te lo cuenta la criptografía

Guía de los talleres manipulativo y tecnológico

te lo cuentan las matemáticas

te lo cuenta la criptografía

Contenido

te lo cuenta la criptografía

1. *Te lo cuentan los algoritmos y la criptografía*

La primera parte del programa *Te lo cuentan las matemáticas* recibe el nombre de *Te lo cuenta la criptografía* y está organizada en torno al segundo martes de octubre, en el que se celebra el Día Internacional de Ada Lovelace.

Dicha primera parte cuenta con dos actividades que la conforman: *Te lo cuenta una espía*, que a su vez consta de dos talleres diferenciados (uno manipulativo y otro tecnológico); y *Te lo cuentan Ada Lovelace y… Xabier García,* un encuentro con un investigador junior en el que se relata la vida científica y personal de matemáticos referentes como Ada Lovelace mientras, paralelamente, se expone el recorrido personal y científico del joven investigador relator.

En la siguiente tabla podemos observar la organización de esta primera parte del programa, incluidos los contenidos y objetivos a desarrollar:

Te lo cuentan los algoritmos y la criptografía **DÍA INTERNACIONAL DE ADA LOVELACE**			
Nombre acción	**Tipo acción**	**Contenidos**	**Resultados y objetivos**
Te lo cuenta una espía	Taller manipulativo	Transmisión de mensajes: clave del César. Aplicaciones: espionaje	Método para cifrar y descifrar mensajes. Máquina de transmisión de mensajes
	Taller tecnológico	Algoritmos para cifrar y descifrar Aplicaciones: firma digital	Programación con Scratch. Software y firma digital.
Te lo cuentan Ada Lovelace y… Xabier García	Encuentro con investigador junior	Historia personal y científica de Ada Lovelace y… Xabier García	Visibilizar la profesión de los investigadores e investigadoras matemáticas. Generar vocaciones matemáticas, especialmente en las niñas.

En esta guía nos centraremos en el diseño y desarrollo de los talleres manipulativo y tecnológico de la actividad *Te lo cuenta una espía.*

1.1. Objetivos específicos

El programa *Te lo cuentan… las matemáticas* persigue cuatro objetivos principales: apoyar la enseñanza de las matemáticas en la última etapa de Educación Primaria, desde un punto de vista científico, tecnológico, atractivo, innovador y complementario a los currículos; fomentar la utilidad social y económica de las matemáticas; promover el gusto e interés por las matemáticas, con el fin último de generar vocaciones matemáticas, poniendo un énfasis especial en las niñas; y visibilizar la profesión de investigador o investigadora en matemáticas.

Para ello, con los talleres manipulativos se pretende que los participantes aprendan matemáticas de un modo diferente al habitual: a través de la manipulación de objetos y materiales a su disposición. Por otra parte, para mantener el interés del público infantil nos apoyaremos también en procesos con soporte tecnológico de forma que puedan trabajar las matemáticas a través de las nuevas tecnologías. Con ambas actividades se busca en definitiva promover el gusto e interés por las matemáticas en el alumnado y convertirlas en algo más atractivo y cercano.

Más concretamente, en el taller manipulativo asociado a *Te lo cuenta una espía* se pretende que los alumnos comprendan la implicación de las matemáticas en el cifrado y descifrado de mensajes, realicen en primera persona dicho cifrado y descifrado y protagonicen personalmente los roles implicados en una comunicación cifrada: emisor, interceptor y receptor.

En el taller tecnológico asociado se tratará el concepto de algoritmo, desarrollando algoritmos concretos para el cifrado y descifrado de mensajes en Scratch. De este modo se intentará que los participantes afiancen los conceptos del taller manipulativo, comprendan la importancia de las matemáticas en el mundo tecnológico que nos rodea y se conviertan en programadores por un día.

2. Taller manipulativo *Te lo cuenta una espía*

2.1. Contenidos a tratar

El taller manipulativo *Te lo cuenta una espía* se centrará en la ***criptografía***, la ciencia que estudia las técnicas cifrado de mensajes con la finalidad de hacerlos solamente comprensibles para los receptores autorizados. Históricamente, en contraposición a la criptografía nace el ***criptoanálisis***, que es la ciencia que estudia los cifrados con el objetivo de romper su seguridad, permitiendo que los mensajes puedan ser descifrados por receptores no autorizados.

El cifrado César

Uno de los primeros sistemas de cifrado conocidos en la historia es el cifrado César. Recibe su nombre del emperador Julio César, quien observaba como sus mensajeros eran interceptados constantemente por sus enemigos. Estos pretendían descubrir las instrucciones militares que el César enviaba a sus ejércitos para obtener ventaja en las batallas.

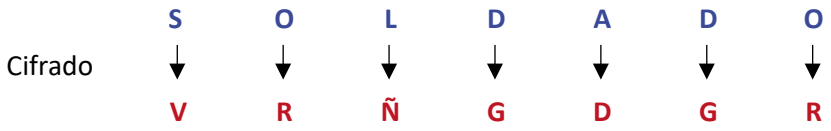
Para evitarlo el emperador decidió enviar sus mensajes cifrados, de forma que solamente las personas destinatarias de esos mensajes fuesen capaces de entenderlos. Aunque cualquier otra persona interceptara al mensajero, el contenido de la carta no tendría sentido aparentemente.

El sistema utilizado por el César funcionaba de la siguiente manera: consistía en sustituir cada letra del mensaje original por la que está situada 3 posiciones después en el abecedario. De esta forma la A sería sustituida por la D, la B por la E… y así sucesivamente.

Por ejemplo, la palabra “SOLDADO” se cifraría de la siguiente forma:

Figura 1

Cifrado de César de la palabra “soldado”, utilizando clave 3



De esta forma, si el mensaje era interceptado por un enemigo la única información que este recibiría sería “VRÑGDGR”.

Ayudándose de la tabla inferior, para cifrar un mensaje bastaría con buscar las letras en la primera fila y sustituirlas por las que están inmediatamente debajo en la segunda fila.

Tabla 1

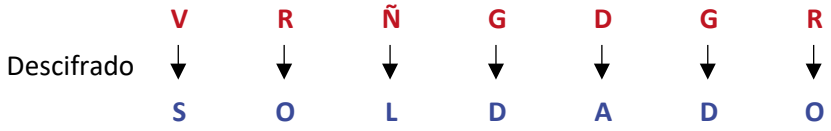
Correspondencia del alfabeto desplazando tres puestos cada letra

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

Ya que el receptor era conocedor de este desplazamiento de 3 letras, recibido el mensaje bastaba con sustituir cada letra por la que se encontraba 3 puestos antes en el abecedario. Utilizando de nuevo la tabla, sería pasar de la fila inferior a la superior. Recuperando el ejemplo el proceso de descifrado sería:

Figura 2

Descifrado de la palabra “vrñgdgr” con cifrado César



Los cifrados de sustitución

El cifrado utilizado por el emperador Julio César es el primer cifrado de sustitución que se conoce. Como su propio nombre indica, los ***cifrados de sustitución*** son aquellos en los que los mensajes se dividen en unidades más pequeñas, que pueden ser letras (lo más habitual) o grupos de letras, y se sustituyen por otras unidades siguiendo un patrón conocido por emisor y receptor. Este patrón es el que permite realizar el proceso de cifrado y también el de descifrado, y es importante que sea:

- sencillo de utilizar: ya que los mensajes tienen que poder cifrarse y descifrarse rápidamente;
- fácil de transmitir: si para transmitir el patrón necesitamos enviar otro mensaje sin codificar, este puede ser interceptado por el enemigo dándole la posibilidad de descifrar también los mensajes, aun no siendo en un principio una persona autorizada.

Por estas razones los sistemas de cifrado suelen utilizar una clave. En cualquier sistema de cifrado se denomina ***clave*** a cierta información (puede ser una palabra, un número…), que es conocida a priori solamente por emisor y receptor, ya que permite cifrar y descifrar cualquier mensaje. Concretamente, en el cifrado César la clave sería el número 3, es decir, el número que indica el desplazamiento del alfabeto utilizado. Solamente con esta información, en este caso un número, ambos protagonistas pueden llevar a cabo la comunicación cifrada.

Cambiando esta clave por cualquier otro número del 1 al 26, ya que nuestro abecedario tiene 27 letras, obtenemos otro cifrado de sustitución distinto. Éste será diferente al del César y tendrá por clave el número de letras que debemos desplazar el alfabeto. Por ejemplo, si escogemos como clave el 5, el cifrado de la palabra "SOLDADO" sería el siguiente:

Figura 3
Cifrado de la palabra "soldado", utilizando clave 5

S	O	L	D	A	D	O
↓	↓	↓	↓	↓	↓	↓
X	T	P	I	F	I	T

El mensaje cifrado sería "XTPIFIT", que vemos que difiere del cifrado con clave César (Figura 1) por lo que da lugar a otro sistema de cifrado de sustitución.

Muchos siglos después del nacimiento de este primer cifrado de sustitución, en 1466, Leon Battista Alberti publicó en su tratado *De Cifris* el primer sistema de cifrado de sustitución polialfabético que se conoce. Un ***cifrado de sustitución polialfabético*** es aquel en el que no hay una correspondencia unívoca letra a letra, es decir, una misma letra en dos posiciones diferentes puede dar lugar a dos letras distintas en el mensaje cifrado. Este tipo de cifrado proporciona una mayor seguridad que el precedente, el de César.

En dicha obra además describe un artilugio que permite cifrar y descifrar con ese nuevo método: el conocido como disco de Alberti. Esta máquina de cifrado consistía en dos discos ensamblados que giran uno sobre otro y el cifrado y descifrado propuestos requería realizar varios giros en el proceso. Obsérvese que estos discos incluyen caracteres, como números o símbolos, ajenos al abecedario.

Figura 4
Disco de Alberti

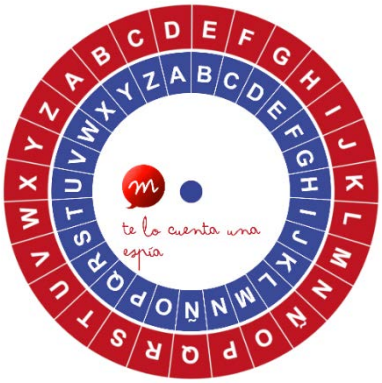
Nota. Tomada de *Disco de Alberti* [Fotografía], 2021, Wikipedia (https://es.wikipedia.org/wiki/Cifrado_de_Alberti).

Si simplificamos esta máquina y colocamos un alfabeto completo en cada uno de los discos, podremos escoger una correspondencia entre el alfabeto del disco externo y del interno para llevar a cabo el cifrado César. Estos discos harían el papel de la tabla de correspondencias (Tabla 1), pero en este caso bastará con ajustar la letra con la que cifraremos la A para obtener directamente la correspondencia del resto del alfabeto.

En la siguiente figura vemos como deberíamos colocar los discos para el cifrado César, haciendo coincidir la A azul del disco interior con la D roja del disco exterior.

Figura 5

Posición de los discos para el cifrado y descifrado con clave 3



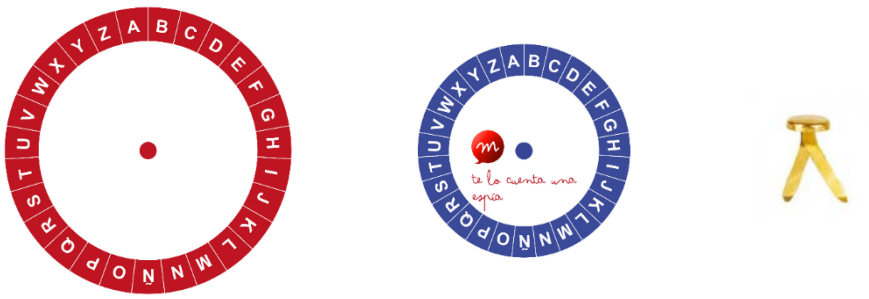
Las ventajas de utilizar este objeto que acabamos de diseñar es que nos permitirá, por un lado, trabajar más rápidamente y, por otro, cifrar y descifrar para cualquier desplazamiento del alfabeto, no solamente para el de 3 posiciones.

2.2. Material

El material para elaborar el taller consiste, por una parte, en material escolar básico (bolígrafos azul y rojo) y, por otra, en material específico. Este último consiste en dos discos (uno de color rojo y otro azul) con los alfabetos, que se pueden encontrar en la página web http://telocuentanlasmatematicas.webs.uvigo.gal/, un encuadernador o chincheta abierta (Figura 6) y la ficha "Comunicación cifrada" (Figura 7).

Figura 6

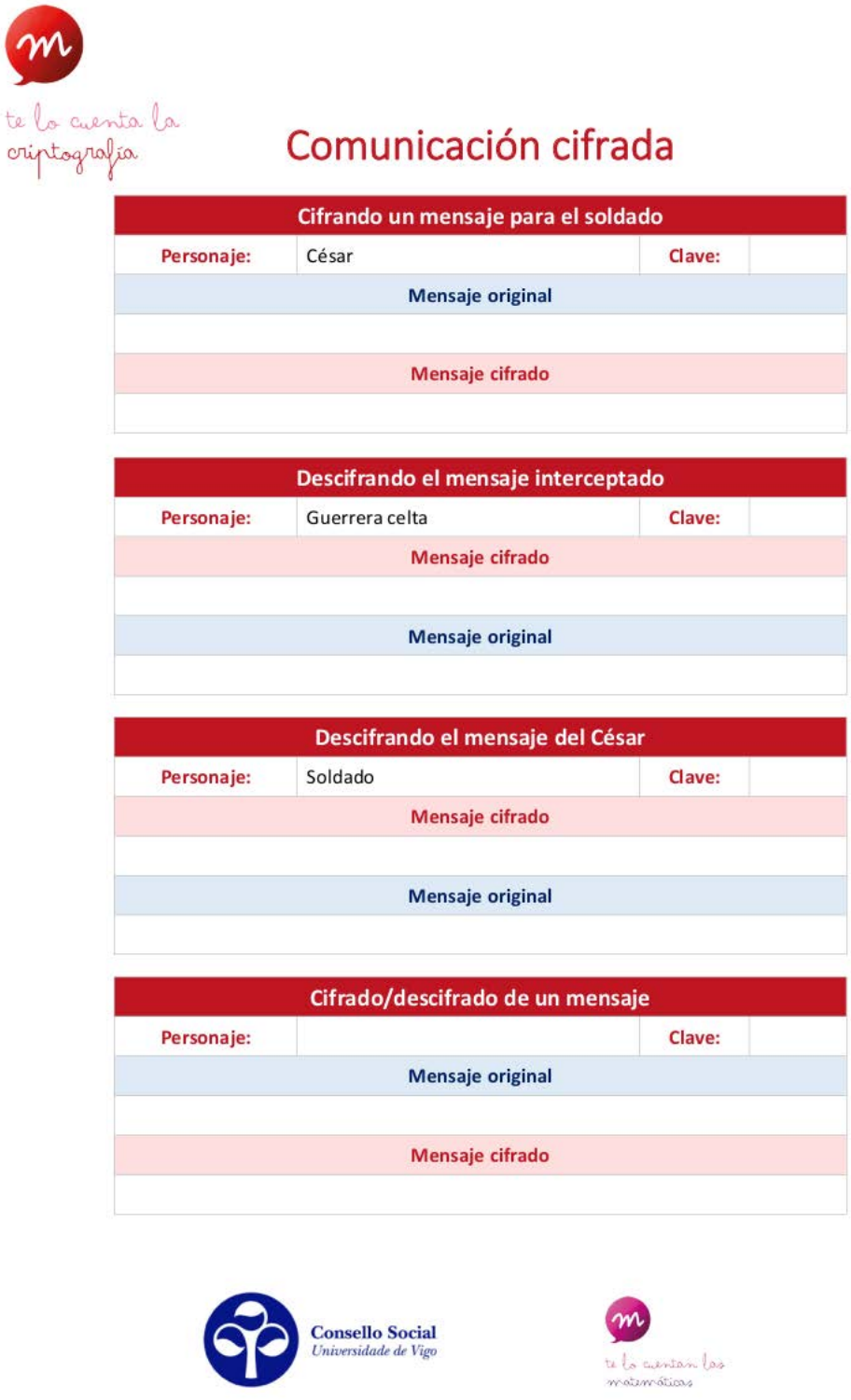
Material específico



Nota. Elaboración propia.

Figura 7

Ficha “Comunicación cifrada”



Comunicación cifrada

Cifrando un mensaje para el soldado			
Personaje:	César	Clave:	
Mensaje original			
Mensaje cifrado			

Descifrando el mensaje interceptado			
Personaje:	Guerrera celta	Clave:	
Mensaje cifrado			
Mensaje original			

Descifrando el mensaje del César			
Personaje:	Soldado	Clave:	
Mensaje cifrado			
Mensaje original			

Cifrado/descifrado de un mensaje			
Personaje:		Clave:	
Mensaje original			
Mensaje cifrado			

Nota. Elaboración propia.

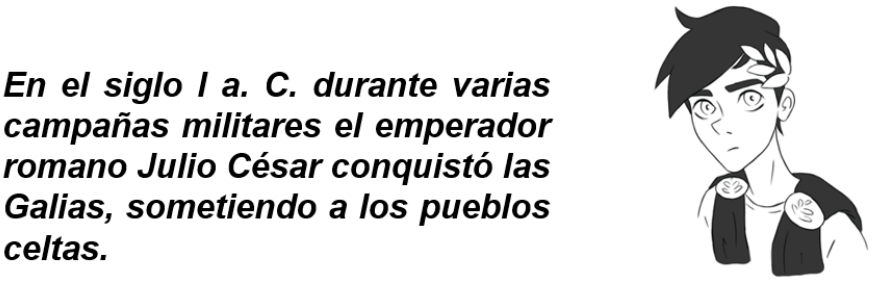
2.3. Desarrollo de la sesión

Las sesiones están pensadas para una duración aproximada de hora y media. En este caso, la actividad estará dividida en cuatro partes diferenciadas, de duración variable en función del tiempo que cada grupo precise consumir.

Primera parte: el origen de la clave César

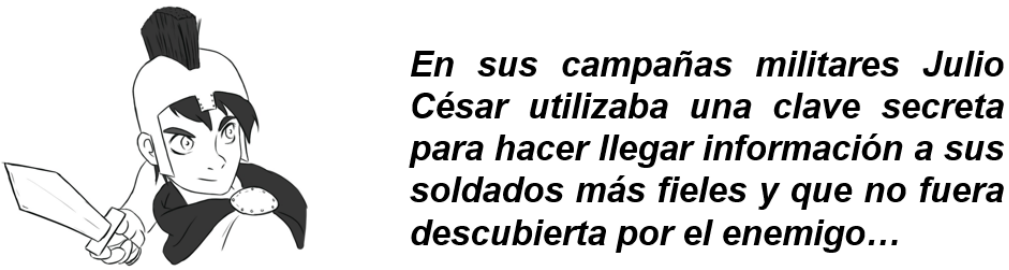
La sesión comenzaría explicando brevemente el origen del cifrado César a través de una historia. Explicaremos que, en el siglo I a. C., durante varias campañas militares el emperador romano Julio César conquistó las Galias, sometiendo a los pueblos celtas (Diapositiva 2).

Figura 8
Contenido de la Diapositiva 2



En sus campañas militares Julio César utilizaba una clave secreta para hacer llegar información a sus soldados más fieles y que no fuera descubierta por el enemigo (Diapositiva 3).

Figura 9
Contenido de la Diapositiva 3



Los guerreros y guerreras celtas capturaban a los mensajeros e intentaban descifrar los mensajes secretos, pero no siempre lo conseguían y con el paso del tiempo el Imperio Romano se extendió hasta *Finis Terrae*, Asia y el norte de África (Diapositivas 4 y 5).

Figura 10

Contenido de la Diapositiva 4

Los guerreros y guerreras celtas capturaban a los mensajeros e intentaban descifrar los mensajes secretos, pero no siempre lo conseguían.

En esta breve introducción se debe presentar y destacar sobre todo el protagonismo de tres personajes: el César, que es el emisor del mensaje; el enemigo que lo intercepta, que podemos identificar con una guerrera celta; y el receptor, que podría ser un soldado romano. Esto será importante para el juego de roles que se propondrá en la tercera parte de la sesión.

Figura 11

Personajes con los que identificamos los roles de la comunicación cifrada

Nota. Elaboración propia. Autora: María Ferreiro Subrido

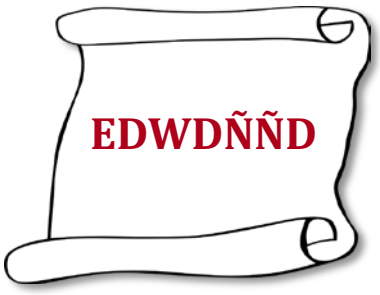
Con esta primera parte pretendemos, por un lado motivar al alumnado a través de un sistema de *storytelling* e introducir al alumnado en las comunicaciones cifradas presentando los tres roles a través de tres personajes, para que les resulten más sencillos de identificar.

Segunda parte: ejemplo de cifrado y descifrado

Comenzaremos esta parte a través de la presentación de un mensaje interceptado por la guerrera celta. Los celtas habían descubierto, después de interceptar el mismo mensaje en numerosas ocasiones, que este era enviado por Julio César cuando ordenaba comenzar un ataque (Diapositiva 6).

Figura 12

Mensaje del César cuando ordenaba comenzar un ataque



Le preguntaremos al grupo si entienden lo que el César quiere decir con el mensaje y les invitaremos a que intenten descubrir qué puede significar. Les podemos preguntar si les parece otro idioma o si se les ocurre alguna idea de cómo ha podido cifrar el César su mensaje. Poco a poco los iremos dirigiendo, aunque puede que ya lo sugieran ellos a través de las múltiples preguntas, hacia la idea de que es una palabra en la que se han cambiado las letras de la original por otras siguiendo un patrón.

Una vez llegada a esa conclusión a través del debate guiado, podremos pasar a fijarnos en las letras de la palabra:

- Es particularmente llamativo que tenga dos letras iguales seguidas ÑÑ. ¿Qué tipo de letras en español suelen ir seguidas? Principalmente la letra l y la letra r.
- En función de su posición en la palabra, ¿cuáles creemos que son las vocales? Deberían ser las D.

Haciendo algunas pruebas con las letras r y l y las cinco vocales, y teniendo en cuenta el momento en el que el César usa este mensaje, podemos guiarlos hasta llegar a la conclusión de que la palabra de la que proviene este mensaje es “BATALLA” (Diapositiva 7).

Figura 13

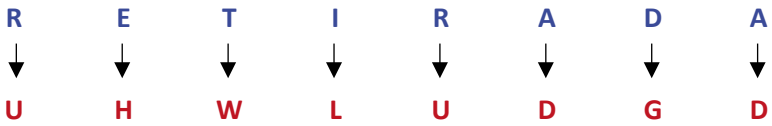
Cifrado de la palabra “batalla” con Clave César

B → E
A → D
T → W
A → D
L → Ñ
L → Ñ
A → D

De aquí deduciremos finalmente cómo funciona el cifrado César: cambiando cada letra del mensaje original por la que está 3 posiciones después en el abecedario. Para que comprendan cómo funciona este método y se familiaricen con él se procederá a hacer un par de ejemplos cortos en la pizarra. Letra a letra iremos recitando en alto el abecedario desde la letra a cifrar hasta 3 letras posteriores, sustituyéndola de esta forma por la correspondiente y obteniendo finalmente el mensaje cifrado.

Propondremos en primer lugar cifrar la palabra “RETIRADA”, por ejemplo. Al ser un ejemplo corto bastará con ir contando letra a letra, hasta la situada 3 lugares después. Obtendremos así:

Figura 14
Cifrado de la palabra “retirada” con Clave César



Inmediatamente después intentaremos realizar el proceso inverso, descifrar “JDPDORV”. Comprobaremos que nos resulta más el descifrado, ya que vamos en el orden inverso en el que conocemos el abecedario. De esta forma será más sencillo recuperar de la palabra “JDPDORV”, el mensaje original: “GANAMOS”.

Mostraremos entonces la Tabla 1 (Diapositiva 9) y explicaremos su contenido: en ella tenemos en la primera fila en azul el alfabeto y en la segunda fila la letra correspondiente en el cifrado César de cada una. De esta forma para cifrar pasaremos de las letras azules a las rojas (de arriba abajo) y para hacer el proceso inverso podremos pasar de las letras rojas a las azules (de abajo arriba).

En esta parte de la sesión aspiramos a que comprendan el funcionamiento del cifrado César. Se deberá hacer hincapié en el concepto de clave de un sistema de cifrado, explicando que en este caso la clave es el número 3 y significa el número de puestos que se desplazan las letras del abecedario.

Además, es recomendable comenzar a identificar colores distintos con los mensajes cifrado y descifrado desde el ejemplo en la pizarra. Por ejemplo, escribiremos el mensaje original en azul y el mensaje cifrado en rojo. La intención es que los participantes identifiquen los mensajes con dicho color para facilitar la comprensión del proceso y evitar confusiones entre cifrado y descifrado.

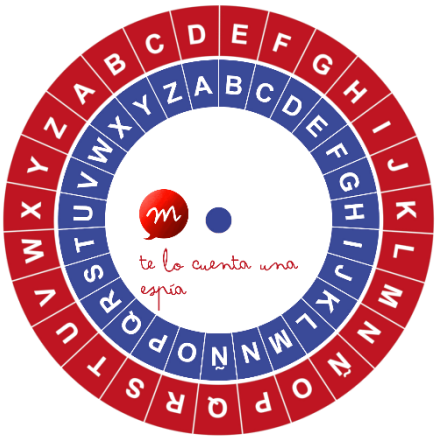
Tercera parte: construcción de la máquina de cifrado y juego de roles

Comenzaremos construyendo la máquina de cifrado. Cada alumno tendrá una ficha con dos discos con abecedarios inscritos para recortar, uno de color rojo y otro azul, y un encuadernador. Deberán unir ambos círculos mediante el encuadernador permitiendo que giren uno sobre el otro.

Una vez construida la máquina será importante recordarles que el cifrado César utiliza como clave el número 3, es decir desplaza el abecedario 3 posiciones. ¿Cómo deben entonces colocar el disco para cifrar y descifrar? Una vez lo hayan descubierto, deberán colocar los discos de forma que la A azul (pues el azul se correspondía con el mensaje original) coincida con la D roja, como se indica en la imagen inferior (Diapositiva 10).

Figura 15

Máquina de cifrado en posición de cifrado y descifrado con clave 3



Procederemos entonces a realizar el juego de roles (Diapositiva 11). Distribuidos en grupos de tres se repartirán los tres roles de la comunicación cifrada: César, que será el emisor; guerrera celta, que será el enemigo; y el soldado del César, que será el receptor. A partir de este momento deberán comenzar a hacer uso de la ficha "Comunicación cifrada" (Figura 7).

El César de cada grupo escogerá un mensaje y procederá a cifrarlo, comprobando que con la máquina es más rápido que haciéndolo letra a letra, ya que ésta le enseña la correspondencia al instante una vez esté correctamente colocada. Deberá escribir el resultado en la tabla de la ficha:

Tabla 2

Tabla para ser cubierta por el César del grupo

Cifrando un mensaje para el soldado			
Personaje:	César	**Clave:**	
Mensaje original			
Mensaje cifrado			

A continuación, lo enviará a su soldado dictando el mensaje en alto. Este deberá transcribirlo en la tabla correspondiente de la ficha:

Tabla 3

Tabla para ser cubierta por el soldado del grupo

Descifrando el mensaje del César			
Personaje:	Soldado	**Clave:**	
Mensaje cifrado			
Mensaje original			

La guerrera celta, que permanecerá atenta escuchando, lo interceptará y copiará para descifrarlo al igual que el soldado receptor.

Tabla 4

Tabla para ser cubierta por la guerrera del grupo

Descifrando el mensaje interceptado			
Personaje:	Guerrera celta	**Clave:**	
Mensaje cifrado			
Mensaje original			

¿Quién conseguirá llevarse la ventaja en la batalla: los romanos o los celtas? Ya que tanto el soldado como la guerrera celta deben realizar el mismo descifrado, el reto del juego consistirá en comprobar quién de los dos lo consigue más rápidamente: la guerrera, de forma que los celtas puedan evitar el ataque; o el soldado romano, lo que permitirá al ejército romano comenzar el ataque y pillar a los celtas desprevenidos.

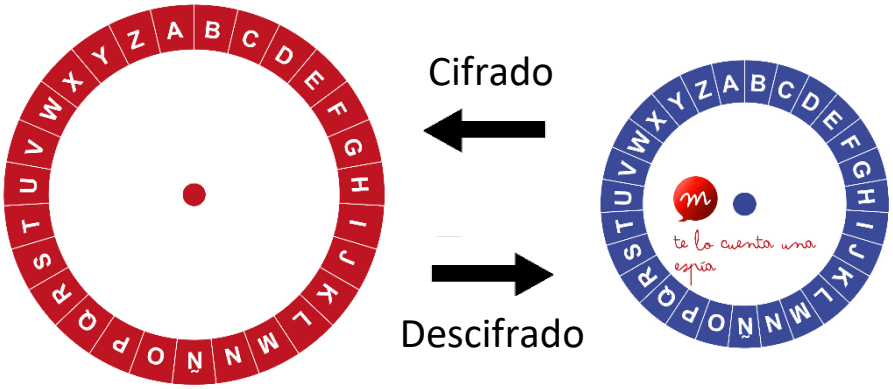
Siempre que el tiempo programado para la sesión lo permita, los grupos que completen el proceso podrán cambiar de rol dentro del propio grupo con la intención de que todos experimenten la función de cada personaje. Para ello podrán utilizar las restantes tablas de la ficha, ya que en el primer juego cada uno solo ha utilizado la del rol correspondiente.

Es importante prestar especial atención para evitar la confusión entre cifrado y descifrado cuando se hace uso de los discos, ya que sustituir las letras del disco externo por las del interno es el proceso inverso a sustituir las letras del interno por las del externo. Es decir, uno de estos procesos cifra mientras que el otro descifra.

En la práctica daría igual cuál se escoge como cifrado y cuál como descifrado, siempre que se mantenga durante todo el proceso. No obstante, en este caso conviene establecerlo previamente para evitar confusiones.

Para ello hemos identificado desde el inicio los colores con los mensajes cifrado y descifrado, tanto en el ejemplo efectuado en la pizarra en la primera parte de la sesión como en las fichas entregadas para construir la máquina (cada disco tendrá las casillas de un color distinto). Recordemos que en nuestro caso hemos elegido que el mensaje original en azul y el mensaje cifrado sea rojo.

Figura 16
Código de colores para el cifrado y descifrado



Al usar la máquina, las casillas del círculo exterior serán rojas y las del interior azules. De esta forma, si pasamos de azul a rojo (del disco interior al exterior) estaremos cifrando y si pasamos de rojo a azul (del exterior al interior) descifrando.

Mantendremos a su vez este código de colores en el juego de roles. El emisor escribirá su mensaje original en azul y el cifrado (que será el que dicte de viva voz a sus compañeros) en rojo. La enemiga celta interceptará el mensaje, lo copiará en rojo y tendrá que pasar de las letras rojas de la máquina de descifrado a las azules para obtener el original. De la misma forma tendrá que actuar simultáneamente el receptor.

De esta forma concluye la tercera parte, que pretende que el alumnado cifre y descifre autónomamente a través de la máquina de cifrado. Así, de forma manipulativa, se irá afianzando el aprendizaje sobre el cifrado César.

Cuarta parte: para profundizar en los cifrados de sustitución

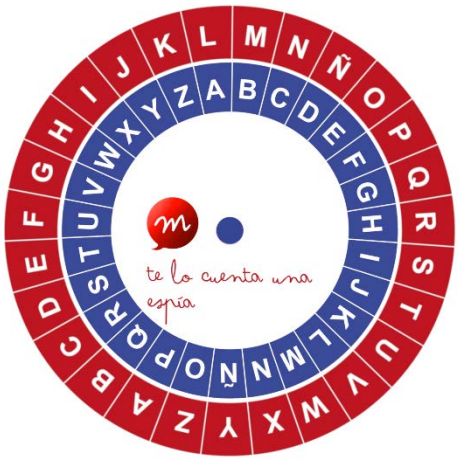
En esta cuarta parte les propondremos que cambien la clave (Diapositiva 12). Es decir, les pediremos que ejecuten nuevamente el juego de roles, pero esta vez el César del grupo podrá elegir otro desplazamiento distinto de 3 (clave César). Una vez construida la máquina es posible realizar otros desplazamientos cambiando la posición de un disco respecto al otro, es decir, girando los discos hasta otra posición distinta de la de la Figura 15.

En este caso habría que advertirles que el emisor tendrá que informar a su receptor del cambio de clave, para que éste pueda descifrar correctamente el mensaje. Se les explicaría que, mirando por qué letra se está sustituyendo la A y contando cuantas posiciones separan ambas letras, podrán comunicarle al receptor el número de desplazamiento escogido (distinto de 3).

Por ejemplo, si el César coloca el disco en la posición de la siguiente figura estaría mandando la A original a la letra L:

Figura 17

Máquina de cifrado en posición de cifrado y descifrado con clave 11



Por tanto, la clave de este cifrado de sustitución sería 11, ya que la L está 11 posiciones después en el abecedario que la A.

El interceptor del grupo, a su vez, deberá estar atento al cambio de clave e interceptar el nuevo número de desplazamiento. Esto le permitirá descifrar el mensaje interceptado correctamente. Como sabemos que todas las letras se desplazarán lo mismo, bastará con que tanto interceptor como receptor recoloquen sus círculos desplazando las letras el número indicado por el César.

Para registrar los mensajes enviados y recibidos cuentan con la última tabla de la ficha, que deberán completar y utilizar en función de su rol en el juego.

Tabla 5

Tabla para ser cubierta en el proceso de cifrado y descifrado con otra clave

Cifrado/descifrado de un mensaje			
Personaje:		**Clave:**	
Mensaje original			
Mensaje cifrado			

En esta última parte se busca que los participantes creen sus propios cifrados de sustitución a través de las distintas claves. Además, se añade un punto de dificultad ya que la tabla a completar es genérica y cada uno de ellos tendrá que ser consciente de proceso asociado a su rol. Esto ayudará a que se afiance su aprendizaje sobre los distintos aspectos a tener en cuenta en las comunicaciones cifradas.

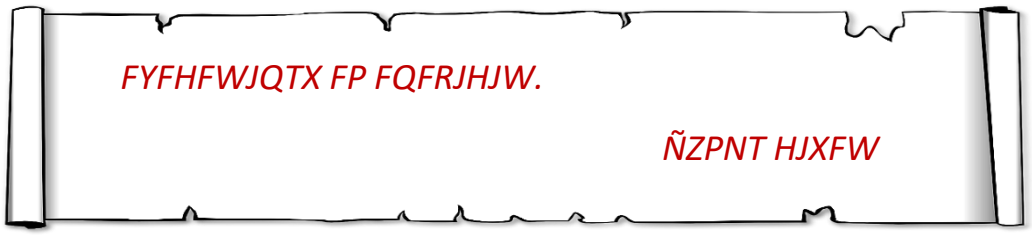
Reto propuesto: en busca de la clave.

En caso de haber podido realizar la cuarta parte, donde han cambiado la clave para obtener un nuevo cifrado de sustitución distinto al del César, se les propondrá el siguiente reto para que realicen voluntariamente fuera de la sesión.

Esta actividad consistirá en un mensaje cifrado y una pista: una de las palabras del mensaje. En este caso todos tomarán el rol de enemigo que ha interceptado un mensaje y, por intuición, conocen alguna de las palabras que lo conforman. El objetivo es que descubran con que clave se ha cifrado dicho mensaje y descifren el mensaje completo.

El mensaje del César interceptado es el de la Figura 18 (Diapositiva 13) y las palabras conocidas son las últimas, ya que suponemos que es la firma: Julio César.

Figura 18
Mensaje desconocido



Para descubrir la clave numérica solo tendrán que contar cuantas letras van desde una de las letras de las palabras conocidas a la correspondiente cifrada: si la J pasa a ser Ñ, esta letra es desplazada 5 posiciones. Luego la clave será 5, pues todas las letras se desplazan lo mismo.

Para descifrar el mensaje simplemente tendrán que situar en su máquina de cifrado una de las letras de las palabras originales conocidas (por ejemplo, la J de Julio) debajo de la que corresponde en el mensaje cifrado (en el caso anterior Ñ). Es decir, deberían colocar la J azul bajo la Ñ roja. Sin mover la máquina podrán comprobar con el resto de las letras de "Julio César" que efectivamente están descifrando con la clave correcta y coincide con la firma. A partir de aquí ya podrán descifrar el resto de mensaje: "atacaremos al amanecer".

3. Taller tecnológico *Te lo cuenta una espía*

3.1. Contenidos a tratar

Los algoritmos

El taller tecnológico asociado a *Te lo cuenta una espía* se centrará en los algoritmos, concepto que está a la orden del día y del cual cada vez es más habitual escuchar hablar en los medios de comunicación. Un ***algoritmo*** no es más que un conjunto de instrucciones bien definidas, ordenadas y finitas que nos permite resolver un problema obteniendo siempre un resultado determinado.

Podríamos decir que un algoritmo es una "receta matemática" que cumple las siguientes condiciones:

- Las instrucciones están **perfectamente ordenadas** y el cambio de este orden puede provocar el fallo del algoritmo. Por ejemplo, en una receta de cocina en muchas ocasiones no importa en que orden se mezclan ciertos ingredientes, pero en un algoritmo debe estar perfectamente definido.
- Las **instrucciones** incluidas en el algoritmo **no dejan lugar a dudas**. De nuevo, en una receta de cocina es habitual que se indique "echar una pizca de sal", pero una pizca de una persona puede ser una cantidad distinta que una pizca de otra distinta. Esto no puede ocurrir en un algoritmo, las instrucciones tienen que ser lo suficientemente claras para que cualquier persona que lo ejecute realice exactamente la misma acción.
- El **número** de instrucciones es **finito**, de forma que sabemos que una vez alcanzado el último paso obtendremos **siempre un resultado**. Esta es una de las características más importantes de los algoritmos, que siempre debemos alcanzar una solución.

Estas tres características convierten una receta en un algoritmo propiamente dicho: **instrucciones ordenadas, claras y finitas que siempre garantizan obtener un resultado**.

Es imprescindible fijarse en la última de ellas: siempre obtendremos un resultado final, pues podría ocurrir que un número finito de instrucciones ordenadas y claras no desemboquen en ninguna solución al problema inicial.

Diseño de algoritmos

Para el ***diseño de algoritmos matemáticas*** se sigue el siguiente procedimiento: cada conjunto de instrucciones, que constituye un posible de algoritmo, se introduce en un ordenador que lo ejecuta durante un determinado tiempo estipulado previamente. En caso de que éste no termine o no devuelva el resultado esperado en dicho tiempo, se descarta y se procede a su corrección. Es decir, ese conjunto de reglas no se considerará un algoritmo propiamente.

Como ya casi hemos avanzado, los aparatos electrónicos más comunes en nuestro día a día funcionan a base de algoritmos: las calculadoras, los ordenadores, los móviles… Estudiar a fondo qué es un algoritmo permite dar respuesta a una de las preguntas más repetida por el alumnado: ¿por qué tenemos que aprender matemáticas si ya tenemos calculadoras y ordenadores?

Los ordenadores o las calculadoras no saben por sí mismos realizar operaciones o resolver problemas. Somos las personas las que "enseñamos" a través de algoritmos a los ordenadores qué tienen que hacer para ayudarnos a resolver un determinado reto planteado.

Además, un ordenador o una calculadora siempre puede fallar y también puede que seamos nosotros los que introduzcamos mal los datos del problema. Por ello es importante que las personas aprendamos matemáticas, para que podamos "enseñar" a los ordenadores a resolver problemas, interpretar las soluciones devueltas y comprobar si son correctas.

Algoritmos para el cifrado de mensajes

El lenguaje de los ordenadores actuales es un lenguaje numérico, que tiene la ventaja de ser un lenguaje más universal y transversal. A la hora de trabajar en entornos informáticos de programación con mensajes compuestos por texto hay que tener en cuenta que puede ser necesario "enseñar" al ordenador cómo trabajar con ellos.

Es habitual que algunos de ellos, como es el caso del entorno con el que trabajaremos en el taller, no traigan incluido un alfabeto de base. Por tanto, en ocasiones será necesario traducir algunos procesos que nosotros realizamos de forma directa a un lenguaje que el ordenador pueda comprender.

Por ejemplo, en el caso de querer programar un algoritmo para el cifrado César, ¿cómo podemos conseguir que el ordenador sea capaz de trasladar cada letra de un mensaje tres posiciones en el alfabeto? En estos casos, la solución más habitual es identificar cada letra con un número y trabajar con el sistema numérico, siguiendo el siguiente esquema:

Figura 19

Posible esquema para trabajo con texto en algoritmos

En cada situación podemos elegir una identificación letra-número que más nos convenga, pero en general el alfabeto se introduce en el ordenador como una lista y se identifica cada elemento con su posición en dicha lista. En el cifrado César, dado que la información que necesitamos utilizar de cada letra es precisamente su posición en el alfabeto, será la más conveniente: la A será el 1, la B el 2 y así sucesivamente.

La transformación que llevamos a cabo en el cifrado César es "desplazar hacia delante tres posiciones", es decir, pensándolo con números sería sumar 3 (la clave César) a la posición

original de la letra. Por tanto, el proceso que el ordenador debería realizar para cifrar una A, por ejemplo, sería:

Figura 20
Esquema para cifrado César letra a letra

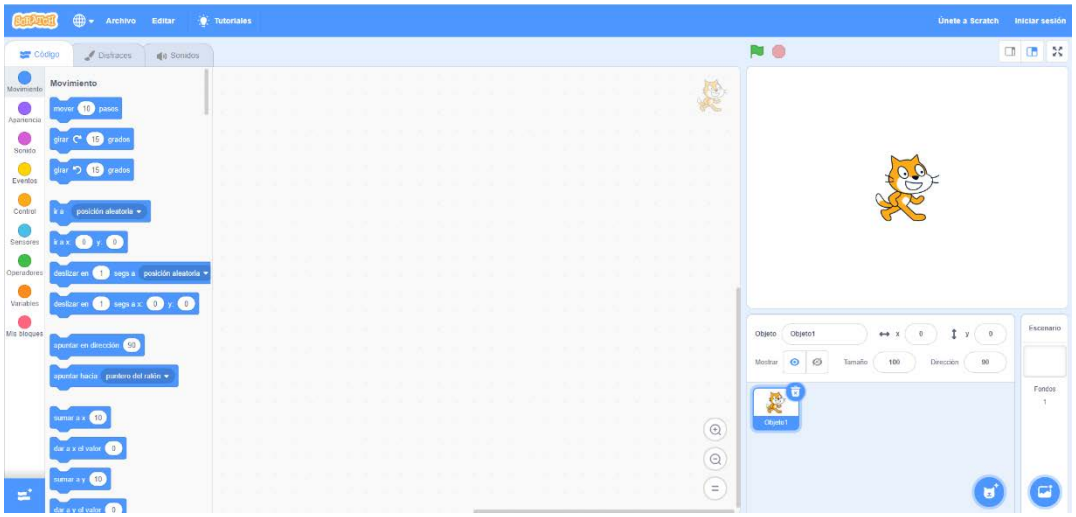
En este sentido, trasladar los procesos al lenguaje numérico tiene diversas ventajas. Por una parte, dotar a los entornos informáticos de todos los posibles alfabetos a utilizar podría suponer un consumo de memoria innecesario. Por otro lado, al ser el lenguaje numérico un lenguaje universal, este nos permite trabajar con cualquier tipo de alfabeto, que ya exista o que sea inventado. Para cifrar y descifrar con nuestro alfabeto lo único que debemos hacer es crear una lista ordenada e introducirla en el ordenador, trabajando con la identificación: elemento del alfabeto - posición en la lista.

3.2. Actividades previas

Dado que en este taller se hará uso de Scratch, lenguaje de programación de uso libre diseñado precisamente para un primer acercamiento a la programación, es conveniente que el alumnado participante se haya familiarizado con el entorno previamente a la sesión.

En este vídeo se presenta una breve introducción en la que se presenta la interfaz, se explica cómo se cambia el idioma a español y se diseñan e implementan un par de pequeños programas: uno que permite girar el gato de Scratch (enlace) y otro que pregunta el nombre del interlocutor y saluda (enlace). En los enlaces se puede trabajar con estos pequeños programas: ejecutarlos, modificarlos, probarlos...

Figura 21
Entorno de trabajo de Scratch



El acceso es sencillo: entrando en la dirección web https://scratch.mit.edu y pulsando "Crear" accederemos al espacio de trabajo de Scratch. Este está dividido en tres secciones (Figura 22): a la izquierda, tenemos los bloques con los que construiremos los programas y que están agrupados en distintos bloques por colores; en la parte central tenemos un espacio donde colocaremos los bloques arrastrándolos y ordenándolos correctamente; y la parte derecha, en la que podremos probar el funcionamiento del programa y cambiar el diseño del personaje que utilizaremos.

Los bloques con los que crear los programas encajan como piezas de puzle. A través de estas formas se refleja la finalidad que tienen (de inicio, apilables, de cierre...) y como pueden encajarse unos con otros.

3.3. Material

El único material necesario antes de la sesión será el vídeo explicativo para familiarizarse con el entorno de Scratch, explicado en el epígrafe anterior.

El material para llevar a cabo el taller será simplemente un ordenador (o *tablet*) con acceso a Internet por cada participante y una serie de enlaces que se encuentran integrados en el siguiente epígrafe, denominados ENLACE 1, ENLACE 2 y ENLACE 3. Además, será conveniente que dispongan del material utilizado en el taller manipulativo: la máquina de cifrado y los mensajes que se hayan intercambiado.

3.4. Desarrollo de la sesión

La duración total prevista para la sesión es de hora y media. Los contenidos de esta se repartirán en tres partes, cuya duración será flexible en función de las necesidades de los participantes y la adaptación de estos Scratch.

Primera parte: primeros pasos con Scratch

Iniciaremos la sesión con una pregunta: ¿por qué funcionan los ordenadores, las calculadoras, los móviles...? A las posibles respuestas como por la electricidad, o con baterías... Les repreguntaremos: ¿cómo saben hacer tan cosas? ¿cómo son tan listos? ¿aprenden como nosotros? (Diapositiva 2).

Pasaremos entonces a explicar brevemente el concepto de algoritmo y las tres condiciones que debe cumplir una sucesión de instrucciones para considerarse algoritmo: estar ordenadas, no dejar lugar a dudas y ser finitas dándonos un resultado final (Diapositiva 3).

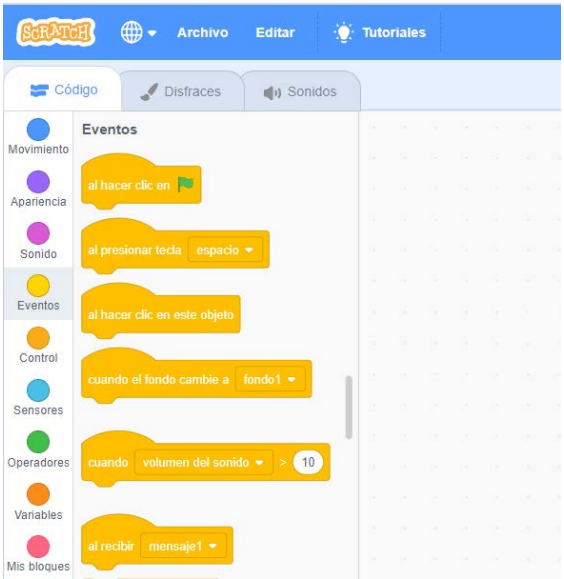
Pasaremos a continuación a poner ejemplos diversos de dónde podemos encontrar algoritmos en nuestro día a día (Diapositiva 4): en los semáforos, el estudio de epidemias, en el pilotaje de aviones, en el diseño de rutas, en la medicina, para realizar cálculos...

Además, conviene explicar e insistir en que para diseñar un algoritmo el primer paso es reflexionar sobre qué datos necesitaremos aportar e introducir para obtener el resultado. El segundo paso es pensar qué camino tendrá que seguir el ejecutor del algoritmo, en nuestro caso el ordenador, para obtener el resultado deseado. Para finalizar deberemos plantearnos de qué forma puede el ordenador devolvernos ese resultado (Diapositiva 5). Podemos escribir estos pasos en una pizarra, de forma que queden visibles para el resto de la sesión y nos ayuden a la hora de diseñar algoritmos.

A continuación, se les presentará Scratch (Diapositiva 6) y se les propondrá que diseñen un pequeño programa que debe pedir dos números y devolver su suma (Diapositiva 7). El docente puede consultar el programa ya completo en este enlace, pero no se lo proporcionaremos al alumnado, sino que iremos acompañándolos en el proceso de creación del algoritmo. Llevaremos a cabo el diseño del programa poco a poco, comprobando su funcionamiento mediante ensayo y error, hasta dar con la formulación correcta definitiva.

- En primer lugar nos preguntaremos **cómo iniciar el programa**. Para ver qué posibilidades tenemos para debemos ir al conjunto de bloques de color amarillo "Eventos" de la izquierda.

Figura 22
Bloques de inicio



Los bloques de inicio se reconocen porque tienen una parte redondeada por encima diferente a la que presentan por abajo. Esto ocurre porque al ser bloques de inicio no se les podrá colocar ningún bloque previamente, todos tendrán que colocarse a partir de este. Como vemos hay diversas formas de hacer que el programa se ponga en

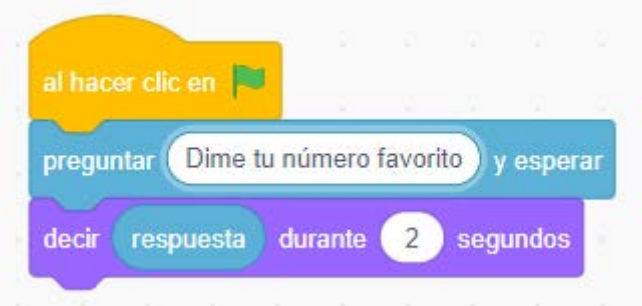
marcha: pulsando el botón de la bandera verde de la parte derecha, tocando una tecla, etc. Podemos escoger la opción de la bandera por ser una de las más sencillas, apta tanto para ordenador como para *tablet*.

- A continuación debemos preguntarnos **qué datos necesitamos introducir** para comenzar y **cómo vamos a proporcionárselos** a Scratch. Preguntaremos a la clase y lo primero que debemos intentar que descubran es que el programa debe pedir números, por lo cual vamos a necesitar realizar una interacción. Para ello deberemos consultar los bloques de color azul claro "Sensores". Dejando que busquen dentro de este bloque brevemente descubrirán que el bloque adecuado es el bloque "pregunta".

  Inmediatamente debajo de este se encuentra el bloque "respuesta". Estos bloques almacenan la respuesta que nosotros introducimos en relación con el bloque de pregunta.

- Colocaremos entonces debajo del bloque de inicio un bloque pregunta, colocando en la parte blanca del bloque la pregunta que queremos que el gato nos haga. Para comprobar el funcionamiento de esta parte del programa podemos colocar un bloque "decir" (situado en los bloques violetas "Apariencia") de forma que el gato reproduzca la respuesta a la pregunta. Este ejemplo quedaría de la siguiente forma:

Figura 23
Pequeño programa con bloques pregunta y bloques decir



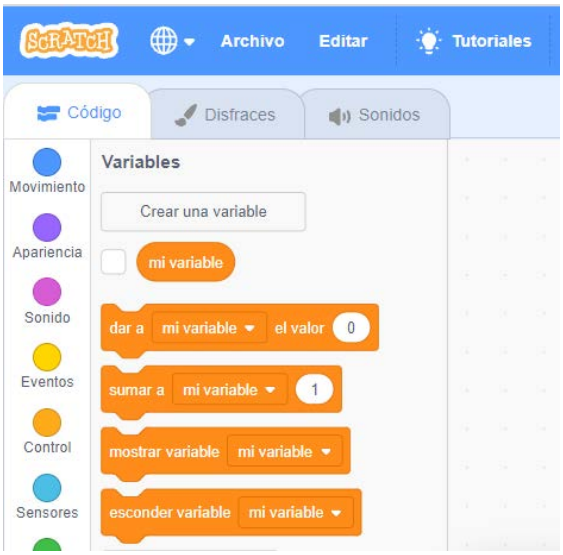
El resultado del programa sería el siguiente:

Figura 24
Ejecución del programa

- Ahora deberemos reflexionar sobre **cuántas respuestas** debemos almacenar. Llegaremos a la conclusión de que necesitamos dos preguntas y dos respuestas, de forma que el ordenador conozca por separado los dos números que luego tendrá que sumar. Como necesitamos sumar dos números y estos no caben a la vez en la "respuesta", necesitamos guardar nuestras respuestas en otras cajas digitales distintas, llamadas **variables.**

  Estas se encuentran en los bloques naranjas del mismo nombre y podemos crear tantas cajas-variables como necesitemos, en el botón blanco "Crear una variable". Es conveniente asociarles nombres que nos permitan recordar qué guardamos en cada una, por ejemplo Num1 y Num2.

Figura 25
Bloquea variable



- Una vez creadas deberemos guardar cada respuesta en cada una de ellas utilizando los bloques "dar a ... el valor ..." que podemos ver en la figura anterior. Hasta este momento, nuestro programa quedaría de la siguiente manera:

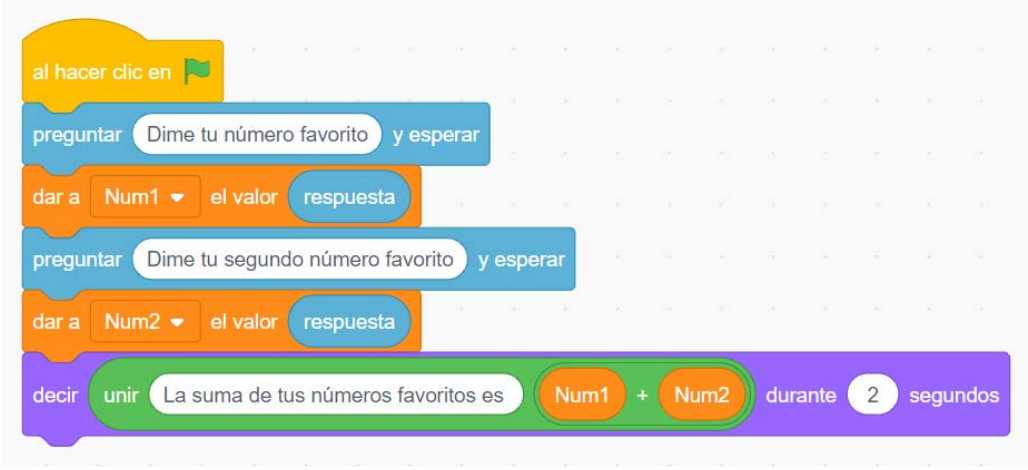
Figura 26
Proceso de guardado de datos en dos variables distintas

- Finalmente tendremos que pedirle al programa que nos devuelva la suma. Para realizar esta operación deberemos acudir a los bloques verdes “Operadores” y encontrar el de la suma. En los dos huecos deberemos colocar las variables Num1 y Num2 para que sus contenidos sumados. Podemos observar que efectivamente la forma de estos bloques coindice con la forma de las partes rellenables (blancas) del bloque suma, lo que significa que encajarán perfectamente.

Figura 27
Programa que suma dos números

- Si queremos añadir un texto a la respuesta, en la misma parte de operadores encontraremos un bloque “unir”. Con él, podremos construir la versión final del problema que se puede consultar en la Diapositiva 8.

Figura 28
Versión final del programa que suma dos números



Terminará esta parte comprobando que el diseño final del algoritmo funciona correctamente. Se explicará entonces la importancia de que las personas entiendan de matemáticas para, por un lado, evaluar si los resultados devueltos son correctos y, por otro, para interpretarlos.

Ya que estas actividades son individuales será importante prestar atención a la evolución de cada participante, pues es posible que algunos confundan los datos de entrada y de salida o no tengan claro en un primer momento como colocar los comandos ordenados para que el programa los ejecute, por ejemplo.

Con la primera parte del taller buscamos en primer lugar introducir al alumnado el concepto de algoritmo. Además, comenzaremos realizando un algoritmo sencillo que les permita vivenciar en primera persona el trabajo de un programador, realizando ensayo y error en la elaboración del diseño. Por último, la intención de programar el algoritmo suma es que se familiaricen con él para su uso en la siguiente parte.

Segunda parte: diseño de un algoritmo de cifrado César

La segunda parte será la parte central de la sesión. En ella los alumnos deberán recordar lo aprendido en el taller manipulativo y diseñar un pequeño programa de cifrado César: un algoritmo que reciba una letra y la desplace 3 posiciones en el alfabeto (Diapositiva 9).

Para ello, en primer lugar se hará un análisis en conjunto del problema a abordar. Explicado el problema a resolver, que ya conocen de la sesión manipulativa, se buscará que entre todos descubran los pasos que debe llevar a cabo el programa, siendo guiados por el responsable de la intervención educativa.

Lo primero sobre lo que deberán reflexionar es cómo solucionar el hecho de que el ordenador no es capaz de contar con letras. A través de un debate colectivo deberán llegar a la conclusión de que la mejor opción es identificar las letras con números, para posteriormente sumarles 3 para desplazarlas (Diapositiva 10). Les preguntaremos a continuación si valen números cualquiera, para acabar deduciendo que deberemos identificar las letras con sus posiciones en el abecedario.

Una vez decidido esto, se deberán diseñar los pasos que ha de seguir el programa. Así, se escribirá en un lugar visible para todos (en una pizarra o en un documento proyectado en una pared, por ejemplo) una lista de pasos elaborada en conjunto y que será similar a la siguiente (Diapositiva 11):

El algoritmo debe:

1. *Pedir una letra para cifrar.*
2. *Convertir dicha letra en un número (en la posición que ocupa en el alfabeto).*
3. *Sumar 3 a esa posición.*
4. *Devolver dicho número a letra (a la letra que ocupa esa posición en el alfabeto).*

Así, mover 3 posiciones se convertirá en sumar 3 posiciones y finalmente tendremos que volver a convertir ese número en la letra correspondiente, que será el resultado a devolver.

A continuación se indicará que entren en el ENLACE 1https://scratch.mit.edu/projects/445607597, en el que aparecerán distintos bloques desordenados en el espacio de trabajo, como se ve en la figura siguiente (Diapositiva 12):

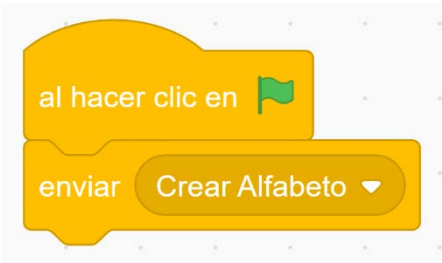
Figura 29
Puzle de bloques para construir el programa de cifrado letra a letra

Este entorno consta ya de un apartado "Escenario" con un pequeño código para generar el "Alfabeto", puesto que no es algo sencillo que se pueda abordar en el tiempo estipulado para la sesión. De esta forma el alumnado podrá trabajar en un entorno en el que el alfabeto es un objeto ya creado.

El reto que les propondremos es que recoloquen los bloques para construir el programa que previamente han diseñado. Antes de empezar, aclararemos la función de dos de los bloques que aún les son desconocidos:

- el bloque amarillo "enviar", que en este caso simplemente crea un alfabeto en Scratch,

  Figura 30
  Inicio creando un alfabeto en Scratch



- el bloque naranja más oscuro "# de elemento de ... en ...", que nos indica la posición del elemento que colocamos en el primer hueco dentro de la lista que elegimos en el desplegable. En este caso concreto, nos indicará la posición de la letra guardada en la caja-variable "Letra" dentro de la lista "Alfabeto".

  Figura 31
  Bloque para obtener la posición de la letra guardada en la variable Letra en el alfabeto

- el bloque naranja oscuro “elemento … de …”, nos permite extraer el elemento que se encuentra en una posición concreta de la lista que escogemos en el desplegable. Por ejemplo en la imagen posterior pedimos la letra del alfabeto que se encuentra en la posición guardada en “Posición” de la lista “Alfabeto”.

Figura 32

Bloque para obtener la letra del alfabeto que está guardada en la variable Posición

Se pretende que el alumnado intente comprender qué acción realiza cada uno de los bloques y los ordene en función del papel que desempeñan. Para comprobar si su programa funciona correctamente podrán utilizar sus máquinas de cifrado. El diseño obtenido debería ser el de la imagen posterior:

Figura 33

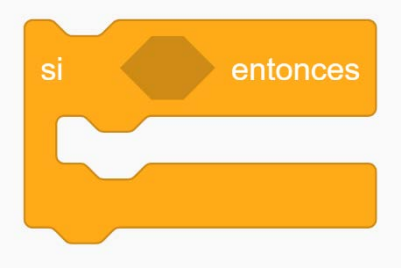
Primera versión del programa de cifrado César letra a letra

Propondremos entonces que prueben su programa cifrando letra a letra la frase “QUEREMOS PAZ” (Diapositiva 13). Construido así, el programa no devolverá resultados cuando la letra escogida sea X, Y o Z, puesto que en ese caso al sumar 3 los desplazamientos obtendremos las sumas 25+3, 26+3 y 27+3. Todos estos valores son superiores a 27 (que es la longitud del alfabeto) por lo que Scratch no encontrará una letra en esa posición de la lista “Alfabeto”.

Cuando alguno de los participantes encuentre el fallo (al intentar cifrar la letra Z de PAZ por ejemplo), se les pedirá que busquen la razón por la que el algoritmo no está correctamente implementado así (Diapositiva 14). Descubrirán, o se les explicará, entonces que es necesario introducir en el algoritmo inicial una condición diferente si la posición de la letra resulta mayor

que 27, por lo que tendrán que utilizar el bloque lógico “si”. Estos bloques se encuentran en el apartado “Control”.

Figura 34
Bloque lógico “si”

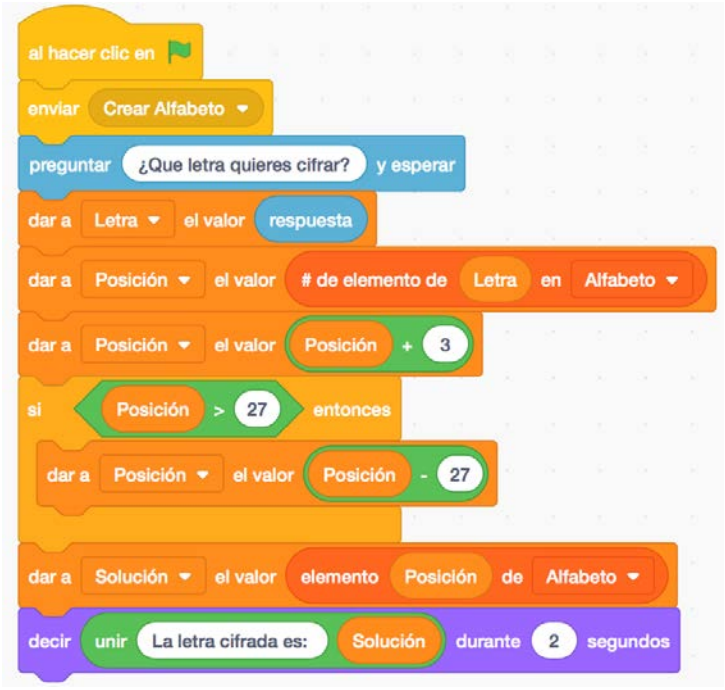


Llegados a este punto podemos proponerles que cojan un bloque de este tipo e intenten colocar un bloque variable después del “si”. Es importante explicarles que este bloque no encajará ya que tiene las esquinas redondeadas, mientras que el hueco que vemos tiene forma de hexágono. Esto ocurre porque el tipo de bloque que coloquemos ahí debe ser un bloque lógico que imponga una condición. Si esa condición se cumple entonces el programa realizará lo que coloquemos debajo.

¿Cuál debe ser la condición que impongamos en esta ocasión? Si la posición resultante del desplazamiento de la letra resulta mayor que 27, es decir si nos salimos del alfabeto, tenemos que volver a empezar por el principio del mismo. Pero volver a empezar en este caso es ir 27 letras para atrás, o lo que es lo mismo, restar 27 a la posición para volver a contar desde la A.

El resultado final se puede probar en el ENLACE 2 (Diapositiva 15):

Figura 35
Versión final del programa de cifrado César letra a letra



Bastará con añadir al programa previo (Figura 34) el bloque “si” después de calcular la nueva posición, para comprobar que si esta se sale del alfabeto se vuelve a contar desde el principio. Corregido el programa podrán probar a cifrar de nuevo las letras de PAZ para comprobar que este sí funciona correctamente.

En esta parte pondrán en práctica lo trabajado en la primera con el algoritmo de la suma. Deberán identificar y trabajar con diversos tipos de bloques, además de organizar las ideas para ordenar los bloques de forma que el programa tenga sentido y devuelva el resultado deseado.

En definitiva, de este modo habrán completado todos los pasos que debe dar un programador para el diseño de un algoritmo: análisis del problema, diseño del algoritmo, comprobación de errores, corrección de errores y comprobación final.

Tercera parte: algoritmo completo del cifrado César

Por último, y si el tiempo restante lo permite, se les presentará un programa de cifrado de César capaz de cifrar y descifrar frases completas (el presente en el ENLACE 3). Se les explicará que este nuevo programa realiza las mismas operaciones que el diseñado por ellos mismos letra a letra, pero en este caso para cualquier frase. Además, este programa tiene dos valores añadidos: no solo cifra sino que también descifra, que sería en proceso inverso al que ellos mismos han implementado; y también permite elegir la clave con la que se quiere cifrar y descifrar.

Figura 36

Apariencia del programa de cifrado César para palabras y frases

Este algoritmo de cifrado más completo comienza cuando accionamos uno de los botones de cifra o descifra que se observan en la figura anterior. Acto seguido el personaje de Scratch nos pregunta que clave queremos utilizar, para posteriormente solicitar el mensaje a cifrar o descifrar.

Se les propondrá que comprueben el buen funcionamiento de este nuevo algoritmo utilizando los mensajes cifrados y descifrados en la sesión manipulativa. En caso de que el tiempo sea suficiente y no haya sido posible proponerlo en la sesión manipulativa, el reto descrito en la

sesión manipulativa podrá ser propuesto en este momento con el objetivo de que descubran la clave y descifren el mensaje con el programa antes mencionado (Diapositiva 16).

Reto propuesto: mensaje de Julio César

El objetivo del taller tecnológico es completar las tres partes descritas previamente. Para los casos en los que el tiempo lo permita o algunos grupos terminen más rápido que otros de realizar las actividades propuestas se les podrá proponer un nuevo reto. En caso de que no sea posible realizarlo en la sesión se les dejará propuesto.

Como Julio César se ha dado cuenta de que los celtas han descubierto qué clave utiliza, ha decidido cambiarla y comenzar a cifrar con otra distinta. Los celtas se han dado cuenta porque han interceptado este mensaje y al intentar descifrarlo con la clave César (con desplazamiento 3) no han obtenido el mensaje original, han obtenido otro mensaje sin sentido (Diapositiva 17).

Figura 37
Mensaje interceptado, cifrado con una nueva clave

Ayudándose del algoritmo completo del cifrado César (ENLACE 3) tendrán que intentar encontrar la clave utilizada y el mensaje originar enviado por el César.

El procedimiento a seguir será ir probando con distintas claves hasta que el programa les devuelva algún mensaje que sea legible. Podrán empezar simplemente con la primera palabra, para realizar las pruebas más rápido, e ir probando con distintas claves numéricas. Una vez que hayan sido capaces de descifrar esa palabra habrán encontrado la clave correcta, que es 5. Conociendo dicha clave solo tendrán que introducirla junto con el mensaje completo para obtener como respuesta: “aprender algoritmos es importante y divertido”.