Algebra in ciphers

ENCIPHERING

Example: $c = 3p + 1$

c = the number of the ciphertext letter's position in the alphabet

p = the number of the plaintext letter's position in the alphabet

For example, say you want to send the letter "e" - since "e" is the fifth letter, $p = 5$.

$c = 3p + 1$

$c = 3(5) + 1$

$c = 15 + 1$

$c = 16$

You will send the 16th letter, or "p."

If you want to send the letter "t," which is the 20th letter, then:

$c = 3p + 1$

$c = 3(20) + 1$

$c = 60 + 1$

$c = 61$

Since there aren't 61 letters in our alphabet, you have to subtract multiples of 26 until you get to a number between 1 and 26, inclusive. In this case, we'll need to subtract 26 and then subtract 26 again (in other words, subtract 52), and then go to the ninth letter (since $61 = 2 * 26 + 9$), so you will send the ninth letter, or "i."

Note to teachers: This will also introduce (or reinforce) the notion of modular arithmetic, since $61 \equiv 9 \mod 26$, which will come in handy later in the student's study of cryptography.

DECIPHERING

When deciphering in this manner, it's a matter of solving the equation for "p." For example, say we know the equation we're working with is the same as above - that is:

$c = 3p + 1$

If you're sent the cipher letter "v," which is the 22nd letter, then to decipher, just plug "22" in for "c," and solve for "p."

$c = 3p + 1$

$22 = 3p + 1$

$21 = 3p$

$7 = p$

Since the seventh letter is "g," you know that this is the plaintext letter corresponding to the ciphertext "v."

On a similar note, say you're sent the cipher letter "r," the 18th letter, and have to decipher using the same equation. Then:

$c = 3p + 1$

$18 = 3p + 1$

$17 = 3p$, so $p = 17/3$.

Obviously, there is no such letter in plaintext. However, in a fashion similar to that used above, we have to add multiples of 26 until we get a whole number when dividing. So, using modular arithmetic, if $17 \equiv 3p \bmod 26$, then $(17 + 26)$ must also $\equiv 3p \bmod 26$, so $43 = 3p$. This, though, gives us $p = 43/3$. We have to do this once more, and add 26 to 43, giving 69. So, $69 \equiv 3p \bmod 26$, so $p = 23$, giving the plaintext "w."