SYNOPSIS

CRYPTOGRAPHER

Cryptography or cryptologyis the practice and study of techniques for [secure communication](https://en.wikipedia.org/wiki/Secure_communication) in the presence of third parties. More generally, cryptography is about constructing and analyzing [protocols](https://en.wikipedia.org/wiki/Communications_protocol) that prevent third parties or the public from reading private messages. Here I am going to encipher and decipher the message and codes in six different ways:

1. Caesar cipher
2. Atbash cipher
3. Polybius square cipher
4. Rail fence cipher
5. Trifid cipher
6. Bifid cipher

In detail explanation about the above types of enciphering the messages and deciphering the codes in different types:

1. **CAESAR CIPHER:**

It type of enciphering in which a letter has a direct translation to another letter.

Eg:

In this example, each letter in the plaintext message has been shifted 3 letters down in the alphabet. i.e A=D,B=E,……….

Plaintext: This is a secret message

Ciphertext: wklv lv d vhfuhw phvvdjh

1. **ATBASH CIPHER:**

The Atbash cipher is a very specific case of a substitution cipher where the letters of the alphabet are reversed. In otherwords, all As are replaced with Zs, all Bs are replaced with Ys, and so on.

Eg:

Plaintext: This is a secret message

Ciphertext: Gsrh rh z hvxivg nvhhztv

1. **POLYBIUS SQUARE CIPHER:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **1** | **2** | **3** | **4** | **5** |
| **1** | A | B | C | D | E |
| **2** | F | G | H | I | K |
| **3** | L | M | N | O | P |
| **4** | Q | R | S | T | U |
| **5** | V | W | X | Y | Z |

A Polybius Square is a table that allows someone to translate letters into numbers. To give a small level of encryption, this table can be randomized and shared with the recipient. In order to fit the 26 letters of the alphabet into the 25 spots created by the table, the letters i and j are usually combined. A alphabet is identified by the first row and then coloumn.

Eg:

Plaintext: This is a secret message  
Ciphertext: 44232443 2443 11 431513421544 32154343112215

1. **RAIL FENCE CIPHER:**

In the rail fence cipher, the plaintext is written downwards on successive "rails" of an imaginary fence, starting a new column when the bottom is reached. The message is then read off in rows.

Eg:

if we have 3 rails and a message of "This is a secret message", you would write out:

T S A C T S G  
H I S R M S E  
 I S E E E A J

The last J is just a random letter to fill in the space. The secret message is then condensed and regrouped.

Secret code:

TSACTSG HISRMSE ISEEEAJ

1. **TRIFID CIPHER:**

|  |  |  |  |
| --- | --- | --- | --- |
| *Layer 2* | | | |
|  | **1** | **2** | **3** |
| **1** | J | K | L |
| **2** | M | N | O |
| **3** | P | Q | R |

|  |  |  |  |
| --- | --- | --- | --- |
| *Layer 3* | | | |
|  | **1** | **2** | **3** |
| **1** | S | T | U |
| **2** | V | W | X |
| **3** | Y | Z |  |

The Trifid Cipher is the [Bifid Cipher](https://www.braingle.com/brainteasers/codes/bifid.php) taken to one more dimension. Instead of using a 5x5 [Polybius Square](https://www.braingle.com/brainteasers/codes/polybius.php), you use a 3x3x3 cube. Otherwise everything else remains the same.

|  |  |  |  |
| --- | --- | --- | --- |
| *Layer 1* | | | |
|  | **1** | **2** | **3** |
| **1** | A | B | C |
| **2** | D | E | F |
| **3** | G | H | I |

The first step is to use the cube to convert the letters into numbers. We will be writing the numbers vertically below the message in the order of Layer, Column, Row.

Eg:

secret message  
311213 2133111  
123322 1211112  
121321 2211132

The numbers are now read off horizontally and grouped into triplets.

311 213 213 311 112 332 212 111 121 213 212 211 132

The cube is used again to convert the numbers back into letters which gives us our ciphertext.

sppsdxmabpmjf

To decipher a Trifid encrypted message, you first convert each letter into its corresponding number via the cube. Now, divide the long string of numbers into three equal rows. Now, read off each column and use the cube to convert the three numbers into the plaintext letter.

1. **BIFID CIPHER:**

The Bifid Cipher uses a [Polybius square](https://www.braingle.com/brainteasers/codes/polybius.php) to encipher a message in a way that makes it fairly difficult to decipher without knowing the secret. This is because each letter in the ciphertext message is dependent upon two letters from the plaintext message.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **1** | **2** | **3** | **4** | **5** |
| **1** | A | B | C | D | E |
| **2** | F | G | H | I | K |
| **3** | L | M | N | O | P |
| **4** | Q | R | S | T | U |
| **5** | V | W | X | Y | Z |

The first step is to use the Polybius Square to convert the letters into numbers. We will be writing the numbers vertically below the message.

Eg:

secret message  
411414 3144121  
353254 2533125

The numbers are now read off horizontally and grouped into pairs.

41 14 14 31 44 12 13 53 25 42 53 31 25

The Polybius Square is used again to convert the numbers back into letters which gives us our ciphertext:

Qddltbcxkrxlk.

These are the different enciphering and deciphering methods I used to pass some secret messages.