Due date: February 2 (in the beginning of the class period)

1. (10 points) Decrypt the following message which was created using the Caesar (shift by 3) cipher:

   \[ \text{LORYHWKHDPHRIKRQRU} \]

2. (10 points) (Taken from Washington-Trappe 2.13.1) Caesar wants to arrange a secret meeting with Marc Antony, either at the Tiber (the river) or at the Coliseum (the arena). He sends the ciphertext:

   \[ \text{EVIRE} \]

   The message was encrypted using a shift cipher; however, Antony does not know the key, so he tries all possibilities. Where will he meet Caesar?

3. (10 points) Compute the following:
   
   (a) \[4321 \mod 26\]
   
   (b) \[-45 \mod 8\]
   
   (c) \[111 \mod 62\]
   
   (d) \[-63 \mod 7\]
   
   (e) \[186 \mod 4\]

4. (20 points) Let \( m \geq 1 \) be an integer and suppose that \( a, b, c, d, k \) are integers such that \( a \equiv b \pmod{m} \), \( c \equiv d \pmod{m} \) and \( k \geq 0 \). Then show that for all integers \( x, y \)

   (a) \[ a + c \equiv b + d \pmod{m} \]
   
   (b) \[ a \times d \equiv b \times c \pmod{m} \]
   
   (c) \[ ax + cy \equiv bx + dy \pmod{m} \]
   
   (d) \[ a^k \equiv b^k \pmod{m} \]

5. (20 points) (Taken from Washington-Trappe 2.13.3) Encrypt \( \text{howareyou} \) using the affine function

   \[ 5x + 7 \pmod{26} \]

   What is the decryption function? Check that it works and describe how you obtained it.
6. (20 points) (Taken from Washington-Trappe 2.13.5)

The following ciphertext was encrypted using an affine cipher mod 26

\[ CRWWZ \]

The plaintext starts \textit{ha}. Decrypt the message and explain your decryption procedure.

7. (20 points) Eve intercepts the following ciphertext created using a substitution cipher:

\[
\text{CBKGS RGKCDMGR TKUSWHUCSRDXN, TGK CXR ZMCTKDFDXG PURGM FUXTKSQFKDX, KJG PUIDG'\text{T TJUK UXG BSCPG CK C KDPG, PUIDXN KJG PURGMT UB KJG FJCSCFKGST TMDNJKMW KU NDIG KJG DPZSGTTDX UB PUIGPXK DX KJG BDXCM BDMP.}
\]

Decrypt this message and say a few words about how you did the decryption.