Hill Cipher

The Hill cipher uses matrix multiplication, mod 26. The encryption key is a n x n matrix with an inverse mod 26, where n is the block size. (We will discuss later how to test if a matrix has an inverse mod 26 or not.) For our purposes, we will illustrate the cipher with n = 2. Consider the following key:

$$\begin{pmatrix} 3 & 1 \\ 6 & 5 \end{pmatrix}$$

To encrypt a plaintext, group the plaintext in pairs: "MA" and "TH", for example. Convert each letter to its numerical equivalent, mod 26, and write it in a nx1 matrix as follows:

$\begin{pmatrix} 12 \\ 0 \end{pmatrix}$ stands for "MA"

Now, multiply the encryption key by the plaintext and reduce mod 26 to get the ciphertext:

$\begin{pmatrix} 3 & 1 \\ 6 & 5 \end{pmatrix}\begin{pmatrix} 12 \\ 0 \end{pmatrix} = \begin{pmatrix} 36 \\ 72 \end{pmatrix} = \begin{pmatrix} 10 \\ 20 \end{pmatrix} \mod 26$, which corresponds to the ciphertext KU.

Here is the encryption of "TH":

$\begin{pmatrix} 3 & 1 \\ 6 & 5 \end{pmatrix}\begin{pmatrix} 19 \\ 7 \end{pmatrix} = \begin{pmatrix} 64 \\ 149 \end{pmatrix} \equiv \begin{pmatrix} 12 \\ 19 \end{pmatrix} \mod 26$, which corresponds to the ciphertext MT.

To decrypt, you need the inverse matrix.

Here's the derivation of the inverse matrix for this particular matrix. Just like modular inverses, an matrix's inverse is the matrix you multiply it by to obtain the matrix identity element, which is 1's down the main diagonal and 0's everywhere else.

Thus, we want integers a, b, c and d, in between 0 and 25, inclusive, that satisfy the following equation:

$$\begin{pmatrix} 3 & 1 \\ 6 & 5 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod 26$$

This yields the equations

$3a + c \equiv 1 \bmod 26$	$3b + d \equiv 0 \bmod 26$
$6a + 5c \equiv 0 \bmod 26$	$6b + 5d \equiv 1 \bmod 26$
$-(6a + 2c \equiv 2 \bmod 26)$	$-(6b + 2d) \equiv 0 \bmod 26$
---	---
$3c \equiv 24 \bmod 26$	$3d \equiv 1 \bmod 26$
$c \equiv 8 \bmod 26$	$9(3d) \equiv 9 \bmod 26$
	$d \equiv 9 \bmod 26$
$3a + c \equiv 1 \bmod 26$	$3b + d \equiv 0 \bmod 26$
$3a + 8 \equiv 1 \bmod 26$	$3b + 9 \equiv 0 \bmod 26$
$3a \equiv 19 \bmod 26$	$3b \equiv 17 \bmod 26$
$9(3a) \equiv 9(19) \bmod 26$	$9(3b) \equiv 9(17) \bmod 26$
$a \equiv 171 \bmod 26$	$b \equiv 153 \bmod 26$
$\equiv 15 \bmod 26$	$\equiv 23 \bmod 26$

Thus, the desired inverse matrix is $\begin{pmatrix} 15 & 23 \\ 8 & 9 \end{pmatrix}$.

Now, we can corroborate that this is the case by decrypting the example above.

$$\begin{pmatrix} 15 & 23 \\ 8 & 9 \end{pmatrix}\begin{pmatrix} 10 \\ 20 \end{pmatrix} \equiv \begin{pmatrix} 610 \\ 260 \end{pmatrix} \equiv \begin{pmatrix} 12 \\ 0 \end{pmatrix} \bmod 26$$

$$\begin{pmatrix} 15 & 23 \\ 8 & 9 \end{pmatrix}\begin{pmatrix} 12 \\ 19 \end{pmatrix} \equiv \begin{pmatrix} 617 \\ 267 \end{pmatrix} \equiv \begin{pmatrix} 19 \\ 7 \end{pmatrix} \bmod 26$$

We can also verify this by multiplying both matrices in question together:

$$\begin{pmatrix} 3 & 1 \\ 6 & 5 \end{pmatrix}\begin{pmatrix} 15 & 23 \\ 8 & 9 \end{pmatrix} \equiv \begin{pmatrix} 53 & 78 \\ 130 & 183 \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod 26$$, as desired.

More generally, if we do this process with variables instead of a specific matrix, we find that the inverse of the matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is $((ad - bc)^{-1}(mod\ 26))\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$.

Thus, the condition under which a 2 x 2 matrix has an inverse is if and only if its determinant, ad-bc, is relatively prime with 26. (More generally, the determinant of an n by n matrix for a Hill cipher has an inverse if and only if its determinant is relatively prime with the alphabet size.)

Using a known plaintext attack, we can break the Hill cipher with n blocks (of n letters) of matching plain-ciphertext pairs.

Consider the following:

Let's say we know that "MA" encrypts to "KU" and that "TH" encrypts to "MT".
Let the unknown key be $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Then we can set up the following equations:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 12 \\ 0 \end{pmatrix} \equiv \begin{pmatrix} 10 \\ 20 \end{pmatrix} \bmod 26 \qquad \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 19 \\ 7 \end{pmatrix} \equiv \begin{pmatrix} 12 \\ 19 \end{pmatrix} \bmod 26$$

$12a \equiv 10 \pmod{26}$ $\qquad$ $19a + 7b \equiv 12 \pmod{26}$
$12c \equiv 20 \pmod{26}$ $\qquad$ $19c + 7d \equiv 19 \pmod{26}$

$6a \equiv 5 \pmod{13}$, based on a derivation shown in the mod notes.
$6c \equiv 10 \pmod{13}$

$11(6a) \equiv 11(5) \pmod{13}$, 11 is the desired inverse
$11(6c) \equiv 11(10) \pmod{13}$

$a \equiv 55 \pmod{13}$
$\equiv 3 \pmod{13}$
$c \equiv 110 \pmod{13}$
$\equiv 6 \pmod{13}$

So, a could be either 3 or 16 (mod 26).
and c could be either 6 or 19 (mod 26).

$19a + 7b \equiv 12 \pmod{26}$
$19(3) + 7b \equiv 12 \pmod{26}$
$7b \equiv -45 \pmod{26}$
$7b \equiv 7 \pmod{26}$, so $b = 1 \pmod{26}$

$19c + 7d = 19 \pmod{26}$
$19(6) + 7d = 19 \pmod{26}$
$7d = -95 \pmod{26}$
$7d = 9 \pmod{26}$
$15(7d) = 15(9) \pmod{26}$
$d = 135 \pmod{26}$
$d = 5 \pmod{26}$

Plugging in $a = 16 \pmod{26}$ yields the solution $b = 14 \pmod{26}$.
Similarly, plugging in $c = 19 \pmod{26}$ yields the solution $d = 18 \pmod{26}$.

Thus, using the given information, we've narrowed down the possible keys to these four:
$\begin{pmatrix} 3 & 1 \\ 6 & 5 \end{pmatrix}, \begin{pmatrix} 3 & 1 \\ 19 & 18 \end{pmatrix}, \begin{pmatrix} 16 & 14 \\ 6 & 5 \end{pmatrix}, \begin{pmatrix} 16 & 14 \\ 19 & 18 \end{pmatrix}$

Trying each one out on the rest of the ciphertext will lead to the correct one. (Technically, you'd have to first invert it, and then apply that inverted matrix to the rest of the ciphertext.)