Affine Ciphers

An affine cipher, (like a shift cipher), is an example of a *substitution cipher*: In encryption using a substitution cipher, each time a given letter occurs in the plaintext, it always is replaced by the same ciphertext letter. For example, the plaintext letter 'e' might be replaced by the ciphertext letter 'K' each time it occurs. The method used for this replacement in affine encryption can be viewed as a generalization of the method used for encryption using a shift cipher. Shift ciphers are a particular type of affine cipher.

The encryption key for an affine cipher is an ordered pair of integers, both of which come from the set $\{0, \ldots, n-1\}$, where n is the size of the character set being used (for us, the character set is the English alphabet, so we have $n = 26$). It is important to note that some of the possible pairs of integers from the set $\{0, \ldots, n-1\}$ are not valid as affine encryption keys. We'll discuss the exact nature of the valid keys a bit later. To describe the encryption, we again consider the following conversion table for the English alphabet:

0	1	2	3	4	5	6	7	8	9	10	11	12
A	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*

13	14	15	16	17	18	19	20	21	22	23	24	25
N	*O*	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*

Suppose we want to encrypt the message "beach" using an affine cipher with encryption key (3, 1).

i. Using the table, we can represent the letters in our message "beach" with their corresponding numbers: 1 4 0 2 7.

ii. Now we multiply each of the numbers from step *i* by the first number in the encryption key, (3 in this case), to get: 3 12 0 6 21.

iii. Next, add the second number in the encryption key, (1 in this case), to each of the numbers from step *ii* to get: 4 13 1 7 22.

iv. Now use the table to replace the numbers from step *iii* with their corresponding letters to obtain the ciphertext: ENBHW.

As with shift ciphers, there is a small complication when the arithmetic we do in steps *ii* and *iii* above produces a number that is larger than 25. For example, if we consider the new plaintext "surf," and use the encryption key (3,1) again, then the resulting ciphertext is "NRLN." The encryption looks this way:

$$\text{surf} \xrightarrow{i} 18, 20, 17, 5 \xrightarrow{ii} 54, 60, 51, 15 \xrightarrow{iii} 55, 61, 52, 16 \xrightarrow{\star} 3, 9, 0, 16 \xrightarrow{iv} \text{DJAQ}$$

What have we done mathematically in the step labelled $\star$? Each number was replaced by the number from the set $\{0, \ldots, 25\}$ that is congruent to it modulo 26. (This idea was introduced in the discussion on shift ciphers.) In summary, affine encryption on the English alphabet using encryption key (α, β) is accomplished via the formula $y \equiv \alpha x + \beta \pmod{26}$.

(Now we can see why a shift cipher is just a special case of an affine cipher: A shift cipher with encryption key ℓ is the same as an affine cipher with encryption key $(1, \ell)$.)

For another example, encryption of the plaintext "sail" using an affine cipher with encryption key (3,7) produces ciphertext "JHFO" this way:

$$\begin{array}{lcllcl}
\text{s} & \longrightarrow & 18 & \longrightarrow & 3 \cdot 18 + 7 \equiv 9 \pmod{26} & \longrightarrow \text{J} \\
\text{a} & \longrightarrow & 0 & \longrightarrow & 3 \cdot 0 + 7 \equiv 7 \pmod{26} & \longrightarrow \text{H} \\
\text{i} & \longrightarrow & 8 & \longrightarrow & 3 \cdot 8 + 7 \equiv 5 \pmod{26} & \longrightarrow \text{F} \\
\text{l} & \longrightarrow & 11 & \longrightarrow & 3 \cdot 11 + 7 \equiv 14 \pmod{26} & \longrightarrow \text{O}
\end{array}$$

How is the original (*plaintext*) message recovered from the ciphertext if the encryption key is known? The following ciphertext was produced using an affine cipher with encryption key (3,7): QTORHG. To decrypt it (i.e., to recover the plaintext message), we can reverse the steps in the encryption: first add 19 (... or subtract 7 ... why is that the same?) to each of the numbers representing the ciphertext letters, then multiply the result by 9 (can you explain why 9? — see below if you're stumped). What we have done can be summarized by the formula $x \equiv 9(y + 19) \pmod{26}$, or, more simply, by $x \equiv 9y + 15 \pmod{26}$, (note $9 \cdot 19 \equiv 15 \pmod{26}$). Here (9,15) is the *decryption key* for the affine cipher with encryption key (3,7).

$$
\begin{array}{lllll}
\text{Q} & \longrightarrow & 16 & \longrightarrow & 9 \cdot 16 + 15 \equiv 3 \pmod{26} \longrightarrow \text{d} \\
\text{T} & \longrightarrow & 19 & \longrightarrow & 9 \cdot 19 + 15 \equiv 4 \pmod{26} \longrightarrow \text{e} \\
\text{O} & \longrightarrow & 14 & \longrightarrow & 9 \cdot 14 + 15 \equiv 11 \pmod{26} \longrightarrow \text{l} \\
\text{R} & \longrightarrow & 17 & \longrightarrow & 9 \cdot 17 + 15 \equiv 12 \pmod{26} \longrightarrow \text{m} \\
\text{H} & \longrightarrow & 7 & \longrightarrow & 9 \cdot 7 + 15 \equiv 0 \pmod{26} \longrightarrow \text{a} \\
\text{G} & \longrightarrow & 6 & \longrightarrow & 9 \cdot 6 + 15 \equiv 17 \pmod{26} \longrightarrow \text{r}
\end{array}
$$

Now let's explain why we multiplied by 9 in the above decryption. We were trying to solve the encryption congruence

$$y \equiv 3x + 7 \pmod{26}$$

for the variable x in terms of y. First, we added 19 to both sides to get

$$y + 19 \equiv 3x + 26 \pmod{26},$$

(it is always valid to add an integer to both sides of a congruence; to understand why, note that the difference of the two sides is still divisible by the modulus). Since we are working modulo 26, this is equivalent to

$$y + 19 \equiv 3x \pmod{26}.$$

At this point, we want to isolate x. If this were an equation instead of a congruence, we could do this by multiplying both sides by $\frac{1}{3}$. However, it is *never* a good idea to introduce fractions into a congruence. But we can multiply both sides by an integer. The integer we need should have the effect of replacing the 3 by a 1. So, we want to multiply by some integer a such that $3a \equiv 1 \pmod{26}$. By inspection, one finds that $3 \cdot 9 = 27 \equiv 1 \pmod{26}$, so 9 is our desired multiplier. Using it, we arrive at

$$9(y + 19) \equiv 9 \cdot 3x \equiv x \pmod{26}.$$

If you want to learn an efficient systematic way to find the 9 (instead of just searching for it), check out the topic of modular inverses and the extended Euclidean algorithm in any introductory number theory text. Because the modulus (26) is small, we can accomplish this with a relatively short search, so we don't discuss the Euclidean algorithm here.

At this point, we can explain fully what comprises a valid encryption key (α, β). In order for the cipher to be useful, the encryption process must be reversible, i.e., (α, β) must have an associated decryption key, say (γ, δ). In order for γ and δ to exist, what must be true of α and β? Looking back at the above example, notice that we needed to subtract β from both sides of the encryption congruence. This is possible for any value of β. But later on, we needed to multiply both sides of a congruence by an integer a ($a = 9$ in the example) such that $\alpha a \equiv 1 \pmod{26}$. This is not possible for every integer α in the set $\{0, 1, \ldots, 25\}$: clearly $\alpha = 0$ doesn't work, but there are non-zero elements of the set that also don't work. For example, if we had chosen $\alpha = 2$, then we would have been trying to find an integer a such that $2a \equiv 1 \pmod{26}$, which is equivalent to $2a - 1$ being divisible by 26. Since $2a - 1$ is always odd, it can never be divisible by the even integer 26. So, we cannot use $\alpha = 2$ in an affine encryption key where the character set has 26 letters.

What other values of α cannot be used? It turns out that if α has a factor other than ± 1 in common with 26, then it is not a valid choice for an encryption key. The valid encryption keys (for a 26-letter character set) are of the form (α, β), where α, $\beta \in \{0, 1, \ldots, 25\}$ and $\gcd(\alpha, 26) = 1$.

A value of α that does work is $\alpha = 11$. What is the integer a such that $\alpha \cdot a \equiv 1 \pmod{26}$? Testing the possibilities between 0 and 25, we see that $19 \cdot 11 = 209 \equiv 1 \pmod{26}$, so $a = 19$ is the desired integer. Thus, for example, if $(11, 14)$ is our encryption key, then the decryption key is $(19, 20)$.

In general, suppose we have a valid encryption key (α, β), with associated decryption key (γ, δ). Then γ is just the integer a discussed above that solves $\alpha a \equiv 1 \pmod{26}$. See if you can write down a formula for δ in terms of α, β, and/or γ.

Here is ciphertext that was produced using an affine cipher on the English alphabet with encryption key $(5, 4)$. Find the decryption key and then decrypt the message.

OYHYJLEVYQBLSRIJLYEC

What about security? We saw last time that shift ciphers are not very secure — they are easily attacked by exhaustive search or frequency analysis. Are affine ciphers better? And if so, is the improvement great enough to make them secure?

Suppose you intercept a ciphertext message that you know was encrypted using an affine cipher on the English alphabet. How many distinct encryption keys (α, β) might have been used? From the above discussion, we know that α must have a gcd of 1 with 26, so must be one of the following numbers: 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25. As β can be any of the numbers 0, 1, ... , 25, we see that there are $12 \cdot 26 = 312$ possible encryption keys, (or 311, if we exclude (1, 0), which would not have changed the plaintext at all). It wouldn't take very long (especially with computer help) to test each of these keys in an exhaustive search. While this is a longer search than one would need in order to break a shift cipher, it is still trivial to accomplish it quickly with computer help. Even worse, as with any substitution cipher, frequency analysis can be used with a high likelihood of quick success on ciphertext messages that are sufficiently long.

Below is ciphertext produced by an affine cipher with undisclosed encryption key. See if you can decrypt it using frequency analysis or exhaustive search. (Note that the line breaks do not necessarily occur between words!)

LREKMEPQOCPCBOYGYWPPEHFIWPFZYQGDZERGYPWFYWECYOJEQCMYEGFGYPWFCYMJ
YFGFMFGWPQGDZERGPGFFZEYCIEDBCGPFEHFBEFFERQCPJEEPQRODFEXFWCPOWPEWLY
ETERCBXGLLEREPFQGDZERFEHFBEFFERYXEDEPXGPSWPGFYDWYGFGWPGPFZEIEYYCSE