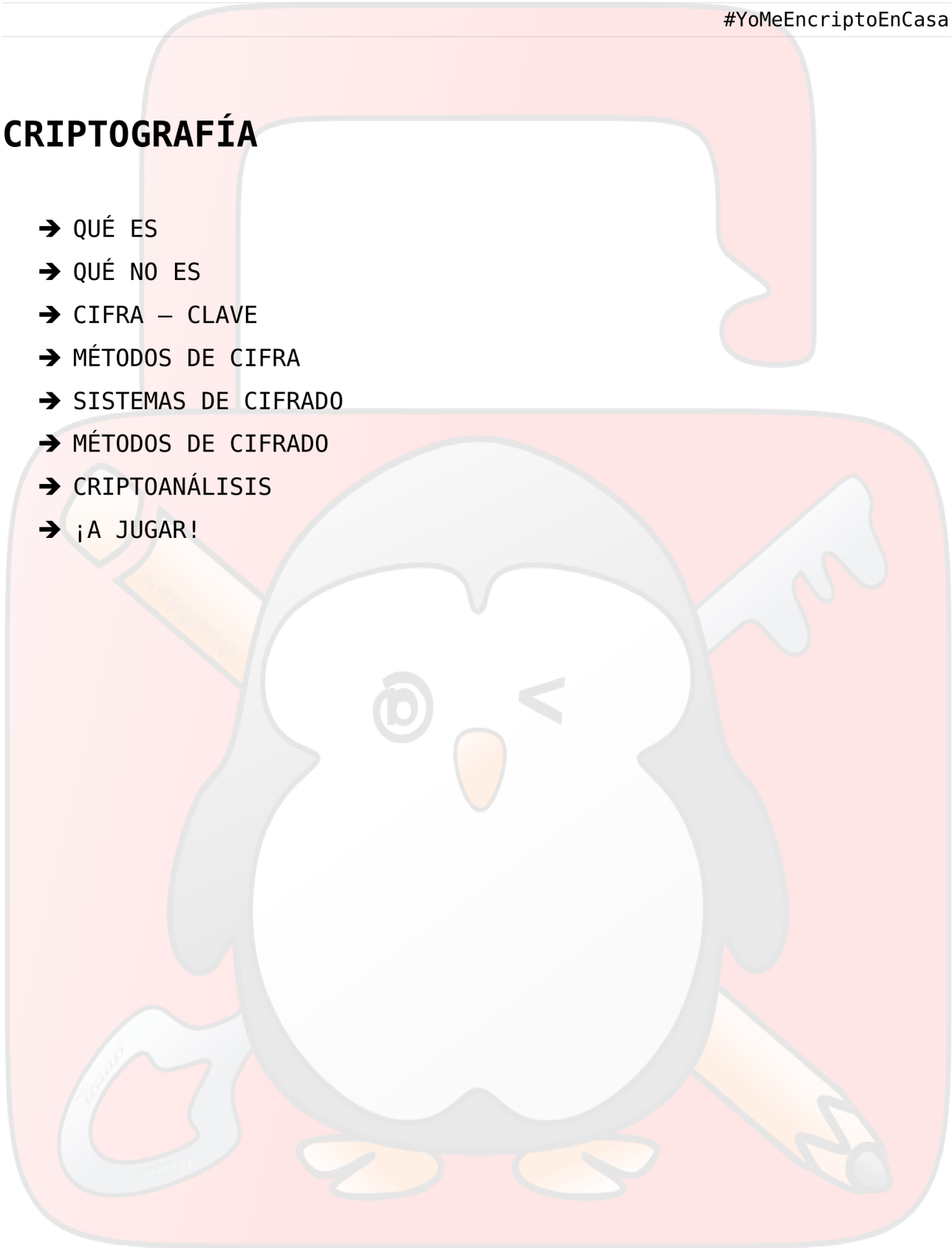
CRIPTOGRAFÍA

- ➔ QUÉ ES
- ➔ QUÉ NO ES
- ➔ CIFRA – CLAVE
- ➔ MÉTODOS DE CIFRA
- ➔ SISTEMAS DE CIFRADO
- ➔ MÉTODOS DE CIFRADO
- ➔ CRIPTOANÁLISIS
- ➔ ¡A JUGAR!



QUÉ ES LA CRIPTOGRAFÍA

Criptografía: palabra que proviene del griego kryptos “oculto” y grafía “representación gráfica; escritura”

La Real Academia Española la define como “el Arte de escribir con clave secreta o de un modo enigmático”.

El proceso de convertir un texto ordinario, denominado “texto en claro” en un galimatías sin sentido aparente (texto cifrado) empleando para ello un método de cifra es lo que se conoce como cifrar[1].

Y llamamos descifrar[2] al proceso inverso: partiendo de un texto cifrado obtener un texto en claro.

QUÉ NO ES LA CRIPTOGRAFÍA

La criptografía **NO** oculta a la vista el mensaje que se quiere enviar, sólo lo convierte en algo a priori ininteligible; si lo que hacemos es ocultar el mensaje, que no se vea en el medio portador, estaremos hablando de Esteganografía.

Como ejemplos de esteganografía tenemos la escritura con tinta invisible (zumo de limón, por ejemplo), la escritura en una cabeza rapada (crece el pelo y no se ve), escribir sobre la cáscara de un huevo duro con una tinta de alumbre y vinagre (traspasa la cáscara y se queda escrito sobre la clara cocida), el micropunto, el “watermarking” (esconder texto en imágenes digitales o música digital)

1 Cifrar: Transcribir en guarismos, letras o símbolos, de acuerdo con una clave, un mensaje o texto cuyo contenido se quiere proteger. Fuente: https://dle.rae.es/cifrar#9Blo7Je

2 Descifrar: https://dle.rae.es/descifrar?m=form

QUÉ ES UN MÉTODO DE CIFRA

Es el conjunto de pasos (algoritmo) que permite el cifrado y el descifrado a partir de una *clave secreta*.

Esta clave puede ser la misma para cifrar y descifrar, con lo que estaríamos hablando de cifra simétrica; o pueden ser distintas y nos estaríamos refiriendo a cifrado asimétrico.

Esta clasificación de cifra simétrica-asimétrica es también la que marca la evolución de la criptografía: *criptografía clásica* (métodos de cifrado simétricos) y *criptografía moderna* (cifrados asimétricos).

El punto de inflexión lo marca, más o menos, el final de la Segunda Guerra Mundial (Enigma) y la aparición de los ordenadores: se empiezan a desarrollar y emplear métodos de cifrado con clave asimétrica, que hacen uso de complejas operaciones matemáticas con números primos muuuuy grandes.

DIFERENCIA CIFRA – CLAVE

Cifra: es el método que se emplea para convertir el texto en claro en un texto ininteligible

Clave[3]: secuencia de números o letras que controla la operación del algoritmo de cifrado, es decir la transformación del texto plano a texto cifrado, y que nada tiene que ver con el texto a cifrar.

3 Clave: https://es.wikipedia.org/wiki/Clave_(criptografía)

SISTEMAS DE CIFRADO

Básicamente hay dos:

- sustitución: sustituyen unas letras por otras, manteniendo el orden de las letras en el mensaje.

- transposición: cambian el orden de las letras que conforman el mensaje.

Obviamente, se pueden combinar ambos métodos con el fin de hacer más fuerte el cifrado, de más difícil averiguación.

MÉTODOS DE CIFRADO (Simétricos, o clásicos)

- Método Atbash (siglo VI a.C.). Sustitución.
- Escítala espartana (siglo V a.C.). Transposición.
- Tablero de Polibio (siglo II a.C.). Sustitución.
- Cifrado de César (± 121 d.C.). Sustitución.
- Cifrado Templario (siglo XIV). Sustitución por símbolos.
- Discos de Alberti (siglo XV). Sustitución polialfabética.
- Tabla de Tritemio (siglo XVI). Sustitución polialfabética
- Tablero de Vigenere (siglo XVI). Sustitución polialfabética evolucionado de la *tabula recta* del abad Tritemio.
- Alfabeto binario de Bacon (siglo XVII). Sustitución
- Método Pig Pen o de los masones (siglo XVIII).Sustitución.
- La cifra Rail Fence (siglo XIX). Transposición.
- La cifra de Lord Wolseley (siglo XIX). Sustitución.
- Rejillas rotativas de Fleissner (siglo XX). Transposición.
- El código de los Scouts (siglo XX). Sustitución.
- Máquina Enigma (siglo XX). Sustitución.

QUÉ ES EL CRIPTOANÁLISIS

El criptoanálisis es el arte de romper los códigos y las cifras.

Complementario de la criptografía, ambos conforman la disciplina, o la ciencia, de la *Criptología*.

Para los cifrados clásicos, de clave simétrica y que son bien de sustitución, de transposición o de ambas, el método por excelencia para criptoanalizar los textos cifrados es el análisis de la distribución de la frecuencia de aparición de las letras en el mensaje. Teniendo en cuenta que cada idioma tiene para cada una de las letras de su alfabeto una distribución porcentual distinta, esto nos ayuda a aplicar una equivalencia entre la frecuencia en que aparecen las letras en el texto cifrado y la frecuencia de aparición de las letras en el idioma del texto en claro.

Esta es una ayuda más que importante para ayudarnos a romper el código.

Pero ¡tranquilos! Que nosotros no vamos a ponernos a criptoanalizar mensaje alguno: eso lo dejamos para cuando estéis estudiando matemáticas en la Universidad, dentro de unos años.

Bibliografía, fuentes:

- ✔ Criptografía, los lenguajes secretos a lo largo de la Historia (Carlos Taranilla), editorial Guadalmazan, ISBN 9788494608599
- ✔ The Code Book, the secrets behind codebreaking (Simon Singh), editorial RandomHouseTeens, ISBN 9780385730624
- ✔ Codes, Ciphers and Secret Writing (Martin Gardner), editorial Dover Publications, ISBN 9780486247618

- ✔ http://www.practicalcryptography.com/
- ✔ https://www.dcode.fr/en
- ✔ https://es.wikipedia.org
- ✔ http://en.wikipedia.org
- ✔ https://es.wikipedia.org/wiki/Clave_(criptografía)
- ✔ http://mikelgarcialarragan.blogspot.com/2016/08/criptografia-xxvi-sabias-que-ii.html
- ✔ https://joseluistabaracarbajo.gitbooks.io/criptografia-clasica/content/index.html
- ✔ https://macs358.org/chapters/01/introduction.html
- ✔ http://www.nymphomath.ch/crypto/activites/index.html
- ✔ https://cryptii.com/
- ✔ http://www.quadibloc.com/crypto/intro.htm
- ✔ http://www.criptohistoria.es/
- ✔ https://es.wikipedia.org/wiki/Rejilla_criptogr%C3%A1fica

App Android: Cryptography, de http://www.nitramite.com

Juego de cartas: CryptoGo Game, de https://www.cryptogogame.com