45 \]  \hspace{1cm} (1 pt)

so that the final decryption function is

\[ x = 26 \times y - 12 \mod 45 \]
\[ x = 26y + 33 \mod 45 \]  \hspace{1cm} (1 pt)

2)

<table>
<thead>
<tr>
<th>Plain Text</th>
<th>T</th>
<th>H</th>
<th>I</th>
<th>S</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plain text index</td>
<td>19</td>
<td>7</td>
<td>8</td>
<td>18</td>
</tr>
<tr>
<td>(17x + 23) mod 26</td>
<td>8</td>
<td>12</td>
<td>3</td>
<td>17</td>
</tr>
<tr>
<td>Cipher text</td>
<td>I</td>
<td>M</td>
<td>D</td>
<td>R</td>
</tr>
</tbody>
</table>

Repeat the same for all of the plain text to get the cipher text as:

IMDRDRBZAEDARIDKQBCQNWMNBALXRRDVKTNKI  \hspace{1cm} (Grading: 5 pts total)
3) There are 200 possible values of \( b \). We must now count the number of possible values of \( a \), which involves counting the number of values in the list 1, 2, 3, ..., 200 that don’t share a common factor with 200. 200 = \( 2^3 \times 5^2 \). So, we must remove all multiples of 2 and 5 from the list. There are 100 multiples of 2 and 40 multiples of 5. But, in these two lists of multiples, there are repeated values. In particular, each multiple of 10 shows up in both lists. There are 20 multiples of 10 in both lists. Thus, the number of values we should remove is 100 + 40 – 20 = 120. There remain 200 – 120 = 80 values in the list that are relatively prime to 200

Thus, the total number of possible keys for the affine cipher with an alphabet size of 200 is

\[ 80 \times 200 = 16,000. \quad (\text{Grading: 5 pts total - 2 pts for 120, 1 pt for 80, 1 pt for 200, 1 pt for product}) \]

4) Assume the decryption function has a form

\[ f^{-1}(c) = (ac + b) \% 26 \]

where \( c \) is the ciphertext character. Since we know that ciphertext \( W \) maps to plaintext \( E \) and ciphertext \( R \) maps to plaintext \( T \), we get

\[ f^{-1}(22) = (22a + b) \equiv 4 \bmod 26 \]
\[ f^{-1}(17) = (17a + b) \equiv 19 \bmod 26 \quad (2 \text{ pts}) \]

Subtracting the above two equations, we get,

\[ 5a \equiv -15 \equiv 11 \bmod 26 \quad (1 \text{ pt}) \]

From the look up table we find that \( 5^{-1} \bmod 26 \) is 21. Thus, we can determine \( a \):

\[ (21)5a \equiv (21)11 \bmod 26 \]

Solving, we get

\[ a \equiv 231 \equiv 23 \bmod 26 \quad (2 \text{ pts}) \]

Back-substituting, we can solve for \( b \):

Solving for \( b \) yields

\[ (22a + b) \equiv 4 \bmod 26 \]
\[ 22(23) + b \equiv 4 \bmod 26 \]
\[ 506 + b \equiv 4 \bmod 26 \]
\[ b \equiv -502 \bmod 26 \]
\[ b \equiv 18 \bmod 26 \quad (2 \text{ pts}) \]

So the decryption function is

\[ f^{-1}(c) = (23c + 18) \bmod 26 \]
5) Let us assume that the two valid affine ciphers are given by the following equation,

\[
\begin{align*}
    f(p) &= ap + b \mod k \\
    g(p) &= cp + d \mod k
\end{align*}
\]

We now try to compose the two ciphers by doing

\[
g(f(p)) = c(ap + b) + d \mod k
\]

Now for this to be a valid affine cipher following has to be true,

\[
gcd(ca, k) = 1
\]

But since \( f \) and \( g \) are valid ciphers,

\[
\begin{align*}
    \gcd(a, k) &= 1 \\
    \gcd(c, k) &= 1
\end{align*}
\]

This means that there are no common factors between \( a \) and \( k \) and \( c \) and \( k \) other than one. Hence their product \( ca \) too, does not contain any factors that would divide \( k \), since it can only contain prime factors of \( a \) and prime factors of \( c \) and no other prime factors. \( \text{(2 pts)} \)

6) Using brute force, we find the encryption key was 16 \( \text{(1 pt)} \), which reveals the plaintext:

When in Rome do as the Romans do. \( \text{(5 pts)} \)

7) Once again, using brute force, we find the decryption keys to be \( a = 5, b = 24 \). \( \text{(2 pts)} \) Applying these decryption keys we obtain the plaintext:

If you have started your homework early great! I will let you in on a little secret in the answer for question eight. \( \text{(6 pts)} \)

8) Once again, using brute force, we find the decryption keys to be \( a = 19, b = 12 \). \( \text{(2 pts)} \) Applying these decryption keys we find the plaintext to be:

The secret is that I will hide a prize on Friday August twenty-ninth. \( \text{(6 pts)} \)
9) Using the Cryptool for frequency analysis and looking at and the repeated n-grams, we find that WDS could be plain text THE. Trying all the two letter combinations and also looking at the frequency charts, we can assume that the first two letters of the plain text are AS so as to mean AS THE. Looking at the incomplete words and their reputation patterns, we can figure out a few more of the substitutions. Whenever stuck, look at the frequency information of the missing letters and make appropriate substitutions.

As the previous message indicated, I will be hiding a prize. The exact location of that prize can only be determined with the information in this message and the following one. In essence, one has to solve all of the decryption problems first to claim the prize. Best of luck to you all. In order to get this prize you must go to the third floor of the HEC building via the central elevator. The next message will tell you more.

**Grading:** 14 pts total, 10 pts for the plaintext (partial possible) and 4 pts for the explanation of process.

10) Cipher text B has maximum frequency. So it could be E in the plain text. The previous message had a word ELEVATOR. Looking for patterns like E_E and looking at the letter frequencies, substitution of L makes sense. Once letters ELVATOR are known, a lot of the other words are partially known. Using context and frequency knowledge we can make appropriate guesses for remaining substitutions.

As you exit the elevator turn left. Take three paces. Turn right. Take ten paces. There will be a box in front of you roughly at eye level. Open it even if you aren’t hurt. When you do you will see some medical supplies as you swing the cover open. Look at the inside of it. It’s red with several plastic pouches. One of those pouches will have an envelope with two free smoothie cards. Take it, you won!

**Grading:** 14 pts total, 10 pts for the plaintext (partial possible) and 4 pts for the explanation of process.

**Points per question:** Q1 = 8, Q2 = 5, Q3 = 5, Q4 = 7, Q5 = 6, Q6 = 5, Q7 = 8, Q8 = 8, Q9 = 14, Q10 = 14. (80 points for the whole assignment)