MATH 406: Homework 8.1 Solutions

1. Encrypt the message LISTENTOITTWICE using a shift cipher with $k = 7$.

   Solution: For each plaintext letter P we do $C \equiv P + 7 \bmod 26$, specifically C is the least nonnegative residue. The result is SPZALUAVPAADPJL.

2. Suppose Eve intercepts the message SLABZMPUKAOLZL sent from Alice to Bob using a shift cipher.

   (a) Use frequency analysis to find the value of k. Explain your steps.

   Solution: We see the most frequent ciphertext letter is L indicating that probably L corresponds to E. Thus when $C = 11$ we have $P = 4$ and so $k \equiv C - P \equiv 7 \bmod 26$.

   (b) Decrypt the message.

   Solution: For each ciphertext letter C we $P \equiv C-7 \bmod 26$ to get the result LETUSFINDTHESE.

3. Encrypt the message LISTENTOITTWICE using an affine cipher with $a = 5$ and $k = 8$.

   Solution: For each plaintext letter P we do $C \equiv 5P+8 \bmod 26$. The result is LWUZCVZAWZZOWSC.

4. Suppose Eve intercepts the message XLULIFIVJQYLL sent from Alice to Bob using an affine cipher.

   (a) Use frequency analysis to find the values of a and k. Explain your steps.

   Solution: The most common letter in the ciphertext is L and the second most common is I. It seems reasonable that L corresponds to E and I correspond to T. That means that we have a and k with

$$\begin{aligned} 11 &\equiv 4a + k \bmod 26 \\ 8 &\equiv 19a + k \bmod 26 \end{aligned}$$

   Taking the second minus the first yields

$$\begin{aligned} 15a &\equiv -3 \bmod 26 \\ (-5)(5)3a &\equiv (-5)(-3) \bmod 26 \\ 3a &\equiv 15 \bmod 26 \\ a &\equiv 5 \bmod 26 \end{aligned}$$

   Then $k \equiv 11 - 4a \equiv 11 - 4(5) \equiv 17 \bmod 26$.

   (b) Find a^{-1}.

   Solution: We need $5a^{-1} \equiv 1 \bmod 26$. We find that $a^{-1} = 21$ does the job.

   (c) Decrypt the message.

   Solution: We solve via $P \equiv a^{-1}(C - 17) \equiv 21(C - 17) \bmod 26$:

C	$21(C-17) \bmod 26$	P
X=23	22	W
L=11	4	E
U=20	11	L
L=11	4	E
I=8	19	T
F=5	8	I
I=8	19	T
V=21	6 G	G
J=9	14 O	O
Q=16	5 F	F
Y=24	R	R
L=11	4	E
L=11	4	E

5. Assume it takes Eve exactly an hour to break an affine cipher. Suppose Alice knows this and so to slow Eve down she figures that she'll encrypt her message with an affine cipher and then re-encrypt the output with different values of a and k and consequently it will take Eve two hours. What's wrong with Alice's reasoning? Use math to make your point rigorously.

   Solution: The problem is that an affine cipher followed by an affine cipher results in just a single affine cipher. In other words if Alice does $C \equiv aP + b \bmod 26$ and then $C' \equiv a'C + b' \bmod 26$ then really $C' \equiv a'(aP + b) + b' \equiv a'aP + (a'b + b') \bmod 26$ and since $\gcd(a, 26) = \gcd(a', 26) = 1$ we know $\gcd(a'a, 26) = 1$ and we have another affine cipher.