Math 373/578 Homework, Week 6, Solutions

**Instruction:** In doing this set of problems, you can use any electronic device to help your computation. But you need to present conclusions based on the analysis of your computation.

1. Convert the base-26 numbers WVU and MATH into base-10 numbers.

**Solution:** First express WVU and MATH as their corresponding base-26 numbers: WVU = (22 21 20)\textsubscript{26} and MATH = (12 0 19 7)\textsubscript{26}. Then convert these into base-10. See below.

\[
\begin{align*}
\text{WVU} &= 22 \times 26^2 + 21 \times 26 + 20 \\
&= 15438 \\
\text{MATH} &= 12 \times 26^3 + 19 \times 26 + 7 \\
&= 211413
\end{align*}
\]

2. Compute WVU + MATH and WVU*MATH as base-26 numbers

**Solution:** We can continue using Matlab to do the computation.

\[
\begin{align*}
\text{WVU} + \text{MATH} &= 12 23 15 1 \\
\text{WVU} \times \text{MATH} &= 12 0 19 7
\end{align*}
\]
3. Julius Caesar, when crossing the River Rubicon, sent to his generals a ciphertext \textit{wkhglhlvfdvw} using Caesar’s cipher (shift cipher) with the mod-26 alphabet. In history, this was considered his declaring war on Rome. However, you happen to know the the first letter is \textit{t}. Can you help to find what the key is and what the plaintext is?

\textbf{Solution:} As this is a Caesar’s cipher, the enciphering function is \( f(x) = x + b \) for some constant \( b \) in \( \mathbb{Z}_{26} \). Since \( t \) is coded as \( w \), \( f(19) = 19 + b = 22 \), and so \( b = 3 \). The encoding function is \( f(x) = x - 3 \), and the decoding function will then be \( g(x) = x - 3 \). We can use matlab to do the computation, considering \( g(x) = E_{1,3}(x) \) as an affine cipher. The plain text is "thedieiscast".

\begin{verbatim}
>> affinecrypt('wkhglhlvfdvw',1,-3)
ans =
    thedieiscast
\end{verbatim}

4. Bob is using an affine cipher to send Alice a ciphertext \textit{TURGIFSFSFERBI} using the usual Mod 26 alphabet. Alice loses the key of this cipher but she figures out that the first two letters are \textit{CR}. Help Alice to find the key and decode the ciphertext.

\textbf{Solution:} Let \( E_{a,b}(x) = ax + b \) be the deciphering function. Then \( 19x + b = E_{a,b}(T) = C = 2 \) and \( 20a + b = E_{a,b}(U) = R = 17 \). It follows that \( a = 15 \) and \( b = 3 \). The cipher text is "cryptananalyst".

\begin{verbatim}
>> affinecrypt('turgifsfsferbi',15,3)
ans =
    cryptananalyst
\end{verbatim}

5. (Exercise 3.16.1) The ciphertext \textit{VHFUHW} has been generated with the Caessar cipher. Determine the key and the plaintext.

\textbf{Solution:} Use matlab.

\begin{verbatim}
>> allshift('vhfuhw')
vhfuhw
wigvix
xjhwjy
ykiikz
zljylz
amkzmb
bmlanc
combody
dpncpe
eqodqf
frperg
gaqfsh
htrgti
iushuj
jvtrivk
kwujwl
lxvkxm
mywlyn
nzxmzo
oaynap
pbzobq
\end{verbatim}
6. Use an affine encrypt function $f(x) = 3x + 7$ to encode the plain text \texttt{theexamisover} using the mod 26 alphabet.

```python
>>> affine_encrypt('theexamisover', 3, 7)
an =
mcttyhrfjxstg
```