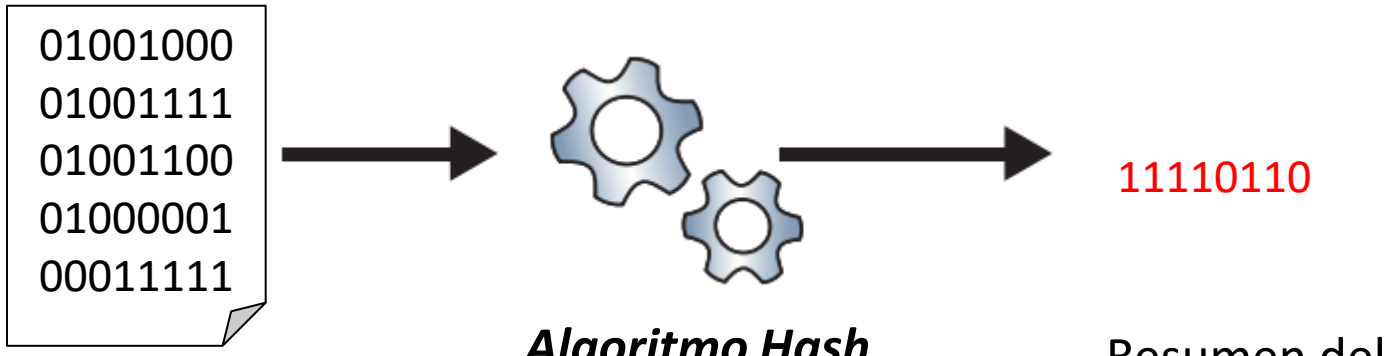
# Lenguaje de Computadoras y sus principales Algoritmos

# Algoritmos Hash

Un algoritmo hash transforma un “archivo de entrada” de longitud variable en una salida de longitud fija, que se conoce como “resumen hash” de ese archivo.

# Algoritmos Hash



# Algoritmos Hash

Principales propiedades de una función hashing h:

**Resistencia a preimágenes**:

Dado z es computacionalmente no factible hallar algún x tal que h(x) = z

**Resistencia a segundas preimágenes**:

Dado x es computacionalmente no factible hallar x'≠x tal que h(x) = h(x')

# Algoritmos Hash

**MD5 (Message Digest 5):**

◦ Acepta una entrada de cualquier longitud y devuelve una cadena de 128 bits.

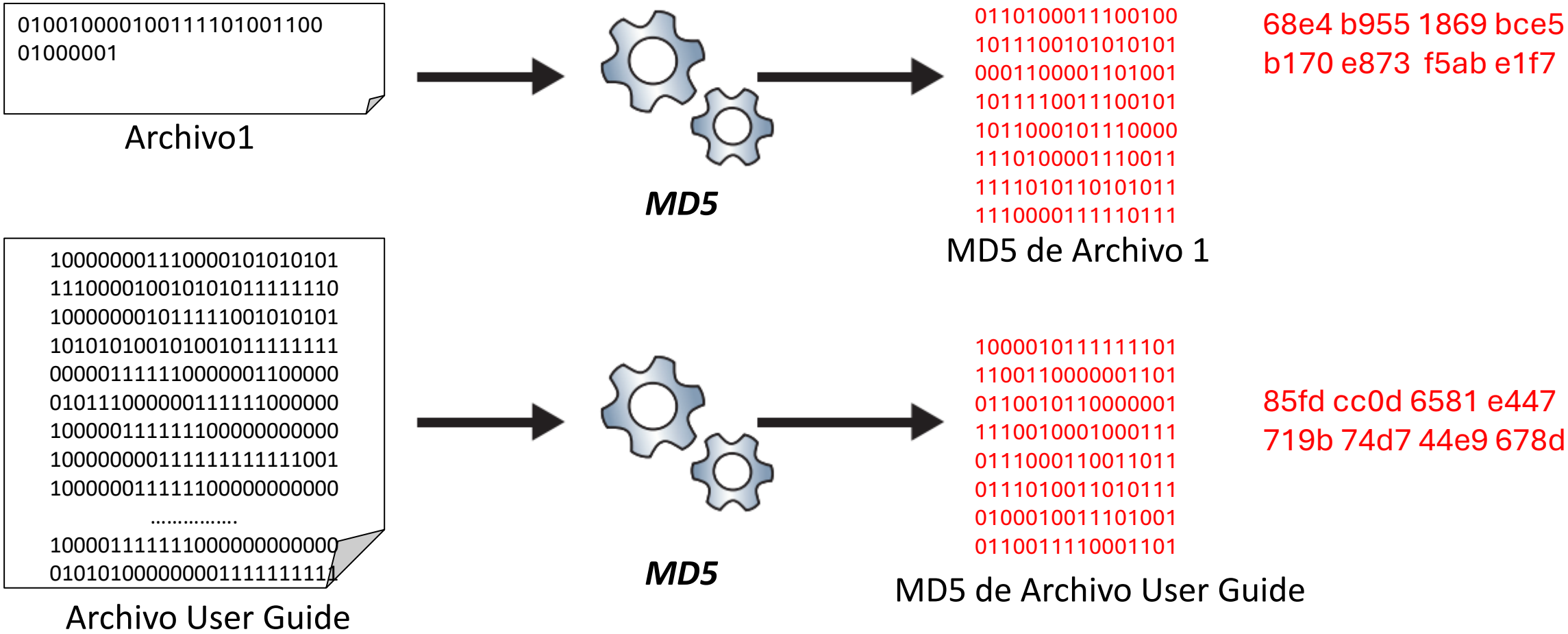
**SHA (Security Hash Algorithm):**

◦ SHA 1 devuelve una cadena de 160 bits.

◦ SHA 256 y SHA 512 con una longitud de salida de 256 y 512 respectivamente.

Ejemplos: https://www.virtualbox.org/.

# Hash MD5


01001000010011110100110001000001
Archivo1
MD5
0110100011100100
1011100101010101
0001100001101001
1011110011100101
1011000101110000
1110100001110011
1111010110101011
1110000111110111
68e4 b955 1869 bce5
b170 e873 f5ab e1f7
MD5 de Archivo 1
10000000111000010101010111
11100001001010101111111010
10000000101111100101010101
10101010010100101111111100
00000111111000000110000001
01011100000011111100000000
10000011111110000000000000
10000000011111111111111001
10000001111110000000000000
.....
10000111111100000000000001
01010100000000111111111101
Archivo User Guide
MD5
1000010111111101
1100110000001101
0110010110000001
1110010001000111
0111000110011011
0111010011010111
0100010011101001
0110011110001101
85fd cc0d 6581 e447
719b 74d7 44e9 678d
MD5 de Archivo User Guide

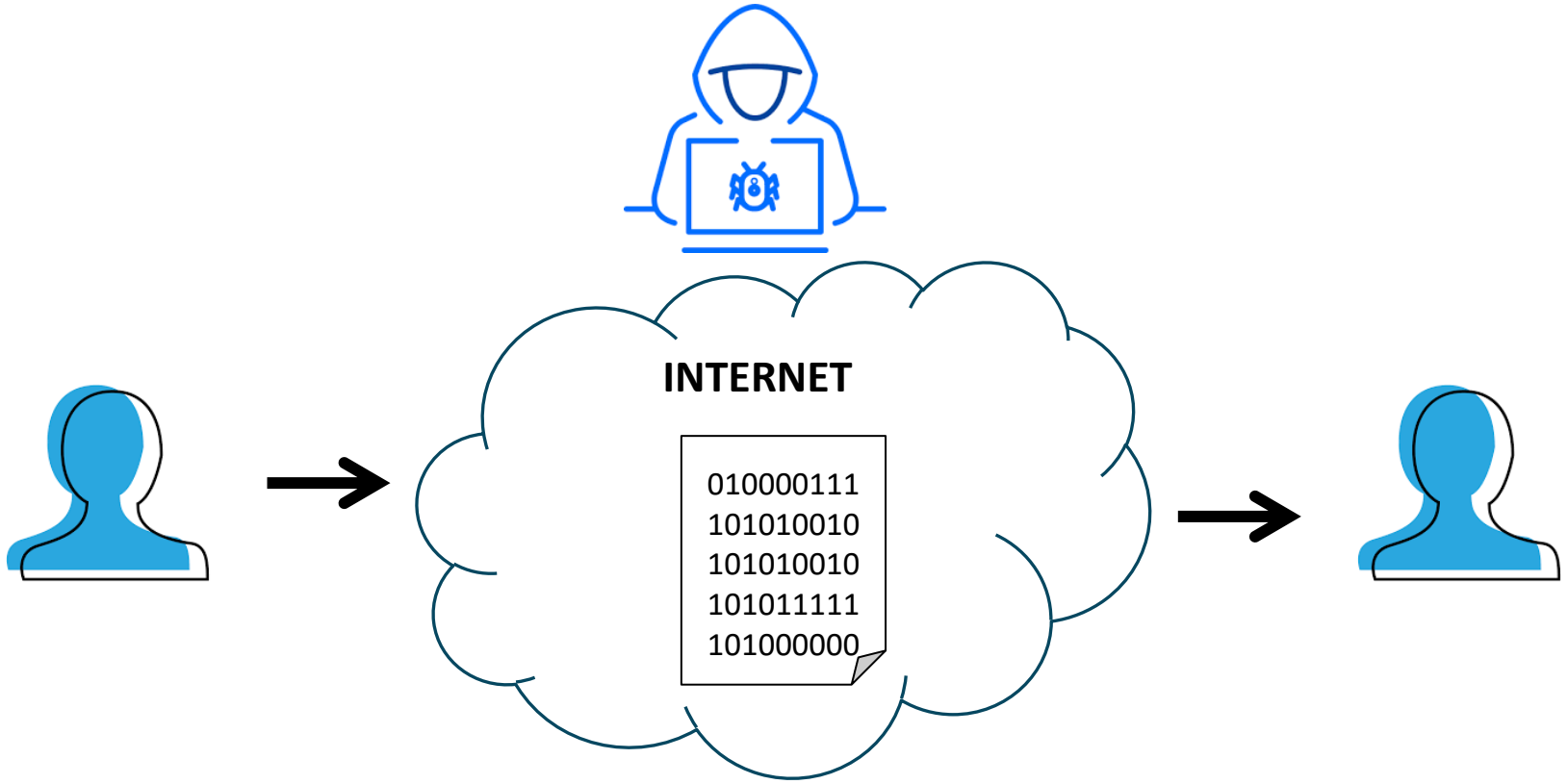
# Algoritmos Hash: ¿Para qué sirven?

Aplicaciones:

Comprobación e **integridad** de archivos recibidos a través de Internet.

Para almacenar las **claves de accesos de usuario** bases de datos o similar.

# ¿Hay algún otro riesgo?



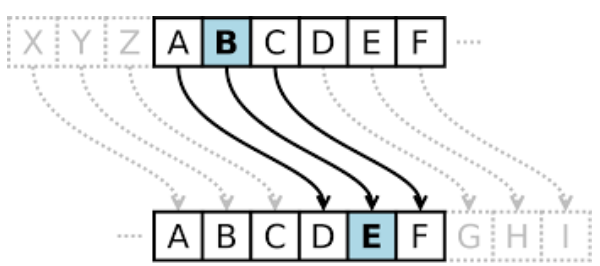
# Encriptar o Cifrar

La palabra criptografía viene del griego:

**cripto** →que significa «ocultar»

**graphos** →que significa «escribir»

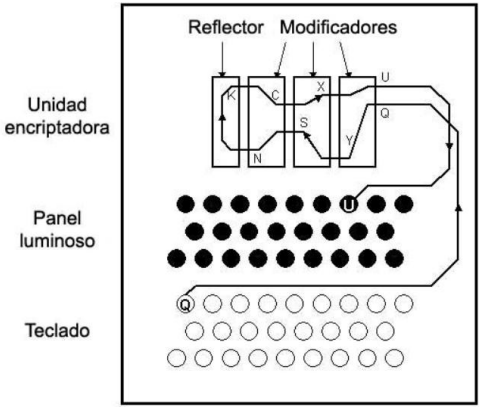
Se podría interpretar como: ***escribir mensajes de forma oculta.***




# Evolución Histórica- Criptografía Clásica

Métodos rudimentarios
***Cifrado de César***: Un carácter o conjunto de caracteres era **sustituido por otro carácter** o conjunto de caracteres.

***Cifrado Escítala:*** Se **cambia el orden** de los caracteres del mensaje para cifrarlo.




# Evolución Histórica- Criptografía Moderna

En esta época la criptografía avanza, mejorando los dispositivos con los cuales se encriptaba.

El caso más conocido es la **Máquina Enigma.**

# Evolución Histórica- Criptografía Actual

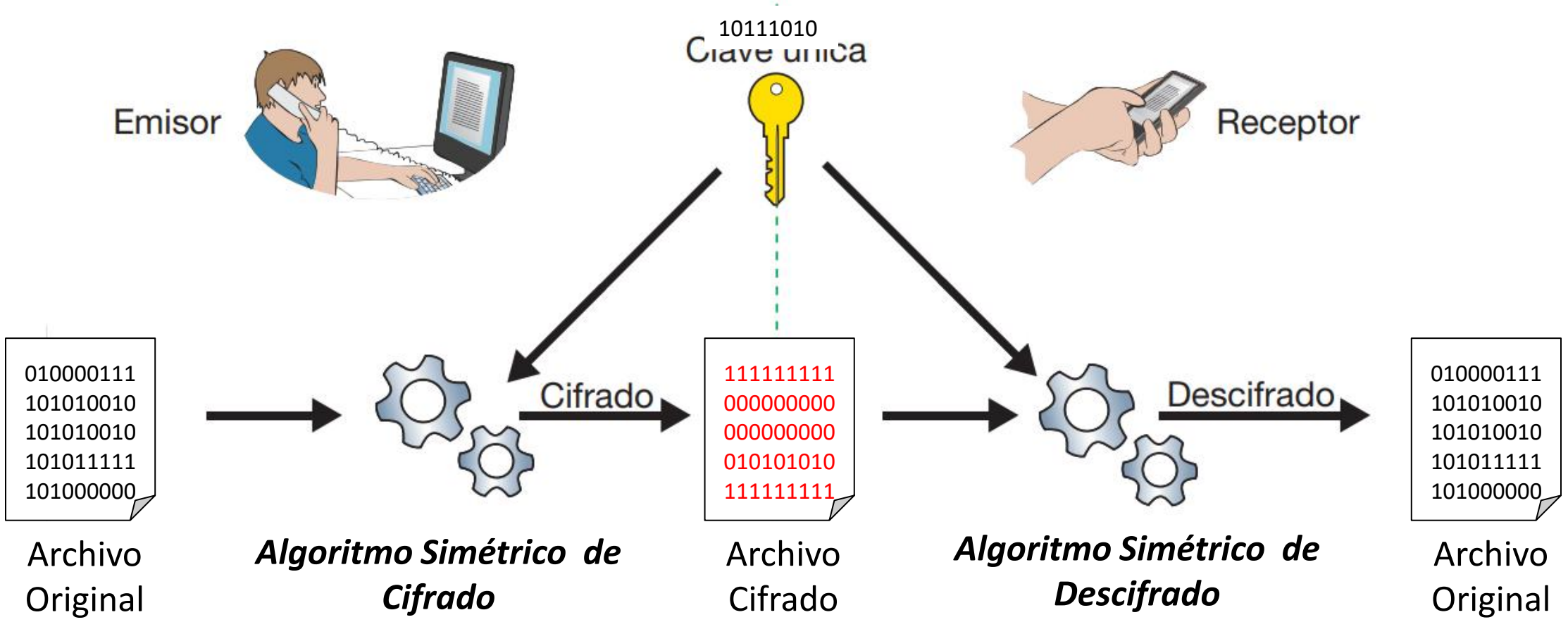

Con la aparición de las **computadoras** y la posibilidad de realizar cálculos matemáticos complejos, comienzan a surgir **algoritmos de cifrado**, que son los que se utilizan actualmente para cifrar la información.

Existen dos clases de métodos de encriptación basados en claves:

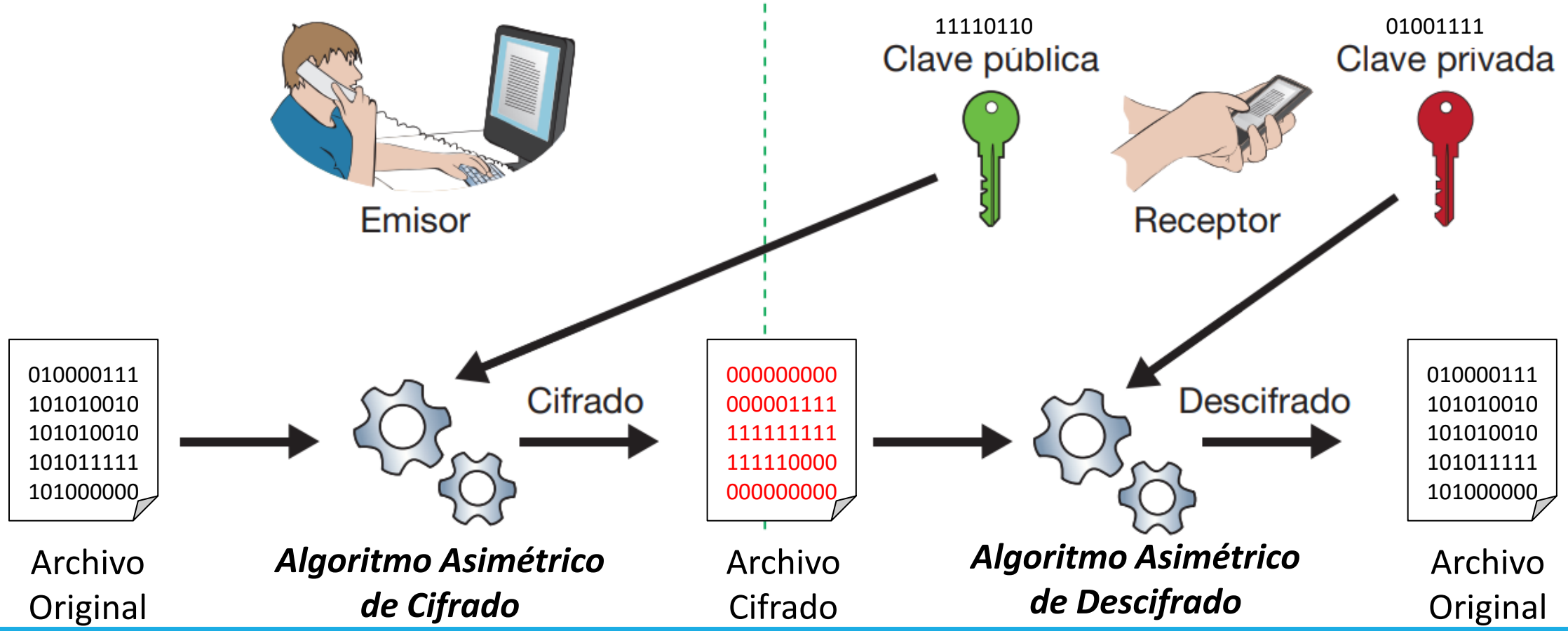
– Cifrado simétrico

– Cifrado asimétrico

# Cifrado Simétrico



# Cifrado Asimétrico



# Algoritmos Simétricos y Asimétricos

- DES (Data Encription Standard):
  Clave de 64 bits, bloque de 64 bits.
- DES triple (aplicar DES tres veces con al menos 2 claves distintas)
- AES (Advanced Encryption Standard)
  Clave de 128, 192 o 256 bits, bloque de 128 bits.
- IDEA (International Data Encryption Algorithm)
  Clave de 128 bits, bloque de 64 bits.
- RSA (Rivest, Shamir y Adleman)
  Clave de 1024, 2048 o 4096 bits, bloque de 1024 bits.
  Ejemplos: https://emn178.github.io/online-tools/des/encrypt/

# Algoritmos de Cifrado

Principio de Kerckhoff:

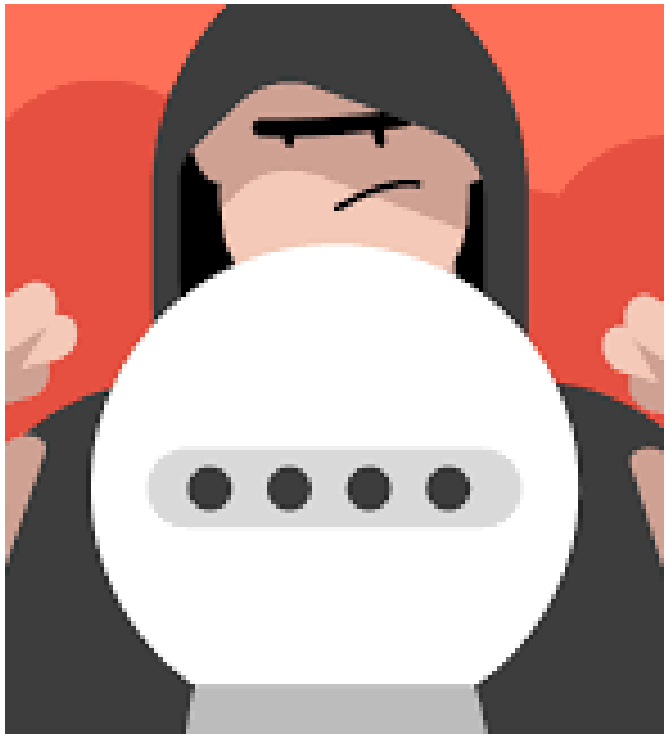
***"Todos los algoritmos de cifrado deben ser públicos; sólo las claves deben ser secretas"***

# Criptografía- Tipos Ataques

**Ataques por fuerza bruta**: consiste en ir probando con todas las combinaciones posibles de claves, hasta encontrar la que permita acceder al mensaje. Es costoso en tiempo de procesamiento.

**Ataques de diccionario:** consiste en intentar descifrar un mensaje encriptado, probando con todas las palabras de un diccionario como clave.

**Ataques criptoanalíticos**: atacan la estructura del algoritmo o de los protocolos que lo utilizan, buscando un "atajo" para realizar menos trabajo que un ataque por fuerza bruta.



# Algoritmos Cifrado: ¿Para qué se usan?

Aplicación:

Garantizar **confidencialidad** de la información.

Ejemplo: WhatsApp

# Actividad

Lectura: CiberAtaqueOcasa.pdf

Analizar esta lectura y buscar su vinculación con los conceptos trabajados.

# Preguntas y Conclusiones