Finding the key to an affine cipher

Overview. The frequency histogram in an affine cipher doesn't line up with the standard frequency histogram, but if we know two of the letters in an affine cipher, we can use algebra to determine the key.

Example. Suppose we have an affine cryptogram, and we have determined through frequency analysis that plaintext `e` is represented by ciphertext `M` and plaintext `t` is represented by ciphertext `R`. That is, the alphabet for this affine cipher looks like

```
. . . . M . . . . . . . . . . . . . R . . . . . .
a b c d e f g h i j k l m n o p q r s t u v w x y z
```

where the dots represent unknown cipher letters.

Since this is an affine cipher, the mapping from plaintext to ciphertext is given by

$$x \mapsto ax + b \bmod 26$$

for some numbers a and b. The numerical equivalents of the four letters we know are

$$\texttt{e} = 4 \qquad \texttt{M} = 12 \qquad \texttt{t} = 19 \qquad \texttt{R} = 17$$

so we know that the following equations hold:

$$a \times 4 + b = 12 \tag{1}$$
$$a \times 19 + b = 17 \tag{2}$$

where all numbers are to be reduced modulo 26. If we subtract equation (2) from equation (1), we get

$$a \times (4 - 19) = 12 - 17 \tag{3}$$

We simplify equation (3) by using a calculator (or cipher disk) to find the values of $4 - 19$ and $12 - 17$. We get

$$a \times 11 = 21. \tag{4}$$

We now go to our mod-26 multiplication table. Looking across the 11^{th} row, we find that $11 \times 9 = 21$ (modulo 26), so it must be that $a = 9$. We have found the first half of our key.

To find b, we simply substitute the value for a into either equation (1) or equation (2) and solve. Let's use equation (1). With $a = 9$, equation (1) becomes

$$9 \times 4 + b \quad = \quad 12 \tag{5}$$

From the multiplication table, we find that $9 \times 4 = 10$ (modulo 26), so this equation becomes

$$10 + b \quad = \quad 12. \tag{6}$$

To solve this for b, we simply subtract 10 from both sides of the equation; we get $b = 12 - 10$, so $b = 2$. The key for this affine cipher is $a = 9$, $b = 2$.

We use this information to complete the alphabet above. We get

```
C L U D M V E N W F O X G P Y H Q Z I R A J S B K T
a b c d e f g h i j k l m n o p q r s t u v w x y z
```

Things to do.

1. Using the technique in the example above, complete the following affine-cipher alphabets:

```
. . . . S . . . . . . . . . . . . . V . . . . . .
a b c d e f g h i j k l m n o p q r s t u v w x y z

. . . . X . . L . . . . . . . . . . . . . . . . .
a b c d e f g h i j k l m n o p q r s t u v w x y z
```

2. What happens when you apply the same technique to these two?

```
. . . . . . . C . . . . . . . . . . . I . . . . . .
a b c d e f g h i j k l m n o p q r s t u v w x y z

. . . . . . . U . . . . . . . . . . . B . . . . . .
a b c d e f g h i j k l m n o p q r s t u v w x y z
```