Cryptography is the practice and study of techniques for secure communication in the presence of third parties called adversaries. More generally, cryptography is about constructing and analysing protocols that prevent third parties or the public from reading private messages; various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation are central to modern cryptography.

In cryptography, a cipher (or cypher) is an algorithm for performing encryption or decryption a series of well-defined steps that can be followed as a procedure. An alternative, less common term is encipherment. To encipher or encode is to convert information into cipher or code.

There are different kinds of Cipher they are:

1. Caesar Shift Cipher
2. Transposition Cipher
3. Book Cipher
4. Pigpen Cipher
5. Play fair Cipher
6. Hill Cipher

You can find the various details of these different kinds of Ciphers on web.

# Mathematical Formulation

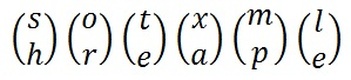
**Hill Cipher (2 x 2):**

**Encryption:**

We shall encrypt the plaintext message "short example" using the keyword hill and a 2 x 2 matrix. The first step is to turn the keyword into a matrix. If the keyword was longer than the 4 letters needed, we would only take the first 4 letters, and if it was shorter, we would fill it up with the alphabet in order (much like a Mixed Alphabet).

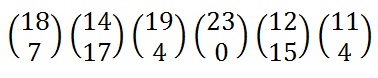
With the keyword in a matrix, we need to convert this into a key matrix. We do this by converting each letter into a number by its position in the alphabet (starting at 0). So, A = 0, B = 1, C= 2, D = 3, etc.

* We now split the plaintext into digraphs, and write these as column vectors. That is, in the first column vector we write the first plaintext letter at the top, and the second letter at the bottom. Then we move to the next column vector, where the third plaintext letter goes at the top, and the fourth at the bottom. This continues for the whole plaintext.

[](http://crypto.interactive-maths.com/uploads/1/1/3/4/11345755/3874131_orig.jpg)

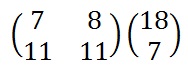
The plaintext "short example" split into column vectors.

Now we must convert the plaintext column vectors in the same way that we converted the keyword into the key matrix. Each letter is replaced by its appropriate number.

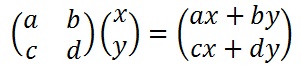
[](http://crypto.interactive-maths.com/uploads/1/1/3/4/11345755/9504506_orig.jpg)

The plaintext converted into numeric column vectors.

Now we must perform some matrix multiplication. We multiply the key matrix by each column vector in turn. We shall go through the first of these in detail, then the rest shall be presented in less detail. We write the key matrix first, followed by the column vector.

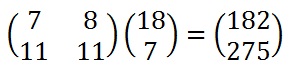


To perform matrix multiplication we "combine" the top row of the key matrix with the column vector to get the top element of the resulting column vector. We then "combine" the bottom row of the key matrix with the column vector to get the bottom element of the resulting column vector. The way we "combine" the four numbers to get a single number is that we multiply the first element of the key matrix row by the top element of the column vector, and multiply the second element of the key matrix row by the bottom element of the column vector. We then add together these two answers.

[](http://crypto.interactive-maths.com/uploads/1/1/3/4/11345755/4654040_orig.jpg)

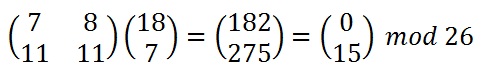
The algebraic rules of matrix multiplication.

In our case we perform the two calculations on the right. We then right these two answers out in a column vector as shown below.

[](http://crypto.interactive-maths.com/uploads/1/1/3/4/11345755/9802105_orig.jpg)

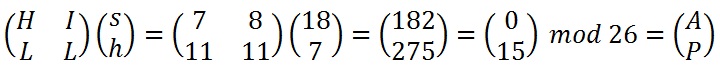
The shorthand for the matrix multiplication.

Next, we must take each of these numbers, in our resultant column vector, modulo 26 (remember that means divide by 26 and take the remainder).

[](http://crypto.interactive-maths.com/uploads/1/1/3/4/11345755/4006075_orig.jpg)

Reducing the resultant column vector modulo 26.

Finally, we must convert these numbers back to letters, so 0 becomes "A" and 15 becomes "P", and our first two letters of the ciphertext are "AP".

[](http://crypto.interactive-maths.com/uploads/1/1/3/4/11345755/9900824_orig.jpg)

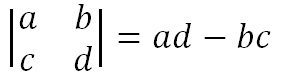
The whole calculation: converting to numbers; the matrix multiplication; reducing modulo 26; converting back to letters.

**Decryption:**

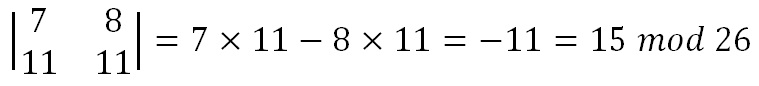
We shall decrypt the example above, so we are using the keyword hill and our ciphertext is "APADJ TFTWLFJ". We start by writing out the keyword as a matrix and converting this into a key matrix as for encryption. Now we must convert this to the inverse key matrix, for which there are several steps.

* Find the Multiplicative Inverse of the Determinant

The determinant is a number that relates directly to the entries of the matrix. It is found by multiplying the top left number by the bottom right number and subtracting from this the product of the top right number and the bottom left number. This is shown algebraically below. Note that the notation for determinant has straight lines instead of brackets around our matrix

[](http://crypto.interactive-maths.com/uploads/1/1/3/4/11345755/4533438_orig.jpg)

Algebraic method to calculate the determinant of a 2 x 2 matrix. Once we have found this value, we need to take the number modulo 26. Below is the way to calculate the determinant for our example.

[](http://crypto.interactive-maths.com/uploads/1/1/3/4/11345755/6449828_orig.jpg)

Calculating the determinant of our 2 x 2 key matrix.

We now must find the multiplicative inverse of the determinant working modulo 26. That is, the number between 1 and 25 that gives an answer of 1 when we multiply it by the determinant. So, in this case, we are looking for the number that we need to multiply 15 by to get an answer of 1 modulo 26. There are algorithms to calculate this, but it is often easiest to use trial and error to find the inverse.

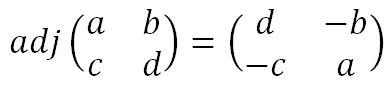
[Picture](http://crypto.interactive-maths.com/uploads/1/1/3/4/11345755/2704112_orig.jpg)

This calculation gives us an answer of 1 modulo 26.

So, the multiplicative inverse of the determinant modulo 26 is 7. We shall need this number later.

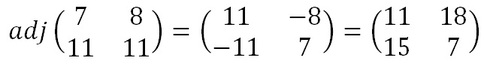
* Find the Adjoint Matrix

The adjoint matrix is a matrix of the same size as the original. For a 2 x 2 matrix, this is straightforward as it is just moving the elements to various positions and changing a couple of signs. That is, we swap the top left and bottom right numbers in the key matrix, and change the sign of the top right and bottom left numbers. Algebraically this is given below.

[](http://crypto.interactive-maths.com/uploads/1/1/3/4/11345755/2475976_orig.jpg)

The adjoint matrix of a 2 x 2 matrix.

Again, once we have these values we will need to take each of them modulo 26 (we need to add 26 to the negative values to get a number between 0 and 25. For our example we get the matrix below.

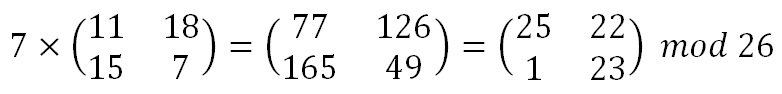
[](http://crypto.interactive-maths.com/uploads/1/1/3/4/11345755/8133953_orig.jpg)

The adjugated matrix of the key matrix.

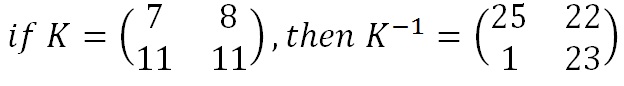
* Multiply the Multiplicative Inverse of the Determinant

by the adjoint Matrix.

To get the inverse key matrix, we now multiply the inverse determinant (that was 7 in our case) from step 1 by each of the elements of the adjoint matrix from step 2. Then we take each of these answers modulo 26.

[](http://crypto.interactive-maths.com/uploads/1/1/3/4/11345755/3227655_orig.jpg)

Multiplying the multiplicative inverse of the determinant by the adjoint to get the inverse key matrix.



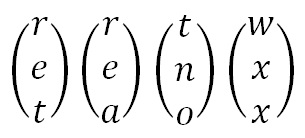
Now we have the inverse key matrix, we must convert the ciphertext into column vectors and multiply the inverse matrix by each column vector in turn, take the results modulo 26 and convert these back into letters to get the plaintext.

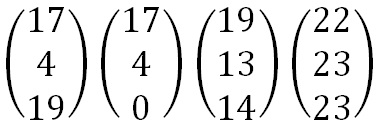
**Hill Cipher (3 x 3):**

**Encryption:**

We shall encrypt the plaintext message "retreat now" using the key phrase back up and a 3 x 3 matrix. The first step is to turn the key phrase into a matrix. Notice that the key phrase is a few letters short, so we fill in the final elements with the start of the alphabet. Now we turn the keyword matrix into the key matrix by replacing letters with their numeric values.

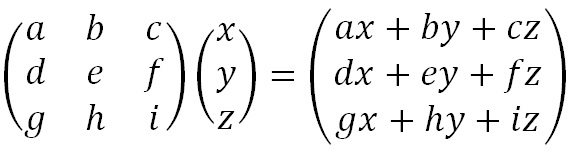
Now we split the plaintext into trigraphs (we are using a 3 x 3 matrix so we need groups of 3 letters), and convert these into column vectors. However, since the plaintext does not go perfectly into the column vectors, we need to use some nulls to make the plaintext the right length. We then convert these into numeric column vectors.

[](http://crypto.interactive-maths.com/uploads/1/1/3/4/11345755/7852819_orig.jpg)

[](http://crypto.interactive-maths.com/uploads/1/1/3/4/11345755/816249_orig.jpg)

The plaintext split into trigraphs and written in column vectors. Note the nulls added to make it the right length

Now we perform matrix multiplication, multiplying the key matrix by each column vector in turn. To perform matrix multiplication, we "combine" the top row of the key matrix with the column vector to get the top element of the resulting column vector. We then "combine" the middle row of the key matrix with the column vector to get the middle element of the resulting column vector. and similarly, for the bottom row. The way we "combine" the six numbers to get a single number is that we multiply the first element of the key matrix row by the top element of the column vector, multiply the second element of the key matrix row by the middle element of the column vector, and multiply the third element of the key matrix row by the bottom element of the column vector. We then add together these three answers.

[](http://crypto.interactive-maths.com/uploads/1/1/3/4/11345755/9506348_orig.jpg)

Algebraic representation of matrix multiplication for a 3 x 3 matrix.

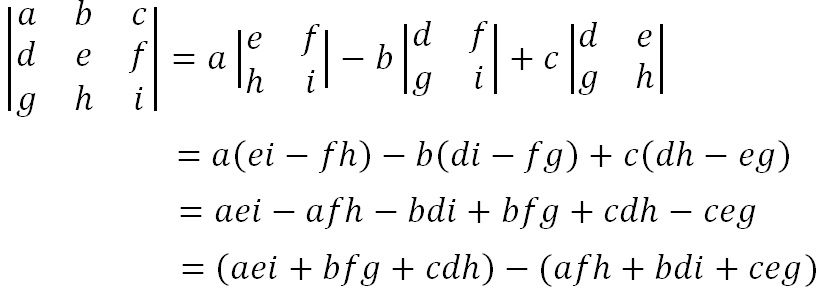
We then follow the same process as for the 2 x 2 Matrix Example. We perform all the matrix multiplications, and take the column vectors modulo 26. Then we convert them back into letters to produce the ciphertext.

**Decryption:**

We shall decrypt the ciphertext message "SYICHOLER" using the keyword alphabet. The first step is to turn the key phrase into a matrix. Notice that the keyword is a letter short, so we fill in the final element with the start of the alphabet. Now we need to convert this into the inverse key matrix, following the same step as for a 2 x 2 matrix. However, the way we calculate each step is slightly different.

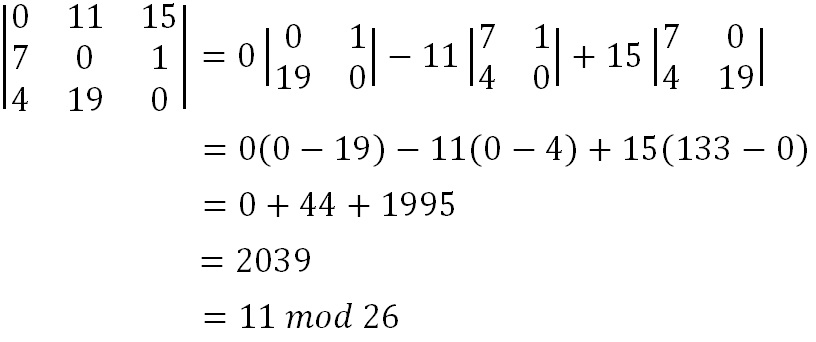
* Find the Multiplicative Inverse of the Determinant

The determinant is a number that relates directly to the entries of the matrix. For a 3 x 3 matrix, it is found by multiplying the top left entry by the determinant of the 2 x 2 matrix formed by the entries that are not in the same row or column as that entry (that is the 2 x 2 matrix not including the top row or left column). Similar steps are done with the other two elements in the top row, and the middle value is subtracted from the sum of the other two. This is shown more clearly in the algebraic version below.

[](http://crypto.interactive-maths.com/uploads/1/1/3/4/11345755/4458084_orig.jpg)

The algebraic representation of finding the determinant of a 3 x 3 matrix.

Once we have calculated this value, we take it modulo 26.

[](http://crypto.interactive-maths.com/uploads/1/1/3/4/11345755/8073467_orig.jpg)

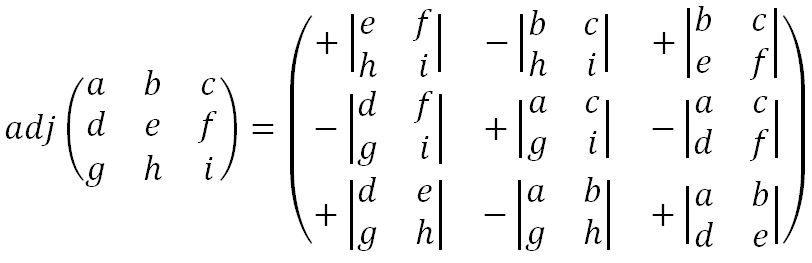
We now must find the multiplicative inverse of the determinant working modulo 26. That is, the number between 1 and 25 that gives an answer of 1 when we multiply it by the determinant. So, in this case, we are looking for the number that we need to multiply 11 by to get an answer of 1 modulo 26. There are algorithms to calculate this, but it is often easiest to use trial and error to find the inverse.

[Picture](http://crypto.interactive-maths.com/uploads/1/1/3/4/11345755/1571506_orig.jpg)

So, the multiplicative inverse of the determinant modulo 26 is 19. We shall need this number later.

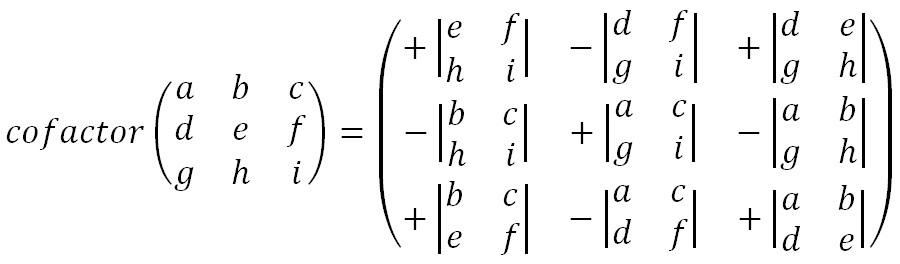
* Find the adjoint Matrix

The adjoint matrix is a matrix of the same size as the original. For a 3 x 3 matrix, this process is somewhat more complex than it was for a 2 x 2 matrix. It requires us to calculate 9 lots of 2 x 2 determinants, and assign them with the correct signs, and put them in the correct places. The algebraic representation is given below.

[](http://crypto.interactive-maths.com/uploads/1/1/3/4/11345755/9613397_orig.jpg)

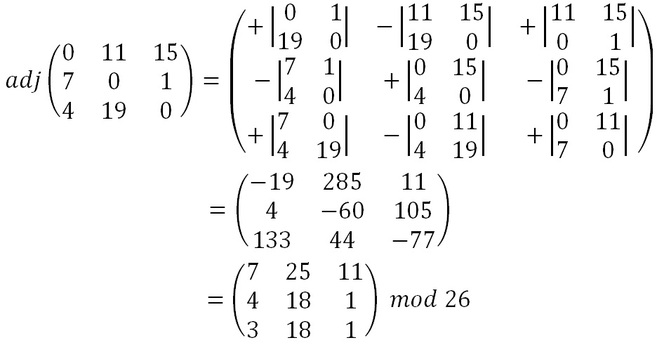
Calculating the adjoint matrix of a 3 x 3 matrix.

Although this seems a bit of a random selection of letters to place in each of the discriminants, it is defined as the transpose of the cofactor matrix, which is much easier to remember how to work out. To find the cofactor matrix, we take the 2 x 2 determinant in each position such that the four values in that position are the four values not in the same row or column as the position in the original matrix. The adjoint is then formed by reflecting the cofactor matrix along the line from top left of bottom right.

[](http://crypto.interactive-maths.com/uploads/1/1/3/4/11345755/7457658_orig.jpg)

The cofactor matrix can be used to find the adjoint matrix. Simply reflect it along the line from top left to bottom right of the matrix.

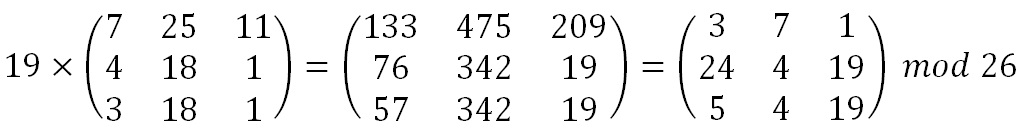
We also need to remember to take each of our values in the adjoint matrix modulo 26. So, for our example we get the working below.

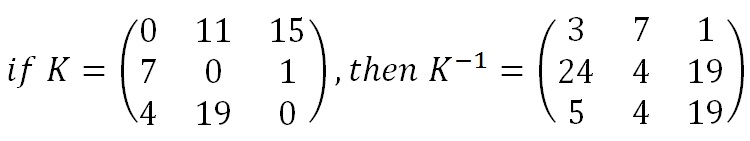
[](http://crypto.interactive-maths.com/uploads/1/1/3/4/11345755/9928545_orig.jpg)

Calculating the adjoint matrix of the key matrix.

* Multiply the Multiplicative Inverse of the Determinant by the adjoint Matrix

To get the inverse key matrix, we now multiply the inverse determinant (that was 19 in our case) from step 1 by each of the elements of the adjoint matrix from step 2. Then we take each of these answers modulo 26.

[](http://crypto.interactive-maths.com/uploads/1/1/3/4/11345755/9529458_orig.jpg)Multiplying the inverse of the determinant by the adjoint matrix gets the inverse key matrix.

[](http://crypto.interactive-maths.com/uploads/1/1/3/4/11345755/2417288_orig.jpg)

The final relationship between the key matrix and the inverse key matrix.

Finally, now we have the inverse key matrix, we multiply this by each

We have written a program in C language to encrypt and decrypt the messages. And they are attached with this report.

**Result:**

Hence with the linear algebra concept the Encoding and Decoding of the message is been done. Now if we enter a message to encrypt in the compiler then it encrypts and shows the encrypted word.

And it can be decrypted by using the inverse key matrix.

**Conclusion:**

There are several methods of conventional cryptography, and since it is not possible to present all the methods, very important and popular methods were presented.

It is seen that the modified Hill cipher Encryption and Decryption requires generating random Matrix, which is essentially the power of security. As we know in Hill cipher Decryption requires inverse of the matrix. Hence while decryption one problem arises that is. Inverse of the matrix does not always exist. Then if the matrix is not invertible them encrypted text cannot be decrypted. But this drawback is eliminated in modified Hill cipher algorithm.

At the same time, this method requires the cracker to find the inverse of many square matrices which is not computationally easy. So, this modified Hill-Cipher method is both easy to implement and difficult to crack.

**Reference:**

[1] [www.wikipedia.com](http://www.wikipedia.com)

[2] <http://www.dcode.fr/hill-cipher>

[3] [www.practicalcryptography.com/ciphers](http://www.practicalcryptography.com/ciphers)