HILL CIPHER

REFERENCE: https://facultyfp.salisbury.edu/despickler/personal/Resources/LinearAlgebra/HillCipherHandoutLA.pdf

Here's an example.
The key for a hill cipher is a matrix e.g.

$$\begin{bmatrix} 2 & 4 & 5 \\ 9 & 2 & 1 \\ 3 & 17 & 7 \end{bmatrix}$$

In the above case, we have taken the size to be 3×3, however it can be any size (as long as it is square). Assume we want to encipher the message ATTACK AT DAWN. To encipher this, we need to break the message into chunks of 3. We now take the first 3 characters from our plaintext, ATT and create a vector that corresponds to the letters (replace A with 0, B with 1 ... Z with 25 etc.) to get: [0 19 19] (this is ['A' 'T' 'T']).
To get our ciphertext we perform a matrix multiplication (you may need to revise matrix multiplication if this doesn't make sense):

$$\begin{bmatrix} 2 & 4 & 5 \\ 9 & 2 & 1 \\ 3 & 17 & 7 \end{bmatrix} \begin{bmatrix} 0 \\ 19 \\ 19 \end{bmatrix} = \begin{bmatrix} 171 \\ 57 \\ 456 \end{bmatrix} \pmod{26} = \begin{bmatrix} 15 \\ 5 \\ 14 \end{bmatrix} = \text{'PFO'}$$

This process is performed for all 3 letter blocks in the plaintext. The plaintext may have to be padded with some extra letters to make sure that there is a whole number of blocks.
Now for the tricky part, the decryption. We need to find an inverse matrix modulo 26 to use as our 'decryption key'. i.e. we want something that will take 'PFO' back to 'ATT'. If our 3 by 3 key matrix is called K, our decryption key will be the 3 by 3 matrix K^{-1}, which is the inverse of K.

$$K^{-1} \begin{bmatrix} 15 \\ 5 \\ 14 \end{bmatrix} \pmod{26} = \begin{bmatrix} 0 \\ 19 \\ 19 \end{bmatrix} = \text{'ATT'}$$

To find K^{-1} we have to use a bit of maths. It turns out that K^{-1} above can be calculated from our key. A lengthy discussion will not be included here, but we will give a short example. The important things to know are inverses (mod m), determinants of matrices, and matrix adjugates.
Let K be the key matrix. Let d be the determinant of K. We wish to find K^{-1} (the

inverse of K), such that K × K^{-1} = I (mod 26), where I is the identity matrix. The following formula tells us how to find K^{-1} given K:

$$K^{-1} = d^{-1} \times adj(K)$$

where d × d^{-1} = 1(mod 26), and adj(K) is the adjugate matrix of K.
d (the determinant) is calculated normally for K (for the example above, it is 489 = 21 (mod 26)). The inverse, d^{-1}, is found by finding a number such that d × d^{-1} = 1 (mod 26) (this is 5 for the example above since 5*21 = 105 = 1 (mod 26)). The simplest way of doing this is to loop through the numbers 1..25 and find the one such that the equation is satisfied. There is no solution (i.e. choose a different key) if gcd(d,26) ≠ 1 (this means d and 26 share factors, if this is the case K can not be inverted, this means the key you have chosen will not work, so choose another one).
That is it. Once K^{-1} is found, decryption can be performed.