**Cipher**

A cipher is defined over (K, M, C):

K – Set of all possible keys.

M – Set of all possible messages.

C – Set of all possible cipher texts.

The cipher itself is an [algorithm](http://en.wikipedia.org/wiki/Algorithm) for performing [encryption](http://en.wikipedia.org/wiki/Encryption) or [decryption](http://en.wikipedia.org/wiki/Decryption) (**E**,**D**). It has series of well-defined steps that can be followed as a procedure.

A cipher must follow properties in order to guarantee that using a **key** the **message** can be converted to a **cipher text**. And that using the same **key** the **cipher text** can be converted in the initial **message**.

E : K x M -> C

D: K x C -> M

**Exercise 1**

For this decryption each letter correspond to another one in the alphabet

A stands for Z

B stands for Y

C stands for X

An extra help:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Z Y X W V U T S R Q P O N M L K J I H G F E D C B A

**Exercise 2**

In [cryptography](http://en.wikipedia.org/wiki/Cryptography), a Caesar cipher, also known as the shift cipher, is one of the simplest and most widely known [encryption](http://en.wikipedia.org/wiki/Encryption) techniques. It is a type of [substitution cipher](http://en.wikipedia.org/wiki/Substitution_cipher) in which each letter in the [plaintext](http://en.wikipedia.org/wiki/Plaintext) is replaced by a letter some fixed number of positions down the [alphabet](http://en.wikipedia.org/wiki/Alphabet). For example, with a left shift of 5, F would be replaced by A, G would become B, and so on.

**Exercise 3**

The Diffie–Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a [shared secret](http://en.wikipedia.org/wiki/Shared_secret) key over an insecure [communication](http://en.wikipedia.org/wiki/Communication) [channel](http://en.wikipedia.org/wiki/Channel_(communications)). This key can then be used to encrypt subsequent communications using a [symmetric key](http://en.wikipedia.org/wiki/Symmetric_key) [cipher](http://en.wikipedia.org/wiki/Cipher).

Diffie–Hellman establishes a shared secret that can be used for secret communications while exchanging data over a public network. The crucial part of the process is that [Alice and Bob](http://en.wikipedia.org/wiki/Alice_and_Bob) exchange their secret colors in a mix only. Finally this generates an identical key that is computationally difficult (impossible for modern [supercomputers](http://en.wikipedia.org/wiki/Supercomputers) to do in a reasonable amount of time) to reverse for another party that might have been listening in on them. Alice and Bob now use this common secret to encrypt and decrypt their sent and received data. The starting color (yellow) is arbitrary, but is agreed on in advance by Alice and Bob, and does not need to be secret.

**Cryptograph Explanation**

The simplest and the original implementation of the protocol uses the [multiplicative group of integers modulo](http://en.wikipedia.org/wiki/Multiplicative_group_of_integers_modulo_n) p, where p is [prime](http://en.wikipedia.org/wiki/Prime_number), and g is a [primitive root](http://en.wikipedia.org/wiki/Primitive_root_modulo_n) modulo p. Here is an example of the protocol, with non-secret values in blue, and secret values in **red**.

1. [Alice and Bob](http://en.wikipedia.org/wiki/Alice_and_Bob) agree to use a prime number *p* = 23 and base *g* = 5 (which is a [primitive root modulo](http://en.wikipedia.org/wiki/Primitive_root_modulo_n) 23).
2. Alice chooses a secret integer ***a*** = **6**, then sends Bob *A* = *g****a*** mod *p*
   * *A* = 5**6** mod 23 = 8
3. Bob chooses a secret integer ***b*** = **15**, then sends Alice *B* = *g****b*** mod *p*
   * *B* = 5**15** mod 23 = 19
4. Alice computes ***s*** = *B****a*** mod *p*
   * ***s*** = 19**6** mod 23 = **2**
5. Bob computes ***s*** = *A****b*** mod *p*
   * ***s*** = 8**15** mod 23 = **2**
6. Alice and Bob now share a secret (the number **2**).