

Computational Thinking Integration Guide for Secondary Education Teachers

Ejemplo scenario

Version F.01

August 2022

Comput

Computational Thinking at School

Erasmus+ KA201 Project: 2019-1-EL01-KA201-062883

Co-funded by the
Erasmus+ Programme
of the European Union



Ι Δ Ρ Υ Μ Α
Κ Ρ Α Τ Ι Κ Ω Ν
Υ Π Ο Τ Ρ Ο Φ Ι Ω Ν
IKY

Computational Thinking Integration Guide for Secondary Education Teachers

Version F.01

Published by University of the Aegean – Laboratory of Learning Technology and Educational Engineering as deliverable of the “Computational Thinking at School” - “CompuT”, Erasmus+ KA201 project - Project Code: 2019-1-EL01-KA201-062883.

Authors:

Fesakis George, Prantsoudi Stavroula, Mavroudi Elisavet,
Volika Stamatia, Kefalas Ioannis

Learning Scripts edited by:

*George Fesakis, Stavroula Prantsoudi, Elisavet Mavroudi, Konstantinos Zervas,
Ioannis Kefalas, Georgia Papamargariti, Alexandra Papamargariti, Evangelia
Stamatarou, Manuel Toro Casaucao, Kristine Feness, Monica Langeland, Sabine
Lauw, Borghild Marie Opdahl, & Trude Sætveit*

Learning Scripts Evaluations and Reflections by:

Anastasios Savas, Vasileios Kasapidis, Monica Langeland, Stavroula Prantsoudi,

August 2022

Computational Thinking Integration Guide for Secondary Education Teachers
Copyright © 2022 by University of the Aegean – LTEE Lab



This work is licensed under the Creative Commons Attribution-NonCommercial-ShareAlike License. To view a copy of this license, visit <https://creativecommons.org/licenses/by-nc-sa/3.0/>.

To cite this work:

Fesakis, G., Prantsoudi, S., Mavroudi, E., Volika, S., Kefalas, I. (2022). *Computational Thinking Integration Guide for Teachers* (5th ed.). Rhodes, Greece: University of the Aegean - LTEE Lab.

Disclaimer:

"The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein."

Comput

Computational Thinking at School

Partners:



Directorate of Secondary Education in Dodecanese



University of the Aegean, Laboratory of Learning Technology and Educational Engineering (LTEE), Rhodes, Greece



2° Upper Secondary School of Rhodes, "Kazoulleio", Rhodes, Greece



Secondary School of Gennadi, Rhodes, Greece



Secondary School of Zipari, Kos, Greece



CEP La Laguna, Tenerife, Spain



IES EL SOBRADILLO, Tenerife, Spain



Fyllingsdalen videregående skole, Bergen, Norway



Agrupamento de Escolas de São João da Talha, Lisbon, Portugal

Ejemplo situación de aprendizaje 1: *The history of computation automation*

Part A. Datos Generales																																	
A.1 Título:	<i>La Historia de la Automatización omputacional</i>																																
A.2 Autor(es/as):	<i>Kefalas Ioannis, Universidad del EGEO</i>																																
A.3 Resumen:	<i>En esta situación de aprendizaje, el alumnado viaja a través de la Historia de la Automatización Computacional. A lo largo de este viaje el alumnado podrá aprender acerca de las primeras máquinas utilizadas para hacer cálculos simples así como su antigüedad centrado en la calculadora mecánica de Pascal, la famosa Pascalina. El alumnado construirá una versión simplificada de la Pascalina y utilizarán la misma para desarrollar algunos cálculos. Esta situación de aprendizaje integra aspectos de la Historia, las Artes y las Ciencias de la Computación de manera creativa y educativa.</i>																																
A.4 Palabras Clave:	<i>Pascalina, Automatización Computacional e Historia de la Ciencia</i>																																
A.5 Versión:	<i>Borrador</i>																																
A.6 Fecha:	<i>29/10/2020</i>																																
A.7 Licencia de Copyright:	<i>Atribución de compartir por igual CC BY-SA</i>																																
Part B. Datos de aprendizaje																																	
B.1 Curso/s:	<i>1º- 2º ESO, edad 12-13 años</i>																																
B.2 Materia/s:	<i>Historia, Artes y Ciencias de la Computación</i>																																
B.3 Topic(s):	<i>Historias de la Automatización Computacional</i>																																
B.4 Dimensiones del Pensamiento Computacional:	<table border="1" style="width: 100%; border-collapse: collapse;"> <tbody> <tr><td>Pensamiento algorítmico (AL)</td><td style="text-align: center;">✓</td></tr> <tr><td>Abstracción (AB)</td><td style="text-align: center;">✓</td></tr> <tr><td>Generalización (GE)</td><td></td></tr> <tr><td>Razonamiento lógico (LR)</td><td style="text-align: center;">✓</td></tr> <tr><td>Coincidencia de patrones (PM)</td><td></td></tr> <tr><td>Descomposición de problemas(PD)</td><td style="text-align: center;">✓</td></tr> <tr><td>Traducción del problema (PT)</td><td></td></tr> <tr><td>Evaluación (EV)</td><td style="text-align: center;">✓</td></tr> <tr><td>Representación (RE)</td><td style="text-align: center;">✓</td></tr> <tr><td>Recopilación de datos (DC)</td><td></td></tr> <tr><td>Representación de datos (DR)</td><td></td></tr> <tr><td>Análisis de datos (DA)</td><td></td></tr> <tr><td>Modelaje (MO)</td><td style="text-align: center;">✓</td></tr> <tr><td>Simulación(SIM)</td><td style="text-align: center;">✓</td></tr> <tr><td>Automatización (AUT)</td><td style="text-align: center;">✓</td></tr> <tr><td>Secuenciación (SE)</td><td></td></tr> </tbody> </table>	Pensamiento algorítmico (AL)	✓	Abstracción (AB)	✓	Generalización (GE)		Razonamiento lógico (LR)	✓	Coincidencia de patrones (PM)		Descomposición de problemas(PD)	✓	Traducción del problema (PT)		Evaluación (EV)	✓	Representación (RE)	✓	Recopilación de datos (DC)		Representación de datos (DR)		Análisis de datos (DA)		Modelaje (MO)	✓	Simulación(SIM)	✓	Automatización (AUT)	✓	Secuenciación (SE)	
Pensamiento algorítmico (AL)	✓																																
Abstracción (AB)	✓																																
Generalización (GE)																																	
Razonamiento lógico (LR)	✓																																
Coincidencia de patrones (PM)																																	
Descomposición de problemas(PD)	✓																																
Traducción del problema (PT)																																	
Evaluación (EV)	✓																																
Representación (RE)	✓																																
Recopilación de datos (DC)																																	
Representación de datos (DR)																																	
Análisis de datos (DA)																																	
Modelaje (MO)	✓																																
Simulación(SIM)	✓																																
Automatización (AUT)	✓																																
Secuenciación (SE)																																	

	<table border="1"> <tr> <td>Testeo (TE)</td> <td>✓</td> </tr> <tr> <td>Entendimiento de las personas – (UP) /Inteligencia Artificial (AI)</td> <td></td> </tr> </table>	Testeo (TE)	✓	Entendimiento de las personas – (UP) /Inteligencia Artificial (AI)																																			
Testeo (TE)	✓																																						
Entendimiento de las personas – (UP) /Inteligencia Artificial (AI)																																							
B.5 Enfoques del Pensamiento Computacional :	<table border="1"> <tr> <td>Retoques, experimentación y juego</td> <td>✓</td> </tr> <tr> <td>Creación, diseño y experimentación</td> <td>✓</td> </tr> <tr> <td>Depuración, hallazgo y arreglo de errores</td> <td></td> </tr> <tr> <td>Perseverancia y seguir adelante</td> <td></td> </tr> <tr> <td>Colaboración y trabajo conjunto</td> <td>✓</td> </tr> </table>	Retoques, experimentación y juego	✓	Creación, diseño y experimentación	✓	Depuración, hallazgo y arreglo de errores		Perseverancia y seguir adelante		Colaboración y trabajo conjunto	✓																												
Retoques, experimentación y juego	✓																																						
Creación, diseño y experimentación	✓																																						
Depuración, hallazgo y arreglo de errores																																							
Perseverancia y seguir adelante																																							
Colaboración y trabajo conjunto	✓																																						
B.6 Contexto temático del proyecto de CompuT:	<table border="1"> <tr> <td>Robótica Educativa o Física Computacional</td> <td></td> </tr> <tr> <td rowspan="5">Proyecto de Ciencias computacionales</td> <td>Modelaje/ Simulación</td> <td>✓</td> </tr> <tr> <td>Modelaje Bifocal</td> <td></td> </tr> <tr> <td>Creación o uso de sensores</td> <td></td> </tr> <tr> <td>Matemáticaso Ciencias Computacionales</td> <td>✓</td> </tr> <tr> <td>Otros:....</td> <td></td> </tr> <tr> <td>Datos del proyecto de Ciencia</td> <td></td> </tr> <tr> <td>Historia de la Ciencia y la Tecnología</td> <td>✓</td> </tr> <tr> <td>Juegos Digitales, programas o aplicaciones móviles</td> <td></td> </tr> <tr> <td rowspan="5">Proyectos de Humanidades Digitales</td> <td>Cuentacuentos digital</td> <td></td> </tr> <tr> <td>Ficción Interactiva</td> <td></td> </tr> <tr> <td>Extracción de textos</td> <td></td> </tr> <tr> <td>Algoritmos de uso diario</td> <td></td> </tr> <tr> <td>Otros:....</td> <td></td> </tr> <tr> <td>Proyectos de Inteligencia Artificial</td> <td></td> </tr> <tr> <td>Enfoque de estudio - Proyectos de clase futuros</td> <td></td> </tr> <tr> <td>Experiencias desenchufadas o uso de manipulativos</td> <td>✓</td> </tr> <tr> <td>Otros:....</td> <td></td> </tr> </table>	Robótica Educativa o Física Computacional		Proyecto de Ciencias computacionales	Modelaje/ Simulación	✓	Modelaje Bifocal		Creación o uso de sensores		Matemáticaso Ciencias Computacionales	✓	Otros:....		Datos del proyecto de Ciencia		Historia de la Ciencia y la Tecnología	✓	Juegos Digitales, programas o aplicaciones móviles		Proyectos de Humanidades Digitales	Cuentacuentos digital		Ficción Interactiva		Extracción de textos		Algoritmos de uso diario		Otros:....		Proyectos de Inteligencia Artificial		Enfoque de estudio - Proyectos de clase futuros		Experiencias desenchufadas o uso de manipulativos	✓	Otros:....	
Robótica Educativa o Física Computacional																																							
Proyecto de Ciencias computacionales	Modelaje/ Simulación	✓																																					
	Modelaje Bifocal																																						
	Creación o uso de sensores																																						
	Matemáticaso Ciencias Computacionales	✓																																					
	Otros:....																																						
Datos del proyecto de Ciencia																																							
Historia de la Ciencia y la Tecnología	✓																																						
Juegos Digitales, programas o aplicaciones móviles																																							
Proyectos de Humanidades Digitales	Cuentacuentos digital																																						
	Ficción Interactiva																																						
	Extracción de textos																																						
	Algoritmos de uso diario																																						
	Otros:....																																						
Proyectos de Inteligencia Artificial																																							
Enfoque de estudio - Proyectos de clase futuros																																							
Experiencias desenchufadas o uso de manipulativos	✓																																						
Otros:....																																							
B.7 Propósito / Objetivo de la Situación de aprendizaje.	<p><i>Al realizar esta situación de aprendizaje, el alumnado habrá desarrollado conocimiento básico acerca de la evolución histórica de la automatización computacional así como se habrá familiarizado con los mecanismos de máquinas simples de computación. Además, el propósito de esta situación de aprendizaje es el de entender la función de una máquina de computación, como la Pascalina y construir su propia máquina convirtiéndose de esta manera en</i></p>																																						

	<i>ingenieros y científicos.</i>	
B.8 Productos de aprendizaje/ Logros¹:	<i>Téngase en cuenta como la situación de aprendizaje puede favorecer el desarrollo general de competencias y habilidades del S. XXI.</i>	
	B.8.1 Conocimiento (Saber)	<ul style="list-style-type: none"> • Reconocer algunos de los mecanismos conectados con la Historia de la Automatización Computacional, tales como la Pascalina. • Describir cómo funciona una máquina de cálculo (Pascalina)
	B.8.2 Habilidades (Saber hacer)	<ul style="list-style-type: none"> • Desarrollar habilidades de construcción mediante el montaje de su propia Pascalina.
	B.8.3 Actitudes-afectivo (Saber ser)	<ul style="list-style-type: none"> • Reconocimiento de la importancia de las máquinas para resolver problemas del día a día. • Reflexionar acerca de la evolución de la Ciencia y que lleva al uso de las dispositivos que utilizamos a día de hoy.
B.9 Competencias horizontales . Habilidades del S. XXI	<i>Esta propuesta didáctica crea las condiciones adecuadas para desarrollar habilidades del S. XXI tales como el pensamiento crítico, la resolución de problemas, la creatividad, la comunicación, la colaboración, la curiosidad, la iniciativa, la perseverancia y la adaptabilidad.</i>	
	B.9.1 Aprendizaje y habilidades de innovación:	<p><i>4C's: Colaboración, Comunicación, Pensamiento Crítico y Creatividad</i></p> <p><i>El alumnado tendrá que colaborar para construir su máquina comunicando, pensando de manera crítica y poniendo de manifiesto su creatividad.</i></p>
	B.9.2 Habilidades de alfabetización digital:	<i>Alfabetización informacional: El alumnado adquirirá conocimiento acerca de los primeros pasos de la revolución informacional.</i>
	B.9.3 Habilidades para la vida:	<p><i>Flexibilidad y adaptabilidad, interacción social y cultural transversal, productividad y responsabilidad y liderazgo.</i></p> <p><i>El alumando adaptará su modelo a sus necesidades y recursos, interactuando con sus compañeros, siendo productivos y responsables en el resultado.</i></p>
B.10 Métodos de	<i>La situación de aprendizaje incluye métodos de enseñanza moderna</i>	

¹ Para la formulación efectiva de aprendizaje instruccional el trabajo de Mager, quien alude a la definición del uso de acciones observables y criterios mensurables en el desempeño de la evaluación en condiciones específicas, Mager, F. (1975). "Preparing Instructional Objectives". (2nd ed.). Belmont, CA: Fearon. & Mager, F. (1997). "Preparing instructional objectives": Una herramienta Crítica en el desarrollo de la instrucción efectiva. "Atlanta: The Center for Effective Performance". Los verbos podrían seguir la taxonomía de Bloom, véase por ejemplo: <https://tips.uark.edu/blooms-taxonomy-verb-chart/>. Es importante utilizar procesos cognitivos de alto rango.. Anderson, L. W., & Krathwohl, D. R. (2001). "A taxonomy for learning, teaching, and assessing", Abridged Edition. Boston, MA: Allyn and Bacon

enseñanza modernos:	<p>tales como:</p> <p><i>Retoques, ya que el alumnado tendrá que armar una pascalina de cartón o cartulina.</i></p> <p><i>Aprendizaje colaborativo, ya que el alumnado deberá trabajar en equipo para completar la tarea.</i></p>		
B.11 Integración de Pensamiento Computacional en el Currículo:	<i>Esta situación de aprendizaje incluye una variedad de disciplinas tales como Historia, Arte y Ciencias Computacionales mezclada con muchas dimensiones del Pensamiento Computacional.</i>		
B.12 Relación con el Currículo y/ o estándares:	<i>Currículo Nacional Griego, Cursos 7 y 8, Currículo de las Ciencias de la Computación.</i>		
B.13. Conocimientos Previos:	<i>No requieren conocimientos previos.</i>		
B.14. Nivel de dificultad de la situación de aprendizaje:	<i>Intermedio</i>		
B.15. Escenario social de la situación de aprendizaje:	<i>El alumnado tendrá que trabajar en pequeños grupos para completar algunas de las actividades de esta situación de aprendizaje.</i>		
B.16 Lugar de la implementación didáctica:	<i>Clase o laboratorio de computación.</i>		
B.17 Duración:	<i>3 x 45' sesiones</i>		
B.18 Material educativo, recursos, instrumentos, herramientas y medios de comunicación y difusión:	B.18.1 "Software":		
	B.18.2 "Hardware":		
	B.18.3 Recursos en línea:	<i>Videos de YouTube, motores de búsqueda</i>	
	B.18.4 Material educativo convencional:	<i>Piezas de cartón o cartulina para la Pascalina, pegamento, clavos o sujetadores ("fasteners") de cabeza redonda.</i>	
Part C. Diseño de la Experiencia de aprendizaje			
C.1. Actividades- Acción- Argumento- Tabla de secuencia del guión gráfico:	Fase 1.	<i>La Historia de las máquinas de computación.</i>	
	Actividad/Tarea	Descripción/Procedimiento	Duración
	<i>A1.1 Ganar atención– Historia de la</i>	<i>El/ La docente muestra los primeros pasos de la computación y proyecta un</i>	<i>20'</i>

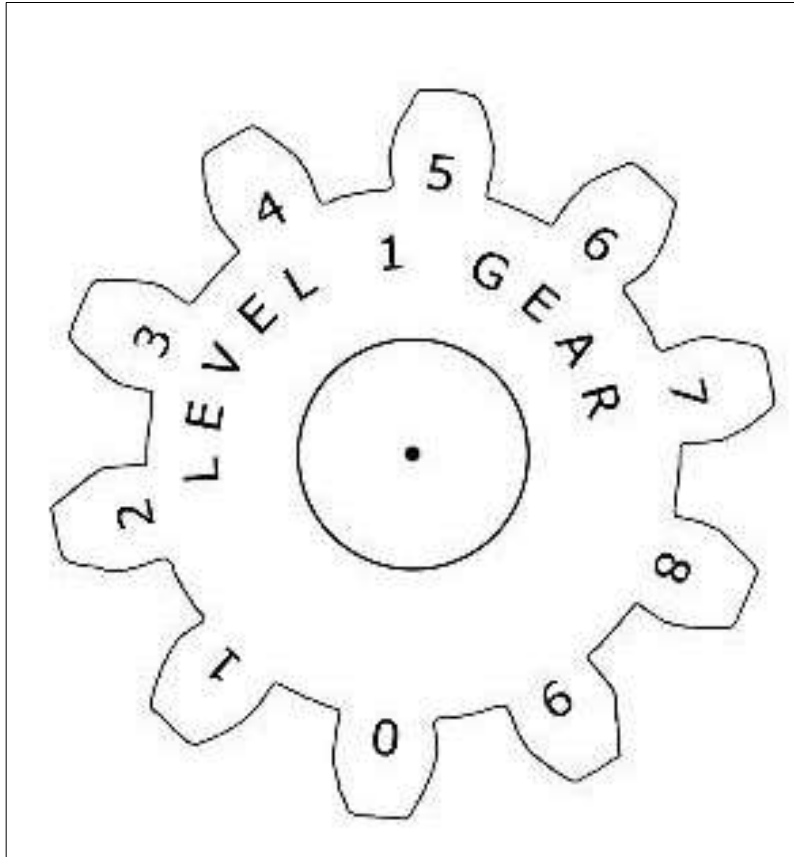
	<p>automatización de la computación.</p>	<p>video relacionado con esta temática para el alumnado https://www.youtube.com/watch?v=O5nskjZ_Gol</p> <p>Al alumnado se le requerirá suponer cual es el uso de lo que han visualizado en el vídeo.</p>	
	<p>A1.2 La introducción de la Pascalina</p>	<p>El/ La docente se centrará en la Pascalina incidiendo con el alumnado en que la Pascalina es un modelo de un mecanismo creado en 1642-44 por Pascal, este mecanismo es capaz de realizar sumas y restas simples tales como $98+6$ y $22-5$. El/ La docentes proyecta un vídeo y explica como funciona la Pascalina: https://www.youtube.com/watch?v=SeyMTzKYKqg&t=151s Se ha de señalar que esto fue un intento que se realizó para automatizar cálculos.</p>	<p>20'</p>
	<p>A1.3 Resumen y siguiente fase.</p>	<p>El/ la docente resume e informa al grupo clase de que en la siguiente fase se dividirán en grupos para construir sus propias Pascalinas de cartulina o cartón e intentarán usarlas para realizar algunas sumas y restas.</p>	<p>5'</p>
	<p>Fase 2.</p>	<p>Construyendo un modelo de Pascalina</p>	
	<p>Actividad/Tarea</p>	<p>Descripción/Procedimiento</p>	<p>Duración</p>
	<p>A2.1 Construye tu Pascalina.</p>	<p>El /la docente proyecta el siguiente vídeo y se discute con el alumnado acerca de cómo se podría construir una Pascalina:</p> <ul style="list-style-type: none"> • Pascaline DIY: https://youtu.be/KgPsTBwn0eM <p>Las diapositivas de la siguiente presentación también se podrían utilizar como por ejemplo la diapositiva #19. https://www.cs.cmu.edu/afs/cs/academic/class/15294-f14/lectures/pascaline/pascaline.pdf</p>	<p>45'</p>

		<p>Se repartirá al alumnado la hoja de trabajo 1 ("Worksheet 1"), papel, cartulina o cartón y clavos o sujetadores ("fasteners") de cabeza redonda para seguir los pasos de la hoja de trabajo 1 ("Worksheet 1") y construir su Pascalina en grupos.</p>	
	Fase 3.	Título de la fase (realizando cálculos con nuestro modelo de Pascalina)	
	A3.1 Comparar los modelos de Pascalina de los distintos grupos.	<p>Los grupos comparan sus modelos de Pascalina de cartulina o cartón para ver si se parecen o son idénticos. Se identifican y corrigen posibles errores de construcción.</p>	5'
	A3.2 Realización de cálculos con el modelo de Pascalina.	<p>El/ La docente comparte la hoja de trabajo 2 ("Worksheet 2") y pregunta al alumnado para que responda a algunas preguntas acerca de esta. El alumnado tendrá que efectuar algunos cálculos para comprobar si su Pascalina funciona correctamente y así luego contestar preguntas más generales que ahondan en la materia de estudio. Si queda algún tiempo restante, pueden darse número extra al alumnado para realizar sumas y restas con ellos.</p>	35'
	A3.3 Resumen y debate	<p>El/La docente pregunta al alumnado para evaluar el tiempo que les lleva realizar una operación usando la calculadora de Pascal. A través de un debate relevante se intentará destacar que el valor de cada invento está relacionado con el tiempo que tarda en realizar la acción.</p>	5'

C.2 Evaluación			
	C.2.1 Retroalimentación del alumnado y reflexión.	<i>El alumnado intentará sumar y restar diferentes números y evaluar su máquina.</i>	
C.3 Tarea de casa/ Trabajo con la familia	<i>No necesario.</i>		
<u>Parte D. Información para el profesorado</u>			
D.1 Adaptación-Modificaciones para la inclusión de todo el alumnado.	<i>Todo el alumnado puede desarrollar esta Situación de Aprendizaje</i>		
D.2 Extensión	<i>Creación de una Pascalina usando "LEGO": https://youtu.be/olfNFXJEZOA</i>		
D.3 Recursos	<i>Videos de YouTube, Search motores de búsqueda, Piezas de la Pascalina de Cartulina o Cartón, pegamento, clavos o sujetadores ("fasteners") de cabeza redonda.</i>		
D.4 Experiencia derivada de la implementación de la situación de aprendizaje			
D.5 Relaciones con otras situaciones de aprendizaje.			
D.6 Revisiones del profesorado			
D.7 Evaluación de la situación de aprendizaje	<i>[1=Very Bad – 5=Very Good]</i>		
D.8 Referencias			
<u>Parte E. Anexos</u>			
	<i>Worksheet 1 – Ensamblaje de la Pascalina</i>		
	<i>Worksheet 2 – La Pascalina en acción</i>		

Worksheet 1 - Ensamblaje de la Pascalina

Vas a construir una máquina para hacer cálculos llamada Pascalina. Utiliza el modelo facilitado justo debajo, copia y corta 5 engranajes y sigue los pasos para construir tu propia Pascalina. Pregunta a tu profesor o profesora si tienes dudas. ¡Buena suerte!



Siguiendo estos pasos, la pascalina se construye de derecha a izquierda:

Haz un nivel de engranaje 1:

1. Conecta un círculo con el engranaje utilizando un clavo para crear el nivel de engranaje 1.
2. Pega el nivel de engranaje 1 en el punto predefinido de la tabla que se ubica abajo a la derecha (Figura 1).
3. Haz un segundo nivel de engranaje 1 y pégalo en el punto que se ubica arriba a la derecha (Figura 2).

Haz un nivel de engranaje 2:

4. Primero haz un nivel de engranaje 1 y luego pégalo a un segundo círculo..
5. Pega el nivel de engranaje 2 en el punto que se ubica en abajo y en medio (Figura 3).
6. Haz un segundo nivel de engranaje 2 y pégalo en el punto que se ubica arriba a la izquierda (Figura 4).

Haz un nivel de engranaje 3:

7. Primero haz un nivel de engranaje 2 y luego pégalo a un tercer círculo.
8. Pega el nivel de engranaje 3 en el punto que se ubica abajo a la izquierda (Figura 5).

9. Dibuja tres punteros en la parte inferior de la Pascalina mostrando los engranajes más bajos (Figura 6).

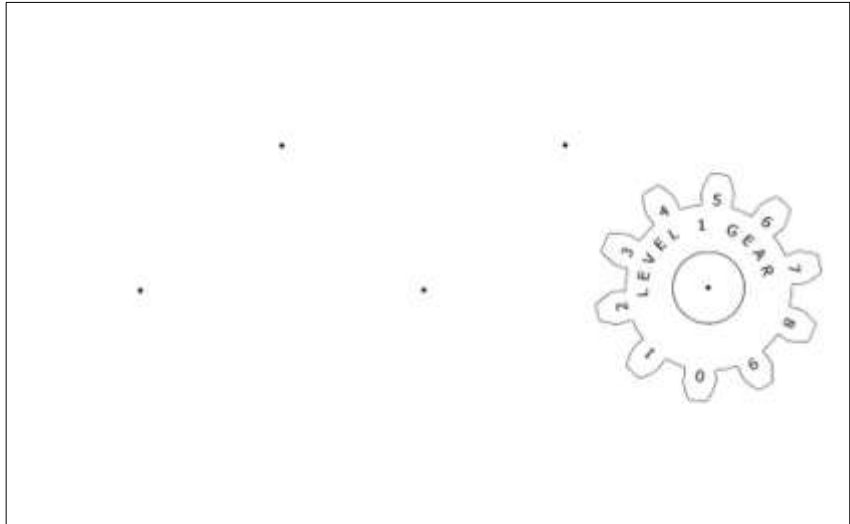


Figura 1

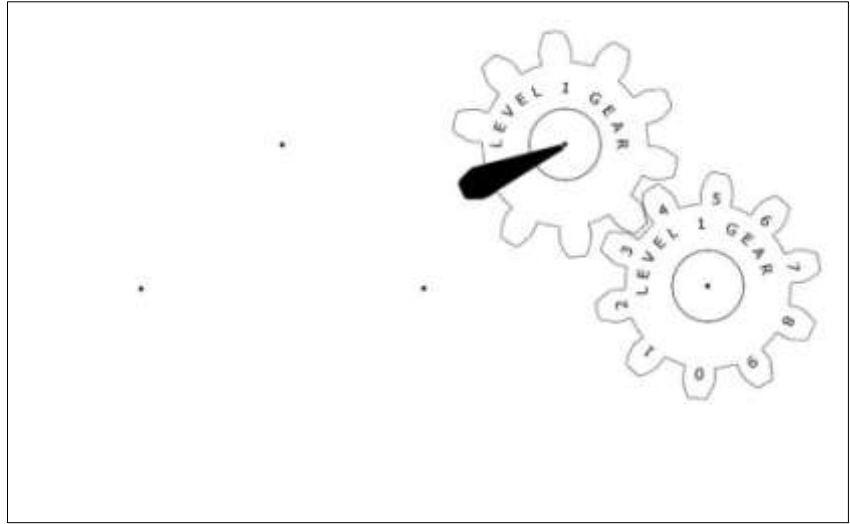


Figura 2

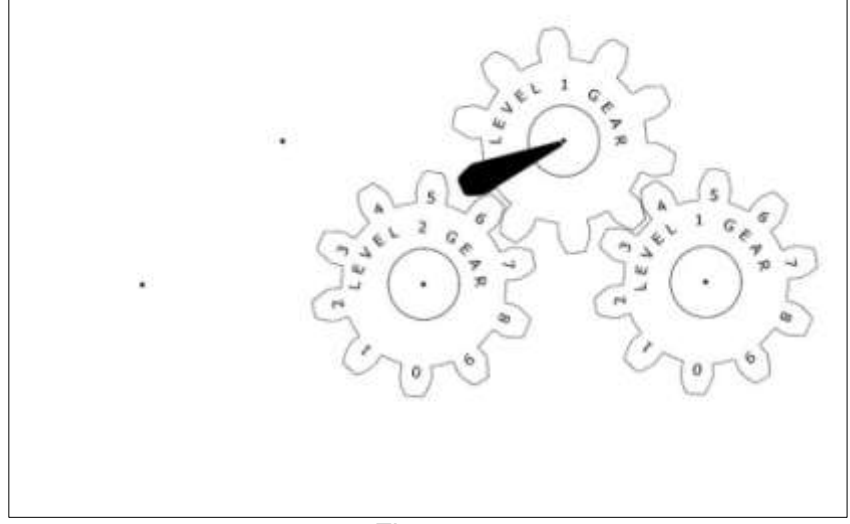


Figura 3

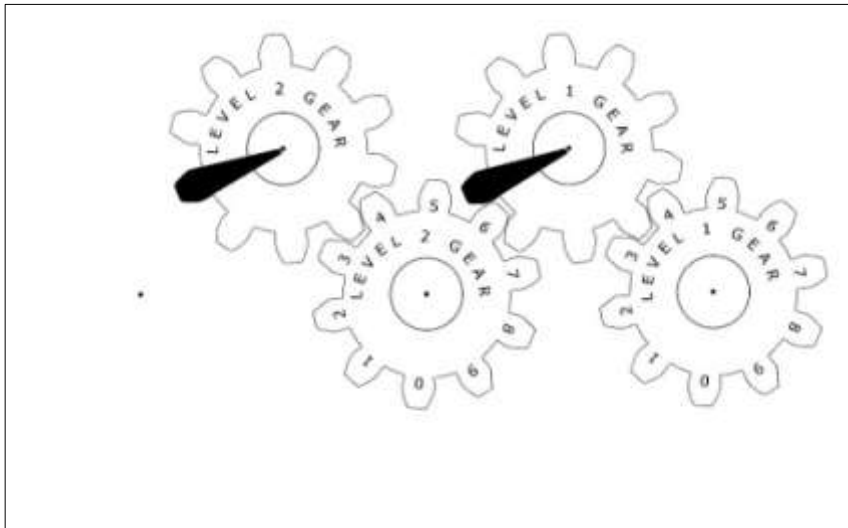


Figura 4

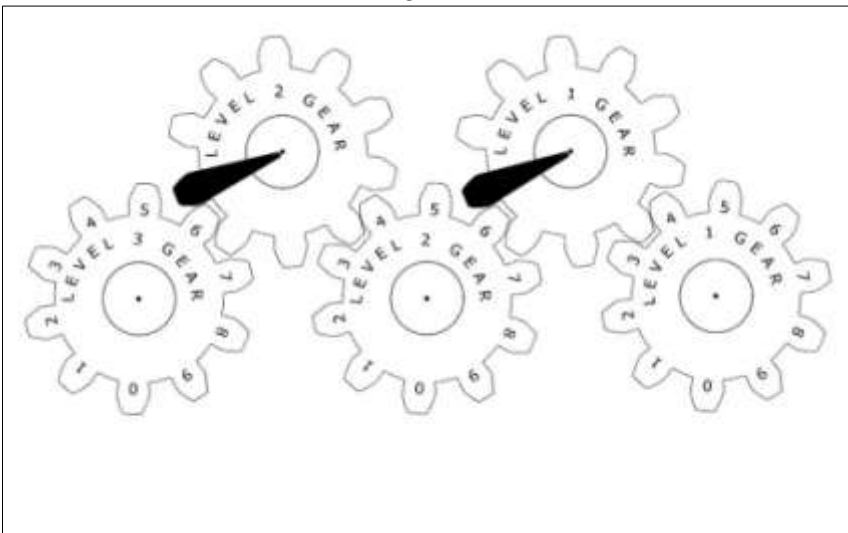


Figura 5

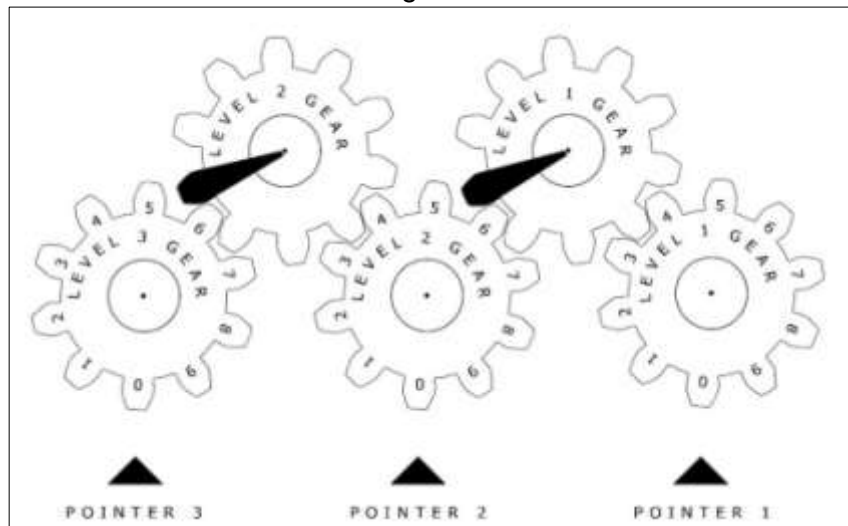


Figura 6

Figure 7

Worksheet 2 – La Pascalina en acción

Nombre(s): _____

Fecha: _____



Has creado una máquina para hacer cálculos llamada Pascalina, ¡Felicidades!

Ahora, veamos si tu máquina funciona correctamente.

1. Usando la Pascalina construida, intenta sumar **87+ 5**. ¿Es correcto el resultado?
2. Ahora intenta calcular **62-4**. ¿Es correcto el resultado?

Intenta responder a las siguientes preguntas

3. El panel frontal de la Pascalina se divide en dos áreas distintas una de entrada o receptora y otra de salida o productora. ¿Podrías localizar estas áreas?
4. ¿Cuál es el número más grande que una Pascalina puede producir?
5. ¿Qué tipos de operaciones aritméticas se pueden producir con la Pascalina?
6. ¿Es posible sumar números no enteros con la Pascalina?
7. ¿Cómo podemos introducir un dígito en la Pascalina?
8. Al realizar una operación la Pascalina ha de reiniciarse ¿Cómo se puede hacer?
9. ¿Cuál es el complemento de nueve de un número y cómo este concepto está relacionado con la Pascalina?
10. ¿Qué tipo de dispositivo es la Pascalina, analógico o digital?



Ahora eres el creador/a de una máquina de computación

¡Bien hecho!

Cenário 03: Gatos e Cães

Parte A. Dados gerais	
A.1 Título:	Gatos e cães
A.2 Autor(es):	Stavroula Prantsoudi, Universidade de Egeu
A.3 Resumo/ Resumo:	<p>Dispositivos inteligentes, ou seja, dispositivos que mostram inteligência, estão cada vez mais cerca dos alunos, que devem, portanto, estar preparados para usar essa tecnologia na sua vida social e profissional futura. Esses dispositivos usam algoritmos que melhoram automaticamente através da experiência que eles criam com base em dados de amostra. Os algoritmos podem tomar decisões ou previsões sem serem explicitamente programados para fazê-lo; a isso chama-se Machine Learning (ML), um subconjunto da Inteligência Artificial (IA).</p> <p>O objetivo deste cenário é apresentar aos alunos os conceitos básicos de ML e IA. Após uma introdução aos conceitos básicos de ML e IA, os alunos são convidados a construir, treinar e testar um modelo de aprendizado de máquina. Em seguida, discutem o problema do desvio da IA tentando encontrar razões e propor soluções. Para alargar o cenário, propõe-se a criação de uma aplicação utilizando um modelo ML.</p> <p>Espera-se que os alunos se familiarizem com conceitos básicos de IA, aprendam a criar e a usar modelos de ML e aumentem sua conscientização sobre questões de ética em IA, no que diz respeito ao uso de aplicações de IA na vida cotidiana, como o viés Algorítmico. Os alunos serão orientados a trabalhar de forma construtiva, colaborativa, em grupos de 2, ao mesmo tempo que interagem com toda a turma e o professor.</p> <p>O cenário introduz o conceito de aprendizagem de máquina e pode ser usado em muitos campos científicos e de diferentes temas, após ser devidamente modificado.</p>
A.4 Palavras-chave:	Aprendizagem de máquina, Inteligência Artificial, reconhecimento de imagem, IA, programação, Scratch
Versão A.5:	Versão 1
A.6 Data:	20/10/2021
A.7 licença de direitos de autor:	Atribuição ShareAlike CC BY-SA
Parte B. Dados de aprendizagem	
B.1 Grau(s):	Graus 9-10 ou Idade(s): 14-15 anos de idade
B.2 Assunto(s):	Ciência da Computação
B.3 Tópico(s):	Programação, Aprendizagem de Máquina, Reconhecimento de Imagem, Inteligência Artificial, Algoritmos

B.4 Dimensões de pensamento computacional:	Pensamento algorítmico (AL)	✓	
	Abstração (AB)	✓	
	Generalização (GE)	✓	
	Raciocínio lógico (LR)		
	Correspondência de padrões (PM)	✓	
	Decomposição de problemas (PD)	✓	
	Tradução de problemas (PT)		
	Avaliação (EV)	✓	
	Representação (RE)	✓	
	Recolha de dados (DC)	✓	
	Representação de dados (DR)	✓	
	Análise de dados (DA)	✓	
	Modelagem (MO)		
	Simulação — (SIM)		
	Automação (AUT)		
	Sequenciamento (SE)		
Ensaio (TE)	✓		
Compreensão das Pessoas — (UP)/Inteligência Artificial (IA)	✓		
B.5 Abordagens de Pensamento Computacional:	Tinkering experimentando & jogando	✓	
	Criando, projetando e fazendo	✓	
	Erros de depuração, detecção e correção	✓	
	Perseverante, continuando	✓	
	Colaborando, trabalhando em conjunto	✓	
B.6 Temática no contexto do projeto de computação:	Robótica Educacional ou Computação Física		
	Projeto de Ciência Computacional	Modelagem/Simulação	
		Modelagem bifocal	
		Sensores usam ou fabricam	
		Matemática e CS	
		Outros: ...	
	Projeto de ciência de dados	✓	
	História da ciência e da tecnologia		
	Jogo digital, software ou aplicativo móvel	✓	
	Projetos de Humanidades Digitais	Narração de Histórias Digitais	
		Ficção interativa	
		Mineração de texto	
		Algoritmos na vida cotidiana	✓
		Outros: ...	
	Projetos de Inteligência Artificial	✓	
Abordagem de estúdio — Projetos Future Classroom			
Desligado experiencial ou usando manipuladores			
Outros:			

<p>B.7 Objetivo/Objetivo do cenário de aprendizagem:</p>	<p>O objetivo do cenário de aprendizagem é familiarizar os alunos com o conceito de Aprendizagem de Máquina e Inteligência Artificial em geral. Os alunos estão cercados por dispositivos que usam aprendizagem de máquina (chatbots, plataformas digitais, plataformas sociais, algoritmos de tomada de decisão, algoritmos de previsão, etc.) e educá-los na forma como esses dispositivos funcionam é uma questão importante para a cidadania futura. Depois de completar o cenário, os alunos terão adquirido compreensão sobre a forma como os algoritmos usam os dados fornecidos para tomar decisões e previsões, e a inteligência que as máquinas mostram será explicada e revelada. Os alunos também estarão cientes das várias questões sociais e éticas levantadas devido a preconceitos algorítmicos.</p>							
<p>B.8 Resultados/objetivos de aprendizagem²:</p>	<p>Espera-se que tenham sido alcançados os seguintes objetivos após a conclusão do cenário:</p>	<table border="1"> <tr> <td data-bbox="483 712 651 974"> <p>B.8.1 Conhecimento</p> </td> <td data-bbox="651 712 1406 974"> <ul style="list-style-type: none"> ● Os alunos sabem como a inteligência artificial é incorporada aos sistemas. ● Os alunos sabem como os modelos de aprendizagem de máquina são construídos e usados para definir o comportamento de máquinas e sistemas. ● Os alunos sabem sobre a importância das suas próprias decisões sobre o treino dos modelos que os algoritmos usam. </td> </tr> <tr> <td data-bbox="483 974 651 1391"> <p>B.8.2 Competências</p> </td> <td data-bbox="651 974 1406 1391"> <ul style="list-style-type: none"> ● Os alunos podem treinar um modelo de aprendizagem de máquina (tomar decisões sobre os grupos de dados e categorizar dados no grupo adequado). ● Os alunos podem testar/avaliar um modelo de aprendizagem de máquina. ● Os alunos podem importar um modelo de aprendizagem de máquina para um algoritmo. ● Os alunos podem construir um algoritmo (que faz uso de um modelo de aprendizagem de máquina) para tomar decisões. ● Os alunos podem modificar um algoritmo (que faz uso de um modelo de aprendizagem de máquina) para tomar decisões. </td> </tr> <tr> <td data-bbox="483 1391 651 1756"> <p>B.8.3 Atitudes afetivas</p> </td> <td data-bbox="651 1391 1406 1756"> <ul style="list-style-type: none"> ● Os alunos desenvolveram habilidades de colaboração. ● Os alunos adquiriram conhecimento sobre conceitos de aprendizagem de máquina. ● Os alunos ganham compreensão sobre a forma como as máquinas e algoritmos da vida cotidiana usam dados para agir de forma inteligente (mostrar inteligência artificial). ● Os alunos adquiriram conhecimento sobre a forma como podem afetar o comportamento de um algoritmo, fornecendo-lhe certos dados. ● Os alunos aumentam a conscientização sobre questões de desvio algorítmico e métodos de preveni-lo. </td> </tr> </table>	<p>B.8.1 Conhecimento</p>	<ul style="list-style-type: none"> ● Os alunos sabem como a inteligência artificial é incorporada aos sistemas. ● Os alunos sabem como os modelos de aprendizagem de máquina são construídos e usados para definir o comportamento de máquinas e sistemas. ● Os alunos sabem sobre a importância das suas próprias decisões sobre o treino dos modelos que os algoritmos usam. 	<p>B.8.2 Competências</p>	<ul style="list-style-type: none"> ● Os alunos podem treinar um modelo de aprendizagem de máquina (tomar decisões sobre os grupos de dados e categorizar dados no grupo adequado). ● Os alunos podem testar/avaliar um modelo de aprendizagem de máquina. ● Os alunos podem importar um modelo de aprendizagem de máquina para um algoritmo. ● Os alunos podem construir um algoritmo (que faz uso de um modelo de aprendizagem de máquina) para tomar decisões. ● Os alunos podem modificar um algoritmo (que faz uso de um modelo de aprendizagem de máquina) para tomar decisões. 	<p>B.8.3 Atitudes afetivas</p>	<ul style="list-style-type: none"> ● Os alunos desenvolveram habilidades de colaboração. ● Os alunos adquiriram conhecimento sobre conceitos de aprendizagem de máquina. ● Os alunos ganham compreensão sobre a forma como as máquinas e algoritmos da vida cotidiana usam dados para agir de forma inteligente (mostrar inteligência artificial). ● Os alunos adquiriram conhecimento sobre a forma como podem afetar o comportamento de um algoritmo, fornecendo-lhe certos dados. ● Os alunos aumentam a conscientização sobre questões de desvio algorítmico e métodos de preveni-lo.
<p>B.8.1 Conhecimento</p>	<ul style="list-style-type: none"> ● Os alunos sabem como a inteligência artificial é incorporada aos sistemas. ● Os alunos sabem como os modelos de aprendizagem de máquina são construídos e usados para definir o comportamento de máquinas e sistemas. ● Os alunos sabem sobre a importância das suas próprias decisões sobre o treino dos modelos que os algoritmos usam. 							
<p>B.8.2 Competências</p>	<ul style="list-style-type: none"> ● Os alunos podem treinar um modelo de aprendizagem de máquina (tomar decisões sobre os grupos de dados e categorizar dados no grupo adequado). ● Os alunos podem testar/avaliar um modelo de aprendizagem de máquina. ● Os alunos podem importar um modelo de aprendizagem de máquina para um algoritmo. ● Os alunos podem construir um algoritmo (que faz uso de um modelo de aprendizagem de máquina) para tomar decisões. ● Os alunos podem modificar um algoritmo (que faz uso de um modelo de aprendizagem de máquina) para tomar decisões. 							
<p>B.8.3 Atitudes afetivas</p>	<ul style="list-style-type: none"> ● Os alunos desenvolveram habilidades de colaboração. ● Os alunos adquiriram conhecimento sobre conceitos de aprendizagem de máquina. ● Os alunos ganham compreensão sobre a forma como as máquinas e algoritmos da vida cotidiana usam dados para agir de forma inteligente (mostrar inteligência artificial). ● Os alunos adquiriram conhecimento sobre a forma como podem afetar o comportamento de um algoritmo, fornecendo-lhe certos dados. ● Os alunos aumentam a conscientização sobre questões de desvio algorítmico e métodos de preveni-lo. 							

²Para a formulação efetiva de objetivos de aprendizagem-instrução, as obras de Mager, que reivindica a definição de ações observáveis e critérios mensuráveis de avaliação de desempenho em condições específicas, poderiam ser úteis. Mager, F. (1975). Preparação de Objetivos Instrucionais. (2a ed.). Belmont, CA: É o Fearon. & Mager, F. (1997). Preparação de objetivos instrucionais: Uma ferramenta crítica no desenvolvimento de uma instrução eficaz. Atlanta: O Centro de Desempenho Eficaz. Os verbos poderiam seguir a taxonomia do conhecimento de Bloom, veja por exemplo: <https://tips.ark.edu/blooms-taxonomy-verb-chart/>. É importante usar verbos de pensamento de ordem superior. Consultado em 21 de dezembro de 2011 Anderson, L. W., & Krathwohl, D. R. (2001). Uma taxonomia para aprender, ensinar e avaliar, Edição abreviada. Boston, MA: Allyn e Bacon

B.9 Competências horizontais — habilidades do século XXI:	B.9.1 Competências de aprendizagem em e inovação:	<p>Colaboração: os alunos trabalham em grupos de 2 e colaboram</p> <p>Comunicação: os alunos se comunicarão com outros grupos para testar os seus resultados</p> <p>Pensamento crítico: os alunos precisam pensar criticamente para tomar decisões sobre as imagens e usam as aulas para treinar os seus modelos</p> <p>Criatividade: espera-se que os alunos melhorem o seu algoritmo alterando trajés, sons e expressões</p>
	B.9.2 Competências em literacia digital:	<p>Literacia da informação: os alunos avaliam informações para treinar adequadamente seu modelo de aprendizagem de máquina</p> <p>Literacia nas tecnologias da informação e comunicação (TIC): os alunos serão capazes de treinar um modelo de aprendizagem de máquina e construir um algoritmo numa plataforma de programação popular (Scratch)</p> <p>Cidadania digital: os alunos estão cientes do conceito de aprendizagem de máquina e da forma como ele é usado em vários campos da vida quotidiana. Estão também cientes da questão do preconceito em matéria de IA.</p>
	B.9.3 Competências de carreira e de vida:	<p>Flexibilidade e adaptabilidade: os alunos podem ser flexíveis e adaptar os seus dados para treinar o seu modelo para reagir em novos casos</p> <p>Iniciativa e autodireção: os alunos devem tomar decisões sozinhos, mas também contribuir para que o grupo chegue a um resultado</p> <p>Interação social e intercultural: os alunos devem interagir com outros grupos e testar os seus resultados</p> <p>Produtividade e responsabilização: os alunos devem tentar produzir o melhor resultado no tempo dado e fazer o seu algoritmo funcionar para o número máximo de casos.</p>
B.10 Métodos de ensino modernos:	Os alunos trabalham em grupos de 2 com base num guião de inquérito colaborativo. Espera-se que eles aprendam por codificação, de forma baseada em projetos.	
B.11 Integração do CT no currículo:	<p>O cenário, dependendo do modelo de aprendizagem de máquina utilizado, pode ser combinado com muitos campos da ciência em termos de interdisciplinaridade. A presente implementação categoriza imagens, para que possa ser usada para categorizar animais, livros, materiais de reciclagem, veículos, máquinas etc. para combinar com Ciência, Sociologia, Educação Ambiental, História etc.</p> <p>Um modelo diferente poderia categorizar texto para combinar com Linguagem e Psicologia (por exemplo, categorização de sentimentos de acordo com as palavras utilizadas). Além disso, um modelo de categorização de áudio poderia ser usado para combinar com Música, Artes, Dança ou qualquer outro assunto.</p>	
B.12 Relação com os currículos e/ou normas:	<p>Currículo Nacional Grego, Grau 9-10, Informática.</p> <p>Qualquer outra idade e/ou assunto em implementação interdisciplinar.</p>	

B.13. Conhecimentos pré-requisitos:	Os alunos precisam ter conhecimento básico de pesquisa na web e gestão de arquivos. Será necessária uma programação de riscos para a execução da extensão.	
B.14. Nível de dificuldade do cenário:	Médio	
B.15. Cenário social do cenário:	Par (2 estudantes), ou individual	
B.16 Local de execução:	Laboratório de computador	
B.17 Tempo de ensino — Duração:	3 x 45' sessões (ou 1x45' +1x90')	
B.18 Material educativo, recursos, instrumentos, ferramentas e meios de comunicação:	B.18.1 Software:	Scratch, navegador da Web https://teachablemachine.withgoogle.com/ https://dancingwithai.media.mit.edu/ https://machinelearningforkids.co.uk/
	B.18.2 Hardware:	
	B.18.3 Recursos em linha:	https://teachablemachine.withgoogle.com/ https://dancingwithai.media.mit.edu/ https://machinelearningforkids.co.uk/ Payne, B.H. & Breazeal, C. (2019). An Ethics of Artificial Intelligence Curriculum for Middle School Students (em inglês). MIT Media Lab (em inglês).
	B.18.4 Material didático convencional:	

Parte C. Design de Experiência de Aprendizagem

C.1. Tabela de sequências de atividades-Action-Plot-Storyboard:	Fase 1.	Título da fase: Introdução e Exploração	
	Atividade/Tarefa	Descrição/Procedimento	Duração
	A1.1 Warm up — Introdução à IA — a definição de IA	O professor partilha a Imagem 1 e segue as diretrizes Os alunos discutem o conceito de inteligência em geral, a definição de Inteligência Artificial e a sua presença na vida cotidiana. Os alunos respondem às perguntas na ficha. Visionam o vídeo https://www.youtube.com/watch?v=nASDYRkbQIY (O que é inteligência artificial? A Sociedade Real) e discutem sobre ele.	15 min.

	A1.2 Aplicações de IA	O professor orienta os alunos para listar aplicações de IA e o seu uso diário, orienta-os a usar alguns deles e propõe outros, categoriza-os com base num mapa conceitual e procura exemplos adicionais de cada categoria. Os alunos também vêem um vídeo https://www.youtube.com/watch?v=3wLqsRLvV-c (O teste de Turing: Um computador pode passar para humano?) e discutir sobre o famoso teste de Turing.	30 min
	Fase 2.	Título da fase: Desenvolvimento e Avaliação	
	Atividade/Tarefa	Descrição/Procedimento	Duração
	A2.1 Conceitos de IA — aprendizagem de máquina e recolha de dados	O professor partilha a Ficha 2 . Seguidamente, incita os alunos a questionarem-se se há uma maneira de ensinar uma máquina para reconhecer qualquer foto e distinguir entre gatos e cães (Discussão). Com base na ficha, os alunos recolhem os dados necessários para construir um modelo para esse motivo.	10 min
	A2.2 Construa, treine e avalie um modelo de aprendizagem de máquina	Seguindo as diretrizes, os alunos constroem um modelo de aprendizagem de máquina na plataforma sugerida https://teachablemachine.withgoogle.com/ . Treinam, testam e avaliam o seu modelo e acrescentam novos exemplos/dados, se necessário.	30 min
	A2.3 Avaliação	O professor partilha a Ficha de Avaliação 2.1 e pede aos alunos que respondam às perguntas para refletir sobre a construção de modelos de ML	5 min
	Fase 3.	Título da fase: Questões éticas da IA	
	Atividade/Tarefa	Descrição/Procedimento	Duração

	<p>A3.1 Aumentar a sensibilização para as questões éticas da IA e lutar contra elas</p>	<p>O professor orienta um debate sobre as questões éticas e sociais suscitadas pela utilização da IA.</p> <p>A Ficha 3 contém algumas perguntas e vídeos propostos para lançar a discussão. O professor pode adaptar o conteúdo da ficha (vídeos e perguntas) a cada aula, sempre com o objetivo de sensibilizar os alunos para as questões críticas da ética e segurança da IA.</p> <p>A duração da sessão e a duração do debate também podem ser adaptadas de acordo com a vontade dos professores.</p>	<p>45 min</p>			
<p>C.2 Avaliação</p>	<table border="1"> <tr> <td data-bbox="480 920 855 1111"> <p>C.2.1 feedback e reflexão dos alunos</p> </td> <td colspan="2" data-bbox="855 920 1398 1111"> <p>Os alunos testarão e avaliarão o seu modelo de ML e compararão os resultados em tempo real. Também preencherão a ficha de avaliação.</p> <p>Os modelos serão avaliados pelos colegas.</p> </td> </tr> </table>			<p>C.2.1 feedback e reflexão dos alunos</p>	<p>Os alunos testarão e avaliarão o seu modelo de ML e compararão os resultados em tempo real. Também preencherão a ficha de avaliação.</p> <p>Os modelos serão avaliados pelos colegas.</p>	
<p>C.2.1 feedback e reflexão dos alunos</p>	<p>Os alunos testarão e avaliarão o seu modelo de ML e compararão os resultados em tempo real. Também preencherão a ficha de avaliação.</p> <p>Os modelos serão avaliados pelos colegas.</p>					
<p>C.3 Trabalho de casa/ Trabalhar com pais-família</p>	<p>Os alunos podem construir os seus modelos de ML em casa e testá-los com dados reais (como os seus próprios animais de estimação). Poderiam também discutir com os seus pais e familiares e encontrar aplicações de IA que já utilizam e propor novas aplicações.</p> <p>O professor pode selecionar e atribuir uma extensão a cada equipa como lição de casa.</p>					
<p style="text-align: center;">Parte D. Informação para os Professores</p>						
<p>D.1 Adaptação — Diferenciação para inclusão de todos os alunos</p>	<p>A construção pode ser adaptada ao tempo de ensino disponível. São propostas 3 sessões de 45 minutos. Caso isso não seja possível, propõe-se que os professores implementem o cenário em 1 sessão de 45 min e 1 sessão de 90 min.</p> <p>Todos os alunos da educação geral podem implementar o cenário sem restrições.</p>					

D.2 Extensão	Uma extensão do cenário poderia ser a construção de uma aplicação no Scratch que utiliza um modelo ML. A ficha 4 pode ser usada por esse motivo, embora não de forma restritiva.	
	Extensão da fase.	Título da fase: Usando inteligência para construir algo útil
	AE.1 Construir uma aplicação (um algoritmo para agir de forma inteligente) (35 min)	O professor partilha a Ficha 4 e os alunos seguem as diretrizes. Os alunos constroem um algoritmo para incorporar um modelo ML que eles criaram anteriormente. Utilizam a plataforma https://machinelearningforkids.co.uk/ e o ambiente de programação Scratch. Os alunos são convidados a estudar os exemplos e tentar construir um modelo e um algoritmo para jogar Rock, papel, tesoura com o computador.
AE.2 Avaliar o algoritmo (teste a sua aplicação) (10 min)	Depois da construção os alunos são convidados a testá-lo e fazer as possíveis modificações. Também ajudam a testar, avaliar e modificar as aplicações de seus colegas de turma.	
D.3 Recursos	https://teachablemachine.withgoogle.com/ https://dancingwithai.media.mit.edu/ https://machinelearningforkids.co.uk/	
D.4 Experiência decorrente da implementação do cenário		
D.5 Relações com outros cenários	Payne, B.H. & Breazeal, C. (2019). An Ethics of Artificial Intelligence Curriculum for Middle School Students (em inglês). MIT Media Lab (em inglês).	
D.6 Comentários por professores		
D.7 Avaliação do cenário	[1=Muito mau — 5=Muito bom]	
D.8 Referências	Payne, B.H. & Breazeal, C. (2019). An Ethics of Artificial Intelligence Curriculum for Middle School Students (em inglês). MIT Media Lab (em inglês).	
Parte E. Anexos		
	Ficha 1, Ficha 2, Ficha 2.1, Ficha 3, Ficha 4	

Aprendizagem de máquina _ Ficha 1

Introdução à IA — Conceitos de IA



Nome(s) dos alunos: ____

Nome do grupo: ____

Data: ____

Hoje vais aprender sobre Inteligência Artificial e a sua presença na nossa vida quotidiana.

A. Definição de IA

A. Em breve responde às seguintes perguntas. Em seguida, discute as tuas respostas com os colegas e o professor:

1. O que é inteligência?

2. Quando é que um ser humano é considerado inteligente?

3. Outras criaturas podem ser inteligentes? Como é que sabes quando isso acontece?

4. As máquinas podem agir de forma inteligente? Que máquinas podem fazer isso?

5. Como achas que qualquer comportamento inteligente pode ser alcançado por máquinas?

6. O que é a **Inteligência Artificial**?

7. Assiste ao vídeo no seguinte link

<https://www.youtube.com/watch?v=nASDYRkbQIY> (Oque é inteligência artificial? A Sociedade Real). Volta para a resposta que deste na pergunta 6 e discuta-a com os teus colegas e o professor.

B. Aplicações de IA

B. Dizem que medida as seguintes aplicações estão a utilizar a IA.

a. Chatbot

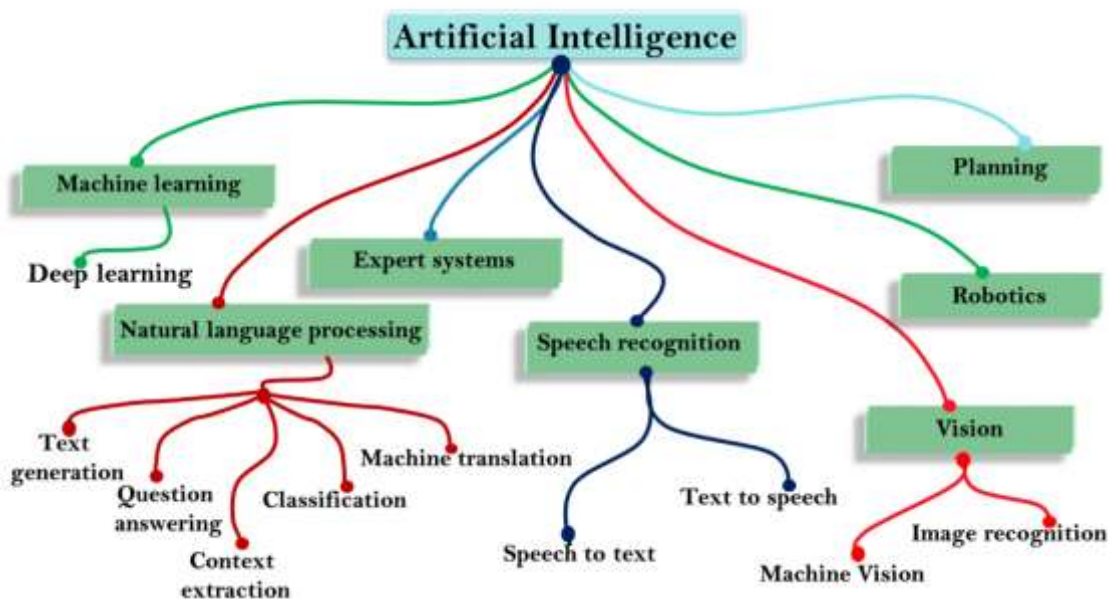
c. Veículos autónomos

b. Motores de busca

d. Robots

- e. Redes sociais
- f. Um sistema de tradução
- g. Anúncios em linha
- h. Assistentes virtuais (Siri, Alexa)

1. Usa os seguintes aplicativos e discute os seus recursos com os colegas de turma:
 - a. Discurso do Google Chrome para Texto
 - b. O chat bot de alerta de saúde da OMS, <https://www.who.int/>
 - c. A aplicação Photomath, <https://photomath.com>
2. Usando o mapa conceitual, pesquisa na Web de forma a encontrares um exemplo de uma aplicação na vida quotidiana, para cada categoria (branch) no mapa. Discute os exemplos que encontraste com os teus colegas e o professor.



3. Vê o vídeo no seguinte link
<https://www.youtube.com/watch?v=3wLqsRLvV-c> (O teste de Turing: Um computador pode passar para humano?). Discute o teste de Turing com os teus colegas e o professor.
4. Existe algum risco causado pela utilização da IA? O que é que eles podem ser?

5. Sugerir formas de eliminar possíveis perigos (se houver) causados pela utilização da IA. Discute a sugestão com os teus colegas e o professor.

Bom trabalho!

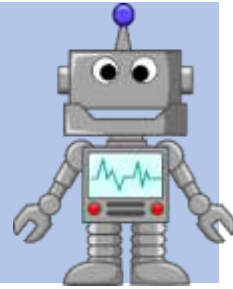
Até agora, aprendeste sobre a definição de Inteligência Artificial e o seu uso na vida quotidiana.

Em seguida, aprenderás sobre conceitos básicos de IA aprendizagem de máquina.



Aprendizagem de máquina _ Ficha 2

Construir um modelo de IA



Nome(s) dos alunos: ____

Nome do grupo: ____

Data: ____

Hoje vais ensinar um computador a decidir se uma imagem mostra um gato ou um cão.

Responde às seguintes perguntas de warm up:

- Um computador pode reconhecer animais (**SIM** ou **NÃO**)? ____
- Em **caso afirmativo**, como é que isso acontece?

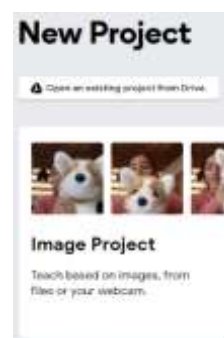
- Se **NÃO**, podemos ensinar um computador a reconhecer animais?

Os computadores tomam decisões usando **algoritmos** e **dados** que as pessoas lhes forneceram. Isso é chamado de **Machine Learning**.

Agora vais ensinar um computador a **classificar** gatos e cães, criando um **modelo**.

A. Constroi o teu modelo

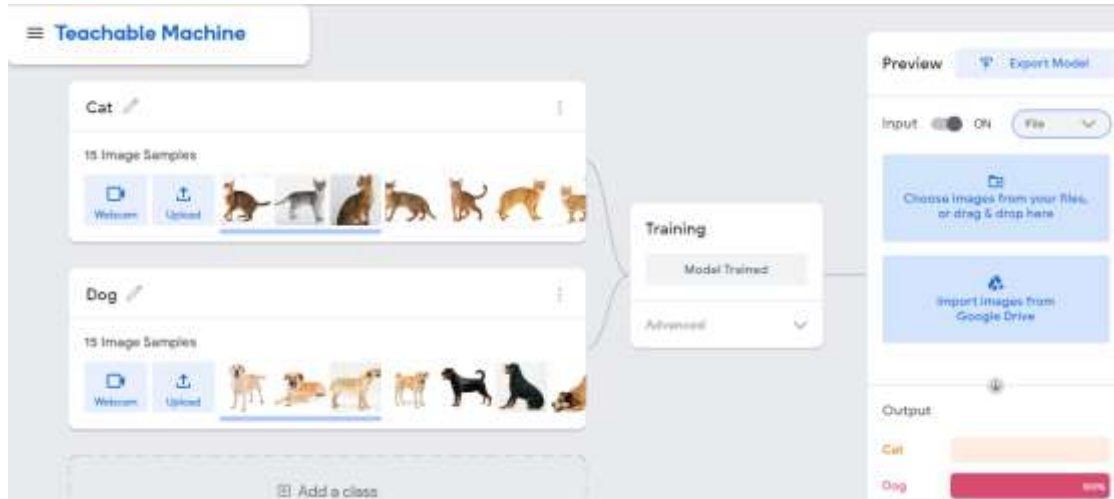
- Cria duas pastas no teu computador e dá-lhes o nome de **Gatos** e **Cães**. Pesquisa na web e recolhe imagens de gatos e cães (pelo menos 10-15 de cada categoria) e guarda-as na pasta apropriada. Certifica-te de que há variedade e diversidade nas imagens que selecionaste.
- Abre um navegador web e visite <https://teachablemachine.withgoogle.com/>
- Clica em «**Começar**». Criarás um novo projeto de imagem então clica nele e seleciona **Modelo de imagem padrão** na janela pop-up.



- Nomeia as duas pastas **Gatos** e **Cães** e faz upload das imagens selecionadas na pasta apropriada.

B. Treina o teu modelo

1. Clica em **Treinar o modelo** e aguarda. O computador pode precisar de alguns minutos para treinar o o modelo. **Sê paciente!** Após a conclusão do treino, o teu modelo deve parecer-se com o abaixo indicado:



2. Para **visualizar** os resultados do teu modelo, usa as opções disponíveis à direita (a webcam ou um novo arquivo).
 - a. No conjunto de dados dos gatos, que diferenças e semelhanças existem entre os gatos?
 - b. No conjunto de dados dos Cães, que diferenças e semelhanças existem entre os cães?
3. Pensa em casos de animais que podes não ter incluído no modelo. Podes sempre voltar ao modelo, adicionar exemplos e executá-lo novamente.

C. Testa o teu modelo

1. Cria uma nova pasta e recolhe alguns **dados de teste**, como imagens de gatos e cães que não incluíste nos exemplos que usaste para treinar o modelo. Recolhe também imagens de outros animais (leão, urso, raposa, coala etc.). Cria um conjunto de dados de teste semelhante ao indicado abaixo:



2. Testa as imagens recolhidas no teu modelo (importar ou arrastar e soltar cada imagem). A máquina irá dizer-te o que reconhece, bem como o quão confiante é. (Também podes ligar a webcam e testar o modelo com imagens impressas). A **saída** está correta?
3. Para cada imagem de teu conjunto de dados de teste, escreve os resultados como na tabela abaixo. Podes explicar cada resultado? Por exemplo, porque é que o modelo acha que o leão é um gato?

Imagem	Classe	Confiança	Resultado
Leão	Gato	82 %	Errado



4. Pede a alguns dos teus colegas para te ajudarem a testar o teu modelo. Troca os teus dados de teste com os dos teus colegas de turma e testa os teus dados num outro modelo e vice-versa. Os resultados são semelhantes? Porquê/Por que não?
5. Estás feliz com as respostas? Se não, não te esqueças que podes voltar ao modelo e adicionar mais alguns exemplos. Treina o teu modelo novamente, depois de ter adicionado exemplos.
6. O que achas que deve acontecer para que o modelo reconheça outros animais além de cães e gatos? Achas que podes criar um modelo que reconheça qualquer animal no planeta?
7. Faz **download do projeto e guarda-o**.

Bom trabalho!

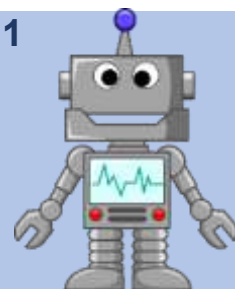
Até agora, treinaste o teu computador para reconhecer imagens como gatos ou cães, assim, treinaste um **modelo de aprendizagem de máquina** alimentando-o com exemplos.

Agora podes continuar a criar algo mais divertido e útil, incorporando o teu modelo em uma aplicação.



Aprendizagem de máquina _ Ficha 2.1

Avaliação



Nome(s) dos alunos: ____

Nome do grupo: ____

Data: ____

Uma vez que aprendeste a construir um modelo de Machine Learning, agora deves ser capaz de prever o comportamento de um modelo com base nos conjuntos de dados usados para o seu treino.

Vê as imagens e conjuntos de dados abaixo e tenta responder às seguintes perguntas:

1. Um modelo de Machine Learning foi treinado com os seguintes dados de treino:

Classe

Imagens

Gato



O que achas que resultará se importares a imagem a seguir?



Cão OU O gato?

2. Um modelo de Machine Learning foi treinado com os seguintes conjuntos de dados de treino:

Classe

Imagens

Gato



Cão







Qual da(s) frase(s) seguinte(s) está(ão) correta(s), no que diz respeito aos resultados do modelo:

- i. Os resultados serão mais precisos para os Cães

- ii. Os resultados serão mais precisos para os gatos
- iii. Os resultados serão igualmente precisos para os Cães e os Gatos

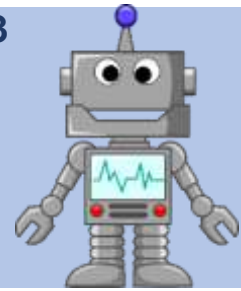
3. Qual dos seguintes conjuntos de dados de formação dará resultados mais precisos? Porquê?

	Gato	Cão
A A.		
B.		



Aprendizagem de máquina _ Ficha 3

Ética/Segurança da IA



Nome(s) dos alunos: ____

Nome do grupo: ____

Data: ____

A Inteligência Artificial (IA) conquistou a vida humana e seu uso é quase inevitável. Junto com seus inúmeros benefícios, vozes de preocupação aumentam a cada dia. Hoje aprenderás sobre as questões sociais e éticas decorrentes do uso da IA, os perigos potenciais e sugestões para estar sempre ciente deles.

DICA: Antes de assistir a cada um dos seguintes vídeos, vê as perguntas que se seguem

Ética e IA

Discute as seguintes perguntas com o teu colega e o teu professor:

1. Existe um sistema de inteligência artificial que funcione corretamente em todos os casos?
2. Acreditas que os sistemas de ML são sempre certos/justos?

Vê ao seguinte vídeo: <https://www.youtube.com/watch?v=tJQSyzBUAew> (Ethics & AI: Igualdade de Acesso e Bias Algorítmicas)

3. Quais são os perigos potenciais da utilização da IA? Como podem afetar as pessoas e a sociedade?
4. O que é que as pessoas e/ou a indústria devem fazer para evitar tais problemas?

Vê ao seguinte vídeo: <https://www.youtube.com/watch?v=BtgcuHQ0cks> (Bias na IA é um problema)

5. Quais são as razões que causam desvios em algoritmos?
6. Podes dar alguns exemplos de algoritmos que podem ter sido tendenciosos?
7. Como é que tais avarias podem ser evitadas?

Visita <https://www.ajl.org/>, o site da iniciação da Liga da Justiça Algorítmica, um esforço para uma IA equitativa e responsável. Navega pelo site para:

8. Listar dois exemplos em que o preconceito de IA afetou as pessoas reais.
9. Propor ações para uma melhor IA.



Parabéns!

Tornaste-te oficialmente um especialista em IA!

Aprendizagem de máquina _ Ficha 4

Aplicações de IA



Nome(s) dos alunos: ____

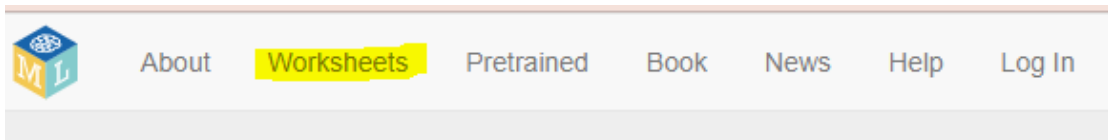
Nome do grupo: ____

Data: ____

Depois de terminares de **treinar o teu modelo**, é hora de usá-lo para fazer algo mais divertido e amigável. Podes pensar e criar qualquer aplicativo que possa ser útil na tua vida quotidiana ou modificar e usar alguns dos existentes.

Criar uma aplicação

1. Visita <https://machinelearningforkids.co.uk/>, outro site onde podes construir e treinar um modelo de aprendizagem de máquina. Clica no menu e navega pelos vários Projetos de Aprendizagem de Máquina. Não são fantásticos?



2. Depois de navegar nos vários projetos, seleciona o **Rock, Paper, Scissors** um e faz download dos documentos. Serás guiado para criar um programa em Scratch para jogar o jogo com o computador.



3. Segue os passos da ficha para treinar um modelo para reconhecer a sua mão como sendo rocha, papel ou tesoura. Em seguida, usa o modelo e programa um aplicativo no Scratch para jogar o jogo com o computador.
 - ✓ Podes sempre voltar ao teu modelo para adicionar mais exemplos.
 - ✓ Podes usar qualquer exemplo de projeto que desejes e modificá-lo para criar a tua própria aplicação. Acima de tudo, olha para o lado divertido da IA.

Bom trabalho!

Agora podes treinar com sucesso um modelo de Machine Learning e



construir um aplicativo para usá-lo. **Parabéns!**

Cenário 04: Criptografia

<u>Parte A. Dados gerais</u>	
A.1 Título:	Criptografia
A.2 Autor(es):	Zervas Konstantinos, Fesakis Georgios — Universidade do Egeu
A.3 Resumo/ Resumo:	<i>O estudo das técnicas utilizadas para garantir a comunicação, uma grande necessidade nos dias de hoje, é chamado de criptografia. Desde os tempos antigos, muitos métodos de criptografia têm sido usados para proteger a comunicação. Os alunos devem estar cientes desses métodos e técnicas e ser capazes de usá-los de acordo, quando necessário. Este cenário é uma introdução aos chamados métodos de criptografia simétrica, como Morse, Braille e Caesar Cipher. Ele também apresenta aos alunos a criptografia assimétrica com base no conceito de criptografia de chave pública. Além disso, através de várias extensões, os alunos podem ter a oportunidade de explorar a máquina enigma, o algoritmo RSA, bem como as várias aplicações do PKE. Pretende-se ensinar métodos e práticas de encriptar e descriptografar mensagens, de uma forma simulada através de software educacional, para que os alunos possam adquirir compreensão e conhecimento do conceito de criptografia.</i>
A.4 Palavras-chave:	Criptografia, criptografia, descodificação, criptografia simétrica/assimétrica, cifra César, Morse, Braille, máquina Enigma, [criptografia de chave pública (PKE), RSA, Assinatura Digital, Autoridades certificadoras]
Versão A.5:	Versão 1
A.6 Data:	05/11/2021
A.7 licença de direitos de autor:	Atribuição ShareAlike CC BY-SA
<u>Parte B. Dados de aprendizagem</u>	
B.1 Grau(s):	Graus 8-10, ou idade(s): 13-15 anos de idade
B.2 Assunto(s):	Ciência da Computação
B.3 Tópico(s):	Criptografia, segurança, criptografia, descriptografia

B.4 Dimensões de pensamento computacional:	Pensamento algorítmico (AL)	
	Abstração (AB)	✓
	Generalização (GE)	✓
	Raciocínio lógico (LR)	✓
	Correspondência de padrões (PM)	✓
	Decomposição de problemas (PD)	
	Tradução de problemas (PT)	
	Avaliação (EV)	
	Representação (RE)	✓
	Recolha de dados (DC)	
	Representação de dados (DR)	
	Análise de dados (DA)	
	Modelagem (MO)	
	Simulação — (SIM)	
	Automação (AUT)	
	Sequenciamento (SE)	
Ensaio (TE)	✓	
Compreensão das Pessoas — (UP)/Inteligência Artificial (IA)	✓	
B.5 Abordagens de Pensamento Computacional:	Tinkering experimentando & jogando	✓
	Criando, projetando e fazendo	
	Erros de depuração, detecção e correção	✓
	Perseverante, continuando	
	Colaborando, trabalhando em conjunto	✓

B.6 Temática no contexto do projeto de computação:	Robótica Educacional ou Computação Física			
	Projeto de Ciência Computacional	Modelagem/Simulação		
		Modelagem bifocal		
		Sensores usam ou fabricam		
		Matemática e CS		
		Outros: ...		
	Projeto de ciência de dados		✓	
	História da ciência e da tecnologia		✓	
	Jogo digital, software ou aplicativo móvel			
	Projetos de Humanidades Digitais	Narração de Histórias Digitais		
		Ficção interativa		
		Mineração de texto		
		Algoritmos na vida cotidiana		✓
		Outros: ...		
	Projetos de Inteligência Artificial			
	Abordagem de estúdio — Projetos Future Classroom			
	Desconectado experiencial ou usando manipuladores		✓	
	Outros:			
B.7 Objetivo/Objetivo do cenário de aprendizagem:	O objetivo do cenário é ajudar os alunos a familiarizarem-se com o conceito de criptografia e vários métodos de criptografar e descriptografar mensagens. Os alunos serão capazes de proteger os seus dados usando vários métodos criptográficos para enviar e receber mensagens numa era em constante evolução da tecnologia.			
B.8 Resultados/objetivos de aprendizagem³:				
B.8.1 Conhecimento	Os alunos demonstram compreensão sobre criptografia.			
	Os alunos explicam a necessidade de criptografar e			

³Para a formulação eficaz dos objetivos de aprendizagem-instrução, o trabalho de Mager sobre a definição de ações observáveis e critérios mensuráveis de avaliação de desempenho em condições específicas, poderia ser útil. Mager, F. (1975). Preparação de Objetivos Instrucionais. (2a ed.). Belmont, CA: É o Fearon. & Mager, F. (1997). Preparação de objetivos instrucionais: Uma ferramenta crítica no desenvolvimento de uma instrução eficaz. Atlanta: O Centro de Desempenho Eficaz. Os verbos poderiam estar de acordo com a taxonomia do conhecimento de Bloom, veja por exemplo: <https://tips.uark.edu/blooms-taxonomy-verb-chart/>. É importante usar verbos de pensamento de ordem superior. Consultado em 21 de dezembro de 2011 Anderson, L. W., & Krathwohl, D. R. (2001). Uma taxonomia para aprender, ensinar e avaliar, Edição abreviada. Boston, MA: Allyn e Bacon

		<p>descriptografar mensagens nesta era tecnológica em constante evolução.</p> <p>Os alunos ilustram exemplos de ameaças on-line durante a comunicação.</p> <p>Os alunos comparam alguns métodos básicos e amplamente utilizados de criptografia.</p>
	B.8.2 Competências	<p>Os alunos podem aplicar sinais Morse para criptografar/descriptografar uma mensagem.</p> <p>Os alunos podem fazer uso de sinais Braille para criptografar/descriptografar uma mensagem.</p> <p>Os alunos podem aplicar a chave de cifra César para criptografar/descriptografar uma mensagem.</p> <p>Os alunos podem experimentar criptografar/descriptografar uma mensagem usando uma simulação da máquina Enigma.</p> <p>(Se as extensões forem implementadas:</p> <p>Os alunos podem aplicar métodos assimétricos para criptografar/descriptografar mensagens (RSA, assinaturas digitais).</p> <p>Os alunos podem criar um novo método para criptografar/descriptografar uma mensagem para comunicar com segurança com um amigo.)</p>
	B.8.3 Atitudes afetivas	<p>Os alunos identificam a necessidade de proteger mensagens criptografando-as.</p> <p>Os alunos tornaram-se conscientes em questões de segurança.</p> <p>Os alunos podem colaborar para encontrar maneiras de comunicar com segurança com seus amigos.</p>
B.9 Competências horizontais — habilidades do século XXI:		
	B.9.1 Competências de aprendizagem e inovação:	<p>Colaboração: os alunos trabalham em grupos de 2 e colaboram</p> <p>Comunicação: os alunos comunicam com outros grupos para testar as suas mensagens criptografadas</p> <p>Pensamento crítico: os alunos precisam pensar criticamente para tomar decisões sobre a forma como vão criptografar as suas mensagens</p> <p>Criatividade: espera-se que os</p>

		alunos pensem em novos métodos para criptografar/descriptografar as suas mensagens
	B.9.2 Competências em literacia digital:	<p>Literacia da informação: os alunos avaliam informações a fim de selecionar o método apropriado para o seu método de criptografia/descriptação</p> <p>Cidadania digital: os alunos estão cientes do conceito de criptografia e das várias maneiras que ele é usado nos campos da vida quotidiana</p>
	B.9.3 Competências de carreira e de vida:	<p>Flexibilidade e adaptabilidade: os alunos devem ser flexíveis e adaptar o seu método de criptografia/descriptação de acordo com os dados fornecidos</p> <p>Iniciativa e autodireção: os alunos devem tomar decisões sozinhos, mas também contribuir para que o grupo chegue ao resultado</p> <p>Interação social e intercultural: os alunos devem interagir com outros grupos e testar os seus resultados</p>
B.10 Métodos de ensino modernos:	Aprendizagem colaborativa	
B.11 Integração do CT no currículo:	<p>A criptografia é um exemplo de arte combinada com a ciência, onde a informática causou uma transformação radical, com implicações sociais para todos os cidadãos. O método computacional de resolução de problemas é claramente visto no caso da criptoanálise.</p> <p>O cenário pode ser combinado com muitos assuntos dependendo da mensagem a ser tratada de cada vez.</p>	
B.12 Relação com os currículos e/ou normas:	Currículo Nacional Grego, Grau 8-10, Currículo de Ciência da Computação	
B.13.	Nenhum conhecimento prévio necessário para implementar com	

Conhecimentos pré-requisitos:	sucesso o cenário atual.	
B.14. Nível de dificuldade do cenário:	Produtos intermédios	
B.15. Cenário social do cenário:	Individual ou par (2 estudantes)	
B.16 Local de execução:	Sala de aula ou laboratório de computador	
B.17 Tempo de ensino — Duração:	4 x 45' sessões	
B.18 Material educativo, recursos, instrumentos, ferramentas e meios de comunicação:	B.18.1 Software:	Para efeitos das prorrogações, entende-se por: https://travistidwell.com/jsencrypt/demo/ , https://www.devglan.com/onlinetools/rsa-encryption-decryption https://8gwifi.org/rsafunctions.jsp https://www.cryptool.org/en/
	B.18.2 Hardware:	
	B.18.3 Recursos em linha:	Vídeos do YouTube
	B.18.4 Material didático convencional:	

Parte C. Design de Experiência de Aprendizagem

C.1. Tabela de seqüências de atividades-Action-Plot-Storyboard:	Fase 1.	Introdução e exploração: Código Morse, esteganografia	
	Atividade/Tarefa	Descrição/Procedimento	Duração
	A1.1 A necessidade de criptografia — Warm up	<p>O professor discute a necessidade de proteger os dados pessoais de outras pessoas em vários momentos da vida quotidiana (por exemplo, transferência de dados privados, como nomes de utente e palavras-passe, credenciais de cartão de crédito, etc.) O perigo de acesso não autorizado a esses dados é discutido com os alunos e eles são convidados a propor métodos para proteger os seus dados de terceiros.</p> <ul style="list-style-type: none"> • Que dados pessoais gostarias de proteger? • Quem achas que quereria roubar seus dados? • Consegues pensar em numa 	10 minutos

		<p>maneira de proteger a tua comunicação de terceiros? Os alunos têm que recorrer à criptografia. Seguidamente discutem o seu uso desde os tempos antigos.</p>	
	A1.2 Métodos de criptografia: O código Morse e esteganografia	<p>Os alunos são divididos em grupos de 2. São introduzidos ao código Morse e à esteganografia. A ficha 1 é partilhada e o código Morse é discutido. Os alunos são convidados a criptografar uma mensagem usando o código Morse e descriptografar uma usando a mesma técnica e a descriptografar uma mensagem de uma imagem (steganografia).</p>	35 minutos
	Fase 2.	Exploração: Código de Braille	
	Atividade/Tarefa	Descrição/Procedimento	Duração
	A2.1 Warm up — link para o assunto discutido anteriormente	<p>Professores e alunos aprofundam a discussão sobre criptografia e descriptografia e o professor pergunta se eles podem pensar em outras maneiras de criptografar as suas mensagens.</p> <p>Em seguida, propõe o código Braille e discute se ele poderia ser usado como um método de criptografia</p>	10 minutos
	A2.2 Exploração — Código em Braille	O professor partilha a Ficha 2 e pede aos alunos para colaborar e criptografar/descriptografar mensagens usando o código Braille.	35 minutos
	Fase 3.	Exploração: Cifra de César	
	Atividade/Tarefa	Descrição/Procedimento	Duração
	A3.1 Warm up — link para discutido anteriormente	<p>Os alunos são apresentados ao método de criptografia de cifra de César e a forma como ele é usado. Uma introdução ao método pode ser encontrada aqui: https://www.youtube.com/watch?v=sMOZf4GN3oc&feature=emb_title O professor pode projetar uma maneira de usá-lo e discuti-lo com os alunos.</p>	10 minutos
	A3.2 Exploração — cifra de César	O professor partilha a Ficha 3 e apresenta os alunos ao método de cifra de César. Os alunos são convidados a	25 minutos

		colaborar para criptografar e descriptografar mensagens usando a cifra de César.	
	A3.3 Discutindo as fraquezas da criptografia simétrica	O professor e os alunos discutem os métodos de criptografia simétrica que usaram até agora para entender que os métodos podem ser decifrados, especialmente com o uso de computadores.	10 minutos
	Fase 4.	Criptografia assimétrica Troca de chaves Diffie-Hellman-RSA	
	Atividade/Tarefa	Descrição/Procedimento	Duração
	A4.1 Warm up — link para discutido anteriormente	O professor faz um resumo da aprendizagem e relembra aos alunos que o principal problema da criptografia é o envio de uma mensagem de um transmissor para um recetor sem ser capaz de ser pego-recebido por um terceiro interferindo na rota da mensagem. Salienta-se também que a principal fraqueza dos métodos de criptografia simétrica é o envio seguro da chave entre transmissor e recetor, sem ser percebido por terceiros. Os alunos são informados de que os problemas criptográficos simétricos têm sido abordados com métodos criptográficos chave pública desde a década de 1970. O professor associa a Criptografia de Chaves Públicas (PKE) ao conhecimento preexistente, apresentando exemplos como mensagens seguras (e-mail), transmissão de informações pela Internet (Secure http — https) e assinaturas digitais. Sugere-se o vídeo relevante: A Internet: As chaves públicas do & de encriptação (Code.org), https://www.youtube.com/watch?v=ZghMPWGXexs são visualizadas.	15 minutos
	A4.2 2 Exploração-Diffie-Hellman Key Exchange algoritmo e PKE	Os alunos são brevemente informados de que o método PKE foi publicado pela primeira vez em 1976 por	30 minutos

		<p>Whitfield Diffie e Martin Hellman, embora seja conhecido de uma época anterior no serviço secreto do estado. O professor partilha a Ficha 5 e apresenta os alunos ao algoritmo Diffie-Hellman Key Exchange. Dependendo da prontidão da turma, o algoritmo só pode ser demonstrado em breve, ou os alunos também podem prosseguir com o estudo do fundo matemático do método, incluído na ficha.</p> <p>A ficha 6 demonstra o método de algoritmo de criptografia assimétrica PKE com o software CrypTool. Os alunos testam o processo PKE e experimentam o método uns com os outros. Também podem usar diferentes ferramentas gratuitas e páginas da web para criar pares de chaves para criptografia-descriptografia.</p>	
C.2 Avaliação	C.2.1 feedback e reflexão dos alunos	Os alunos criam chaves RSA públicas e, em seguida, trocam mensagens criptografadas e tentam descriptografá-las. Se eles são capazes de completar o processo, considera-se que adquiriram conhecimento do método.	
C.3 Trabalho de casa/ Trabalhar com pais-família	Os alunos são convidados a aplicar o método RSA: geração de chaves, criptografia/descriptografia e troca de mensagens com os pais usando diferentes ferramentas on-line e software de simulação.		
Parte D. Informação para os Professores			
D.1 Adaptação — Diferenciação para inclusão de todos os alunos	Todos os alunos devem ser capazes de implementar o cenário.		
D.2 Extensão	D.2.1. Máquina Enigma Folha de trabalho 4: O professor introduz o uso de máquinas para criptografia com o exemplo da máquina Enigma. Estas máquinas		

eram extremamente difíceis de decifrar tanto por seres humanos como por outras máquinas. A tentativa de Alan Turing de descobrir a maneira como a máquina Enigma codifica mensagens, abriu o caminho para o desenvolvimento da ciência da computação.

Inicialmente, como a máquina Enigma funciona é demonstrada e explicada com a ajuda de vídeo.

Em seguida, os alunos praticam duas simulações de máquinas Enigma:

1. Em primeiro lugar, uma simulação simples feita com papel que simula a máquina com um rotor.

2. Em segundo lugar, uma simulação com o software educacional CryptTool.

Os alunos são convidados a colaborar para criptografar e descriptografar mensagens usando simulações de máquinas Enigma.

Vídeos sugeridos:

https://www.youtube.com/watch?v=-mdSvGUd0_c

https://www.youtube.com/watch?v=ASfAPOiq_eQ

D.2.2. Jogo educativo

Um jogo pode ser organizado para que os alunos consolidem os métodos de criptografia. Exemplos indicativos:

- 1. Os alunos são divididos em A. Os Criptografistas e B. Os Hackers. Os criptógrafos escolhem uma mensagem e um método e os hackers tentam partir o seu «código» descriptografando as mensagens. Os métodos de criptografia praticados pelos alunos são usados.**
- 2. Os alunos inventam um jogo de mistério escondido: tesouro. Especificamente, uma série de instruções para aceder ao tesouro oculto são criptografadas e tornadas acessíveis com QR-Codes colocados em diferentes lugares. Os jogadores devem descriptografar a mensagem QR-Code para descobrir onde está a próxima (a primeira é dada). Para decodificação, eles podem usar lápis de papel, os seus programas e cryptool.org. O tesouro pode ser o endereço web do filme «jogo de imitação».**
- 3. Os alunos podem construir uma sala de fuga. A fuga a partir da qual exigirá a decodificação das instruções.**

D.2.3. Reflexão sobre Criptografia

Os alunos podem:

- estudar e discutir as aplicações do método RSA. Observe como problemas de segurança de dados intratáveis são explorados (por exemplo, calculando grandes números primos).**

	<ul style="list-style-type: none"> - discutir e pesquisar criptografia e privacidade - estudar políticas e leis de criptografia. Qual é a posição dos cidadãos? <p>D.2.4. A biografia de A. Turing (filme «jogo de imitação»)</p> <p>Os alunos podem assistir ao filme «jogo de imitação», que se refere à biografia de Alan Turing e seus esforços para decifrar o algoritmo em que a máquina Enigma é baseada. Seguindo isso, os alunos discutem questões de criptografia. Além disso, temas que se estendem a partir deste, por exemplo, história, língua, educação para a paz, direitos humanos e educação sexual podem ser explorados em cooperação com outros temas como arte, história, biologia e outros temas como projetos intertemáticos.</p> <p>D.2.5. Antecedentes matemáticos do método RSA</p> <p>Os alunos são apresentados ao fundo matemático do método. A ficha 8 ilustra o método com pequenos números primos. Os alunos podem praticar, encontrar números primos computar matematicamente chaves e criptografar mensagens com o método RSA.</p> <p>Conhecimento matemático de poderes e operação mod são pré-requisitos.</p> <p>Este cenário-extensão pode ser combinado com Maths (cálculos de poderes e aplicação de regras mod).</p> <p>D.2.6. Assinaturas digitais</p> <p>O professor conecta o PKE através de exemplos de mensagens seguras (e-mail), transmissão de informações pela Internet (Secure http — https) e assinaturas digitais. A assinatura digital de documentos ou mensagens feitas usando a chave oculta para criptografia e a chave pública para descryptografia também é exibida. Levanta-se o problema da pretensão e da identificação e introduz-se o papel das autoridades de certificação. A ficha 7 ajuda os alunos a explorar o procedimento de Assinatura Digital e a praticar a fase de verificação de assinatura com o software CrypTool.</p>
D.3 Recursos	YouTube
D.4 Experiência decorrente da implementação do cenário	
D.5 Relações com outros cenários	
D.6 Comentários	

por professores	
D.7 Avaliação do cenário	[1=Muito mau — 5=Muito bom]
D.8 Referências	<p>Grimm, R., Kempe, T., Löhr, A., & Scholle, O. (2015). Informatik (em inglês). (Schöningh-Schulbuch, 1. Auflage, 4. É o Druck. Paderborn: É o Schöningh.</p> <p>Spioncamp (2019).Bergische Universität Wuppertal, consultado em https://ddi.uni-wuppertal.de/website/repoLinks/v287_Alle-Stationen-hintereinander.pdf</p>
<u>Parte E. Anexos</u>	
	<p>Ficha de trabalho 1</p> <p>Ficha de trabalho 2</p> <p>Ficha de trabalho 3</p> <p>Ficha de trabalho 4</p> <p>Ficha de trabalho 5</p> <p>Ficha de trabalho 6</p> <p>Ficha de trabalho 7</p> <p>Ficha de trabalho 8</p>

CRIPTOGRAFIA

Ficha de trabalho 1



Nome(s) do(s) aluno(s): ____

Nome do grupo: ____ Data: ____

Criptografia é a prática de usar técnicas para comunicar com segurança na Internet, ao tentar trocar mensagens. Com a criptografia, podes criptografar as tuas mensagens para evitar que terceiros tenham acesso a elas. O recetor terá que descriptografar a mensagem para lê-la.

1. Pensa numa **mensagem** que gostarias de enviar a um amigo e anota:

O que achas que deves fazer para **criptografar** a mensagem, para que ninguém mais a entenda? Escreva sua mensagem criptografada:

O que é que o teu amigo precisa saber para que ele/ela possa **descriptografar** a mensagem?

Em 1832, antes da invenção dos telefones, o americano Samuel Morse inventou um dispositivo chamado **telégrafo Morse**, que foi usado para transmitir mensagens em longas distâncias. Uma rede de cabos foi gradualmente estabelecida em todo o país. Os cabos não transmitiram som, mas impulsos elétricos de longa ou curta duração, de acordo com a tabela abaixo.

A	● █	U	● ● █
B	█ ● ● ●	V	● ● ● █
C	█ █ █ ●	W	● █ █ █
D	█ ● ●	X	█ ● ● █
E	●	Y	█ ● █ █
F	● ● █ ●	Z	█ █ ● ●
G	█ █ ●		
H	● ● ● ●		
I	● ●		
J	● █ █ █ █		
K	█ ● █ █		
L	● █ █ ● ●		
M	█ █ █		
N	█ █ ●		
O	█ █ █ █ █		
P	● █ █ █ ● ●		
Q	█ █ █ ● █ █		
R	● █ █ ●		
S	● ● ●		
T	█		
		1	● █ █ █ █ █
		2	● ● █ █ █ █
		3	● ● ● █ █ █
		4	● ● ● ● █ █
		5	● ● ● ● ●
		6	█ ● ● ● ●
		7	█ █ ● ● ● ●
		8	█ █ █ ● ● ● ●
		9	█ █ █ █ ● ● ● ●
		0	█ █ █ █ █ █ █

Entre as letras houve uma breve pausa e entre palavras uma mais longa. Sinais de luz também podem ser usados para a transmissão do código Morse.

2. Com base na tabela acima, podes entender a seguinte mensagem?

— ● — — — ● ● ● ● — — — ● ● ● ● — — — ● ● ● ● — — — ● ● ● ●

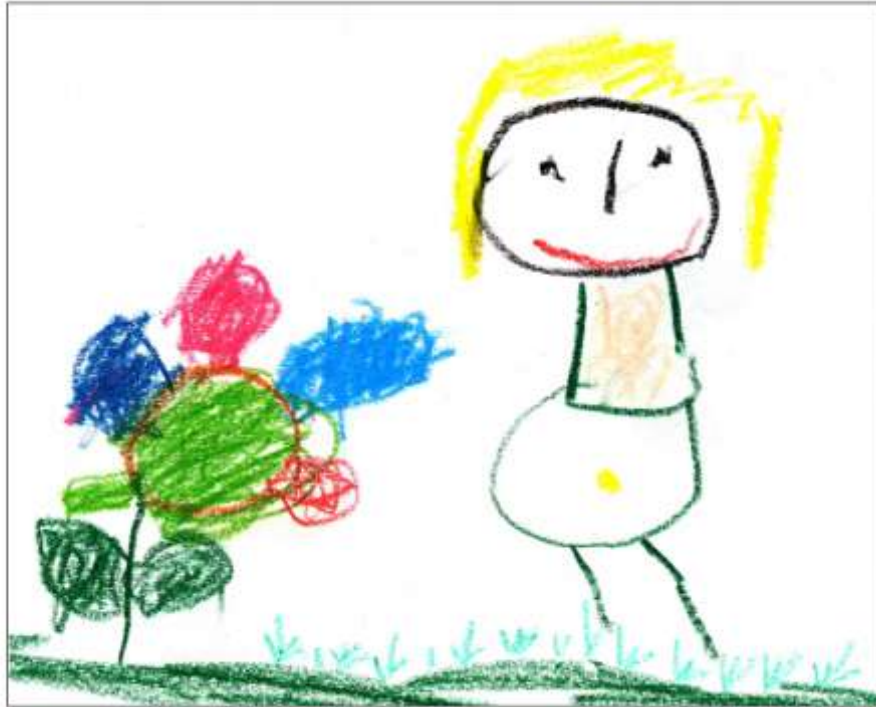
—

3. Qual é o sinal Morse para **SOS**? (Este é o sinal de ajuda internacional.)

—

4. Em grupos de dois, tente enviar uma mensagem para outro grupo de teus colegas piscando uma lente para representar os sinais Morse.

Outra maneira de transmitir mensagens é escondendo-as, por exemplo, em imagens. Este método é chamado de **esteganografia**. Se olhares para a imagem abaixo, podes não notar que há uma mensagem escondida nela. Mas a imagem contém uma mensagem no código Morse. Os caules longos e curtos da erva são os traços e pontos, respetivamente, enquanto cada tufo é uma letra.



Spioncamp (2019).Bergische Universität Wuppertal, consultado em https://ddi.uni-wuppertal.de/website/repoLinks/v287_Alle-Stationen-hintereinander.pdf

5. Consegues encontrar a mensagem secreta? ____
6. Como desenharias uma imagem para criptografar uma mensagem para seu amigo?

Muito bem!

CRIPTOGRAFIA

Ficha de trabalho 2



Nome(s) do(s) aluno(s): ____

Nome do grupo: ____ Data: ____

CÓDIGO DE BRAILLE

Louis **Braille** nasceu em França em 1808 e ficou cego após um acidente aos 3 anos de idade. Aos 14 anos, desenvolveu um sistema que as pessoas cegas podem ler. Esse sistema consiste em pontos levantados que alguém pode sentir com os dedos. Os sinais de Braille estão representados na Tabela 1.

Mesa1. Sinais em Braille

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
⠒	⠒	⠒	⠒	⠒	⠒	⠒	⠒	⠒	⠒	⠒	⠒	⠒
1	2	3	4	5	6	7	8	9	0			
⠒	⠒	⠒	⠒	⠒	⠒	⠒	⠒	⠒	⠒			

Palavras e números são decifrados usando sinais diferentes antes deles. Com estes sinais, o leitor sabe se o que se segue é uma letra, ou um número:

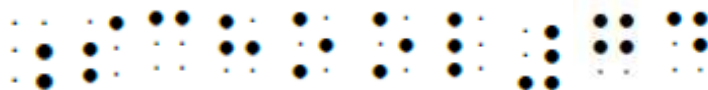


quando uma **palavra** segue, ou



quando um **número** segue.

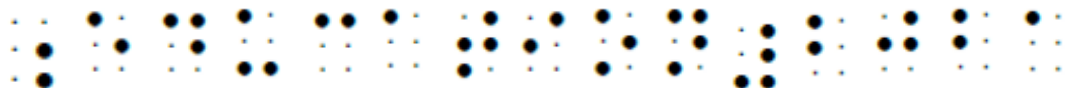
Por exemplo:



é o código para a **Escola**

74.

1. Podes descriptografar a seguinte mensagem?



2. Usando a ponta do lápis, tenta codificar o teu nome e idade, pontuando no formulário abaixo.

Usa a tabela de sinais Braille para ver que sinal corresponde a cada letra.

The image shows a large rectangular grid consisting of 10 rows and 15 columns. Each cell in the grid contains a 2x3 arrangement of small circles, representing a Braille dot pattern. The circles are arranged in two vertical columns of three circles each. This grid is intended for students to use a pencil to mark or code their names and ages by filling in specific dots.

Pede ao teu colega para ler o que escreveu com os olhos fechados, por toque.

BOM TRABALHO!



CRIPTOGRAFIA

Ficha de trabalho 3



Nome(s) do(s) aluno(s): ____

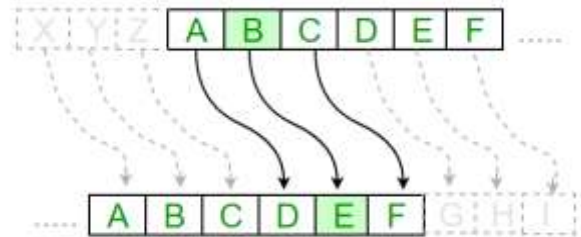
Nome do grupo: ____ Data: ____

CIFRA DE CÉSAR

A **cifra** de César (ou código César) é um dos mais famosos e fáceis sistemas de criptografia, usado por Júlio César (100-44 a.C.) para as suas mensagens. De acordo com este método, cada letra de uma mensagem é substituída por outra letra, um número fixo de posições no alfabeto. O número de posições é definido pela **chave**, ou deslocação de César, **por exemplo**, deslocação para a esquerda de 3 ou para a direita de 4, etc.



Método: Primeiro, tens que escolher um número de 1 a 26, que terás que compartilhar com o recetor. Isso é chamado de **chave** e o recetor irá usá-lo para descriptografar a tua mensagem.



Precisas escrever o alfabeto em duas linhas: primeiro as letras de A a Z e, em seguida, cada letra substituída, começando pela letra na posição logo após a chave.

Por exemplo, no caso de a chave ser 4, a letra A será substituída por E (a letra após a quarta), a letra B será substituída por F e assim por diante. As quatro primeiras letras (ABCD) seguem logo após Z.

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

1. Com base no acima referido, usa a chave de cifra de César 4, a palavra **ANNA** será criptografada para **ERRE**. Podes criptografar a seguinte mensagem usando o método acima (Caesar cifra chave 4)?

A CRIPTOGRAFIA É FANTÁSTICA: ____

2. Com base no acima referido, podes descriptografar a seguinte mensagem?

GSQTYXIVW VSGO: ____

Variação:

O método apresentado pode ser facilmente variado, de modo que foi encontrada uma variação do mesmo. O remetente e o recetor terão de chegar a acordo sobre uma **palavra-chave**, por exemplo, a **palavra DODEKANISOS** (um complexo insular na Grécia). A palavra-chave está escrita no início do alfabeto (as mesmas letras não são repetidas). Em seguida, substituis cada uma das outras letras pelo resto das letras do alfabeto, começando pela última letra da palavra-chave. Vê o exemplo abaixo:

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

Esta tabela será usada para codificação e decodificação.

3. Com base na variação acima, se usares a chave de cifra César **DODEKANISOS**, agora podes criptografar a seguinte mensagem?

A CRIPTOGRAFIA É FANTÁSTICA: ____

4. Também com base no acima referido, podes agora descriptografar a seguinte mensagem?

GSQTYXIVW VSGO: ____

5. Percebes alguma diferença?

ATIVIDADE:

Em grupos de dois, concorda em uma palavra-chave e cria a tabela correspondente abaixo usando a cifra de César:

	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
Substituído por:																										

Envia uma mensagem criptografada para o outro. Conseguiste descriptografar a mensagem que recebeste?

Agora podes criptografar e descriptografar mensagens usando o método de cifra César!

Trabalhos de casa: Por que não tentas fazer o teu próprio disco de cifra?



Muito bem!

ENIGMA MÁQUINA DE CRIPTOGRAFIA

Ficha de trabalho 4



Nome(s) do(s) aluno(s): ____

Nome do grupo: ____ Data: ____

Enigma máquina de criptografia

A máquina «Enigma» foi inventada em 1923 pelo engenheiro alemão Arthur Scherbius. O seu nome vem da palavra grega «enigma». Esta máquina foi originalmente usada para fins comerciais, estava comercialmente disponível antes da Segunda Guerra Mundial, mas foi modificada em muitas variantes e usada para criptografar ordens do exército alemão na Segunda Guerra Mundial. Relatos históricos conferem que Alan Turing, um funcionário da contra-inteligência inglesa, conseguiu quebrar o código. «O jogo de imitação» é um filme que se refere a esses eventos e ao trágico destino de Turing.

Método de Encriptação/Decodificação

Em seguida, uma simulação simplificada do motor é apresentada. Consiste em duas rodas, uma interna e uma externa. A roda interna gira enquanto a roda externa permanece fixa.

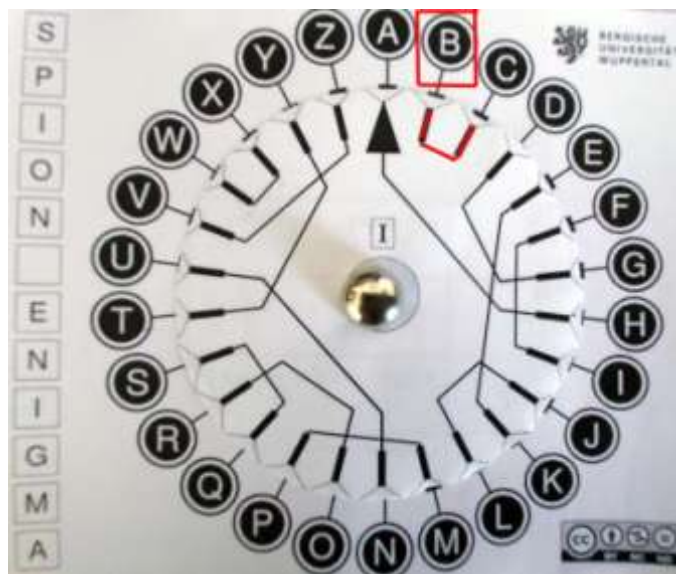
Pré-requisito: Tanto o remetente quanto o destinatário devem possuir a máquina!

Instruções de encriptação:

- Coloca a seta para apontá-la para a chave.
- Em seguida, localiza a letra da mensagem que queres criptografar.
- Segue o link. Esta é a primeira letra encriptada.
- Em seguida, vira a seta para a direita para que ela aponte para uma letra para baixo (apontando para a letra seguinte da tecla no sentido horário).
- Segue o link. Esta é a segunda carta encriptada.
- Faz o mesmo para que todas as letras da mensagem sejam criptografadas. Não te esqueças de girar a seta uma letra para baixo cada vez no sentido horário.

Exemplo

1. Foi acordada uma carta-chave. Por exemplo, «A». A seta grande da roda interna deve apontar para a letra chave, que é a letra «A».
2. Se, por exemplo, quisermos encriptar a palavra «B»
3. A seta grande na roda interior deve indicar a chave, ou seja, «A».
4. Para criptografar a primeira letra B, vê o seu mapeamento. A letra B corresponde à letra C. C é, por conseguinte, a primeira letra cifrada.



5. Para criptografar a próxima letra, gira a seta grande uma posição para baixo no sentido horário. Deves agora apontar para B.



6. Para criptografar a letra Y notar que Y está conectado a X. A segunda letra criptografada é, portanto, X.

7. Gira a seta mais uma posição no sentido horário. Deves agora apontar para a letra C.



8. Para criptografar a letra E notar que E está associado a D. A terceira letra criptografada é, portanto, D.

De acordo com o procedimento acima descrito, a **palavra** BsE foi encriptada no texto cifrado **CXD**.

Instruções de descodificação:

- Coloca a seta apontando para a letra que é a chave.
- Em seguida, localiza a letra que desejás descriptografar.
- Sigue o link. Esta é a primeira letra da mensagem encriptada.
- Em seguida, vira a seta uma letra para baixo (apontando para a próxima letra da chave) no sentido horário.
- Sigue o link. Esta é a segunda carta encriptada.
- Faz o mesmo para todas as letras da mensagem. Não te esqueças de girar a seta uma letra de cada vez no sentido horário.

Construção de rotor

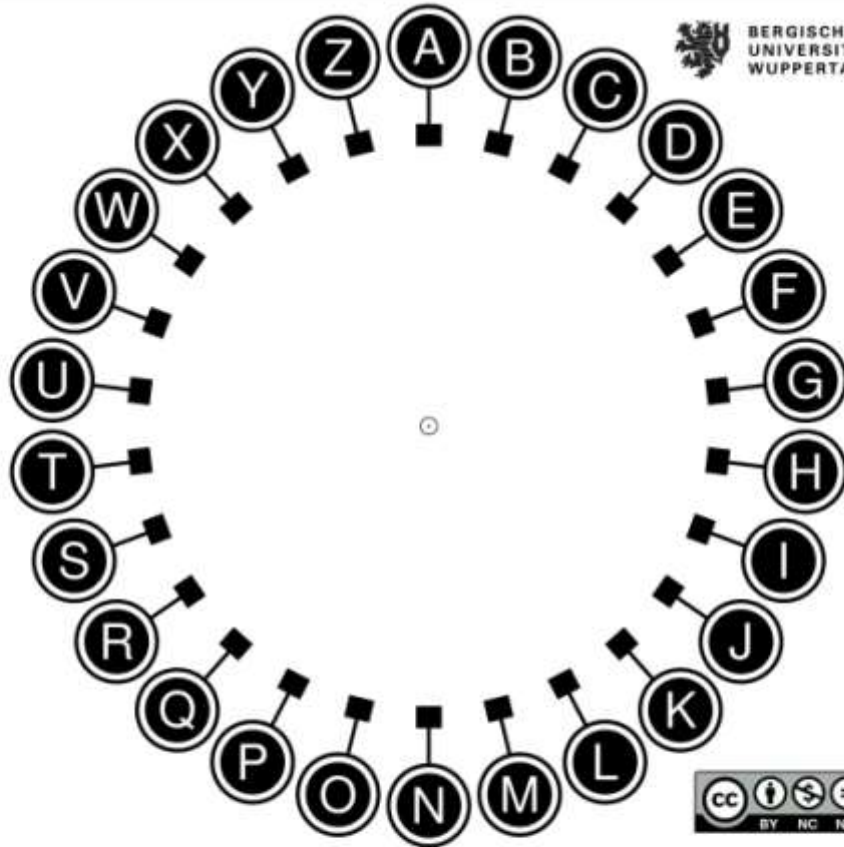
Imprime os dois discos do rotor.

Usa um suporte de CD/DVD. Neste caso, corta o círculo cinzento interno.

Alternativamente, usa um  (pino de desenho da bolha)

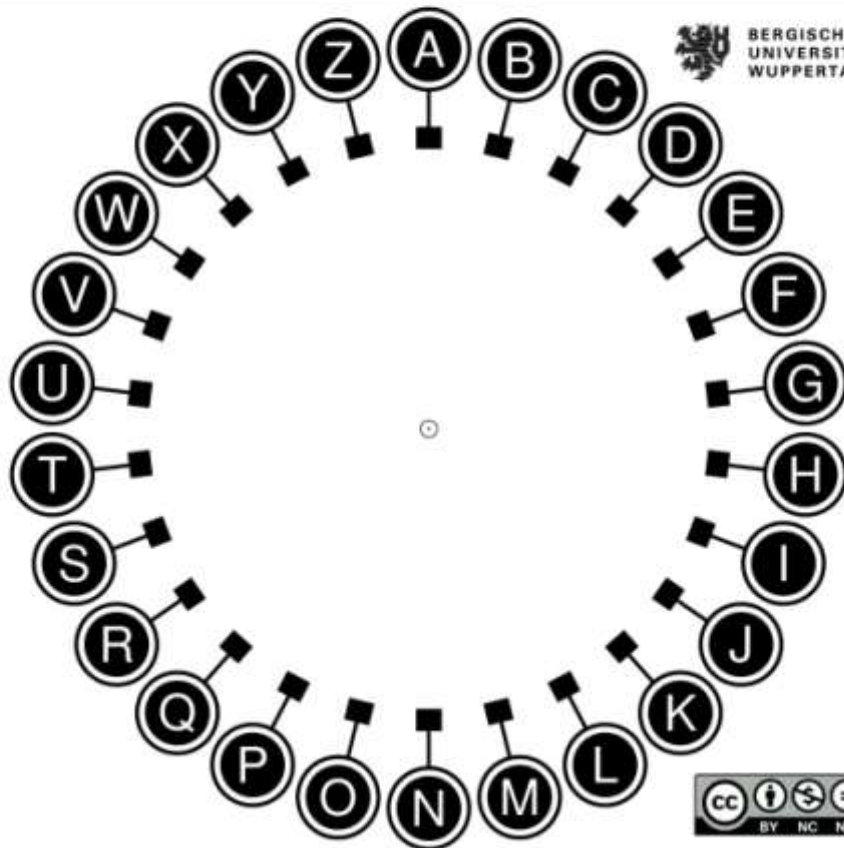
S
P
I
O
N

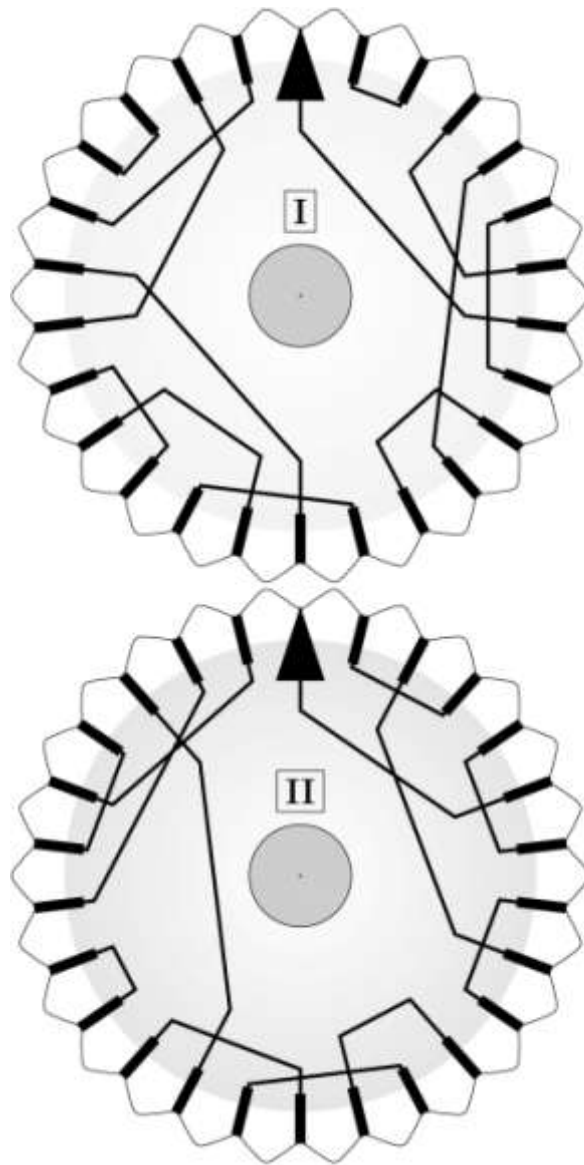
E
N
I
G
M
A



S
P
I
O
N

E
N
I
G
M
A





Spioncamp (2019).Bergische Universität Wuppertal, consultado em https://ddi.uni-wuppertal.de/website/repoLinks/v287_Alle-Stationen-hintereinander.pdf

Extensão da folha de trabalho 4

Atividade 1

Simulação com rypToolC

A própria Máquina Enigma usa três rotores desse tipo, que são de fato cilindros.

Para uma introdução à operação da Máquina Enigma, vê os dois vídeos sugeridos aqui.

https://www.youtube.com/watch?v=-mdSvGUd0_c

https://www.youtube.com/watch?v=ASfAPOiq_eQ

Vamos tentar um exemplo de simulação que está perto da realidade.

Faz o download da ferramenta de simulação cryptool1.4.41

<https://www.cryptool.org/de/cryptool1>

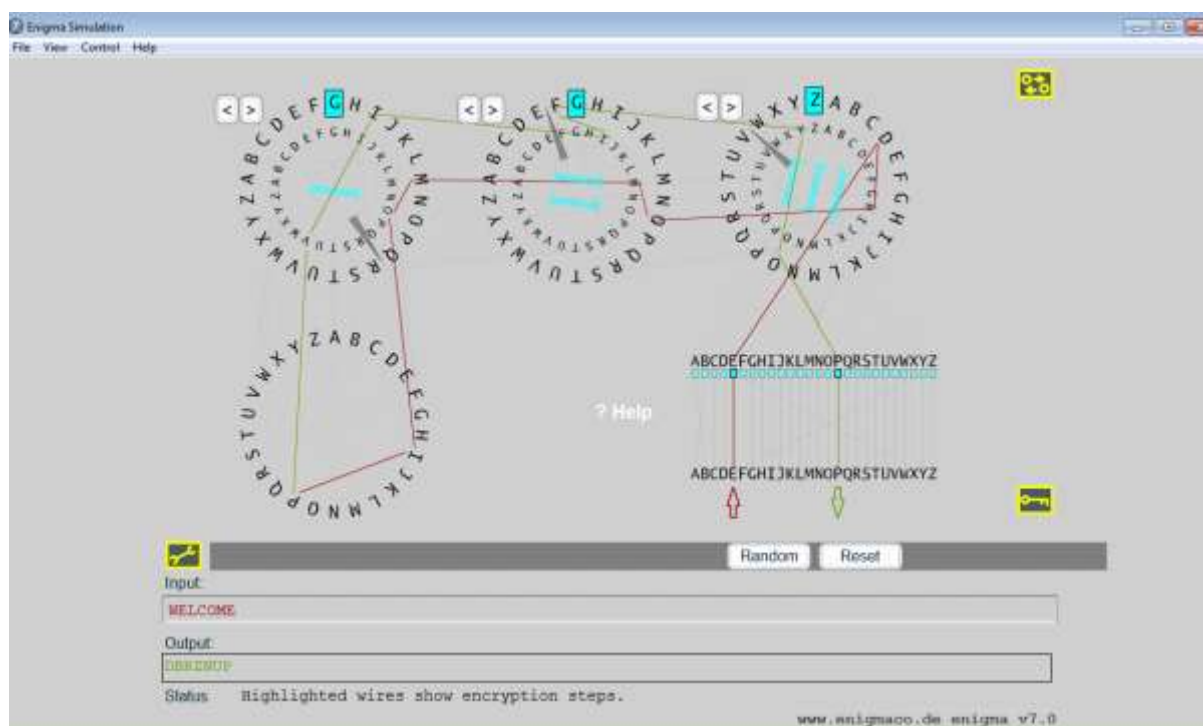
A partir do [esite](http://www.cryptool-online.org) www.cryptool-online.org.

Abra o menu e escolhe *Individ. Procedimentos/Visualização de algoritmos/Enigma*

Como posso criptografar um texto simples?

- O primeiro passo é constituir uma chave. Neste caso, uma chave consiste em duas partes.
- O segundo passo é decidir quais os pares de letras que devem ser trocados ou trans posicionados no plugboard, por exemplo, A a B e também F a X. Observa que as configurações do rotor no início da entrada de texto devem ser escolhidas para os três rotores, por exemplo, F-E-S.
- O terceiro passo é «REESTABELECEER» a máquina inteira para o «estado inicial», clicando em «RESET». A máquina está agora pronta para criptografar a primeira amostra.
- O quarto passo é arrastar o pequeno círculo amarelo por baixo de A para B e soltar o botão do rato. Assim, A e B foram trocados. Por favor, troca F e X da mesma forma.
- O quinto passo é definir as configurações do rotor mencionadas pressionando os botões «<» ou «>» acima de cada rotor específico. Cada clique do rato coloca um rotor uma posição para a frente na direção indicada.

- Finalmente, a palavra «bem-vindo» é digitada. A linha «Output:» deve mostrar o texto cifrado i.e.«DBRZNUP». O texto criptografado parece completamente diferente em comparação com o original, a única semelhança é o mesmo número de letras.



Atividade 2

Encriptação — Descrição com Simulador de Enigma-máquina (CryptTool)

Os alunos são divididos em dois grupos: uma encriptação e um grupo de decodificação. Usando o software CryptTool, cada grupo, respectivamente, encripta ou descriptografa mensagens depois de ter inicialmente acordado sobre os valores que os rotores terão e duas transposições de letras.



Corte em torno das bordas das três caixas de texto abaixo.

Memorando secreto para criptografar e descriptografar grupos

1. Defina os valores do rotor (A-p, alfabeto inglês)
 - rotor 1=
 - rotor 2=

rotor3=

2. Definir a alternância de letras

... → ...

**Para ser mantido
em segredo**

Instruções para o grupo de encriptação

Abrir CrypTool (*Individ. Procedimentos/Visualização de algoritmos/Enigma*).

Definir os rotores conforme acordado

Definir as transposições de letras

Digitar o texto para criptografar

Enviar o texto criptografado para o seu grupo de decodificação

Instruções para o grupo de decodificação

Abrir CrypTool (*Individ. Procedimentos/Visualização de algoritmos/Enigma*).

Definir os rotores conforme acordado

Definir as transposições da carta

Digitar o texto para descriptografar

Verificar a mensagem descriptografada

Encriptação assimétrica: Diffie- Hellman algoritmo

Ficha 5



Nome(s) do(s) aluno(s): ____

Nome do grupo: ____ Data: ____

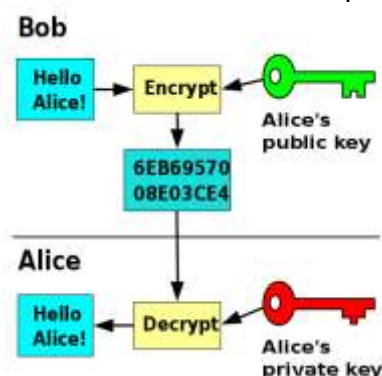
Diffie- algoritmo Hellman

Método

A criptografia floresceu quando se tornou possível para o remetente criptografar a mensagem com uma chave secreta, enviar outra chave pública para o destinatário e permitir que o destinatário descriptografe a mensagem usando apenas a chave pública. Qualquer terceiro que tenha acesso à chave pública não pode descriptografar a mensagem! É por isso que tal processo foi chamado de **criptografia assimétrica**: Mas isso é possível?

Por muitos anos foi considerado impossível trocar uma chave que, mesmo que um terceiro soubesse, não poderia decodificar a mensagem criptografada. Em 1976, Martin Hellman, Whitfield Diffie e Ralph Merkle desenvolveram o algoritmo de Diffie-Hellman que permite que duas partes concordem em uma chave, que mesmo um terceiro não saberia como descriptografar a mensagem.

O diagrama abaixo (wikimedia.org) ilustra os passos para enviar uma mensagem. Duas chaves diferentes para criptografia e decodificação são usadas. Cada utente fornece livremente a sua chave pública para enviar mensagens criptografadas que só ele pode descriptografar com a sua chave secreta-privada.



Vamos explicá-lo com um exemplo: Bob e Alice concordam em usar um número de chave. Um terceiro Ismene pode obter (por escutar!) o número da chave pública.




Bob e Alice usam a chave para codificar e decodificar mensagens que são trocadas, não secretamente, Ismene pode vê-las, mas não pode criptografá-las.

Bob e Alice aparentemente concordam no início em usar um **número** primo p . Eles também devem concordar com um número **natural**, digamos c . Deve $c < p$.

Bob então escolhe um inteiro positivo α (menos de p) que ele mantém em segredo.




Alice também escolhe um inteiro positivo β (menos de p) que ela mantém em segredo.

Bob e Alice podem calcular a **chave «K»** com base nas fórmulas dadas na tabela abaixo. Ismene poderia saber p , c , A e B , mas não pode calcular a chave K porque ela não conhece α e β .

Espaço privado	Espaço público	Espaço privado
Bob 	Ismene 	Alice 
<div style="border: 1px solid black; padding: 2px; width: fit-content; margin-bottom: 5px;">escolha α, $\alpha < p$</div> <div style="border: 1px solid black; padding: 2px; width: fit-content; margin-bottom: 10px;">computar $A=c^\alpha \text{ mod } p$</div> <div style="border: 1px solid black; padding: 2px; width: fit-content; margin-bottom: 10px;">B ←</div> <div style="border: 1px solid black; padding: 2px; width: fit-content;">computar $\square=B^\alpha \text{ mod } p$</div>	<div style="border: 1px solid black; padding: 2px; width: fit-content; margin-bottom: 10px;">determinar p και c</div> <div style="border: 1px solid black; padding: 2px; width: fit-content; margin-bottom: 10px;">A</div> <div style="border: 1px solid black; padding: 2px; width: fit-content; margin-bottom: 10px;">B</div>	<div style="border: 1px solid black; padding: 2px; width: fit-content; margin-bottom: 5px;">escolha β, $\beta < p$</div> <div style="border: 1px solid black; padding: 2px; width: fit-content; margin-bottom: 10px;">computar $B=c^\beta \text{ mod } p$</div> <div style="border: 1px solid black; padding: 2px; width: fit-content; margin-bottom: 10px;">A</div> <div style="border: 1px solid black; padding: 2px; width: fit-content;">computar $\square=A^\beta \text{ mod } p$</div>

Referência: Spioncamp (2019). Bergische Universität Wuppertal, consultado em https://ddi.uni-wuppertal.de/website/repoLinks/v287_Alle-Stationen-hintereinander.pdf

Aqui está um exemplo com números

Espaço privado	Espaço público	Espaço privado
Bob 	Ismene 	Alice 
<div style="border: 1px solid black; padding: 2px; width: fit-content; margin-bottom: 5px;">escolha α, $\mu\epsilon \alpha < p$</div> <div style="text-align: center;">$\alpha=4$</div> <div style="border: 1px solid black; padding: 2px; width: fit-content; margin-bottom: 10px;">computar $A=c^\alpha \text{ mod } p$</div> <div style="text-align: center;">$A=5^4 \text{ mod } 17$</div> <div style="text-align: center;">$A= 625 \text{ mod } 17$</div> <div style="text-align: center;">$A=13$</div> <div style="border: 1px solid black; padding: 2px; width: fit-content; margin-bottom: 10px;">B ←</div> <div style="border: 1px solid black; padding: 2px; width: fit-content;">computar $\square=B^\alpha \text{ mod } p$</div>	<div style="border: 1px solid black; padding: 2px; width: fit-content; margin-bottom: 10px;">$p=17$ και $c=5$</div> <div style="border: 1px solid black; padding: 2px; width: fit-content; margin-bottom: 10px;">A</div> <div style="border: 1px solid black; padding: 2px; width: fit-content; margin-bottom: 10px;">B</div>	<div style="border: 1px solid black; padding: 2px; width: fit-content; margin-bottom: 5px;">escolha β, $\beta < p$</div> <div style="text-align: center;">$B=7$</div> <div style="border: 1px solid black; padding: 2px; width: fit-content; margin-bottom: 10px;">computar $B=c^\beta \text{ mod } p$</div> <div style="text-align: center;">$B=5^7 \text{ mod } 17$</div> <div style="text-align: center;">$B= 78.125 \text{ mod } 17$</div> <div style="text-align: center;">$B=10$</div> <div style="border: 1px solid black; padding: 2px; width: fit-content; margin-bottom: 10px;">A</div> <div style="border: 1px solid black; padding: 2px; width: fit-content;">computar $\square=A^\beta \text{ mod } p$</div>

$\square = 10^4 \text{ mod } 17$ $\square = 10.000 \text{ mod } 17$ $\square = 4$		$\square = 13^7 \text{ mod } 17$ $\square = 62.748.517 \text{ mod } 17$ $\square = 4$
---	--	---

A chave que Bob e Alice usarão é 4. Esta chave pode ser usada para criptografar e descriptografar mensagens.

Podes usar a calculadora do Windows em visão científica para calcular poderes e divisões com mod.




Pergunta: É possível para Ismene encontrar a chave K?

Resposta: Sim, tentando combinações de números de 0 a p.

No caso de p é pequeno, como aqui, encontrar a chave é fácil. Mas se os números a serem escolhidos são grandes, então é impossível mesmo com os computadores mais rápidos disponíveis para encontrar a chave através de testes de número.

Atividade 1

Compute key \square aplicando o algoritmo Diffie- Hellman para números $p=7$ και $c=4$

Espaço privado	Espaço público	Espaço privado
Bob 	Ismene 	Alice 
\square escolha $\alpha, \alpha < p$ $\alpha = \dots$ \square computar $A = c^\alpha \text{ mod } p$ $A = \dots$ $A = \dots$ $A = \dots$	\square $p=7$ και $c=4$	\square escolha $\beta, \beta < p$ $B = \dots$ \square computar $B = c^\beta \text{ mod } p$ $B = \dots$ $B = \dots$ $B = \dots$
\square $B \leftarrow$	\square A \square B	\square A
\square computar $\square = B^\alpha \text{ mod } p$ $\square = \dots$ $\square = \dots$ $\square = \dots$		\square computar $\square = A^\beta \text{ mod } p$ $\square = \dots$ \dots $\square = \dots$

Encriptação assimétrica: Procedimento PKE (RSA)

Ficha de trabalho 6



Nome(s) do(s) aluno(s): ____

Nome do grupo: ____ Data: ____

Atividade 1

O funcionamento do algoritmo RSA será demonstrado em duas partes com o CrypTool:

- A geração de uma chave RSA,
- A encriptação e descodificação de mensagens

De acordo com a RSA, a comunicação criptografada entre duas partes exige:

- uma chave pública, que consiste em um par de números (N, e)
- uma chave retrête, que também consiste em um par de números e que permanecem secretas (N, d)

Geração de chaves RSA

Para criar uma chave RSA seleciona **Procedimentos individuais \ RSA Cryptosystem \ Demonstração RSA.**

Para a chave RSA, são necessários dois números primos diferentes, p e q.

Digita dois números primos nos campos **Número Prime p** e **Número Prime q**, ou gera dois números primos aleatórios, p e q.

Como exemplo, desejamos gerar uma chave RSA aleatória de 256 bits. Para fazer isso, clica no **botão Gerar números primos...** Semelhante à seleção de menu **Indiv. Procedimentos \ Demonstração RSA \ Gerar Números Prime...**, uma caixa de diálogo abre-se na qual gerar números primos p e q. Para o número primo p, escolha $2^{127}+2^{126}$ como **limite inferior** e 2^{128} como **limite superior**, e ativa para o intervalo de valores o botão de rádio, **Ambos são iguais**. Quando clicas em **Gerar números primos**, dois números primos p e q de comprimento de bit entre 127,5 e 128 são gerados. Quando p e q são multiplicados juntos, o resultado é módulo de RSA N de comprimento de bit maior que $2 \cdot 127,5 = 255$, ou seja, uma chave RSA de 256 bits.

Os números primos podem ser gerados com a frequência que quiserem. Se clicares no botão de pressão **Aplicar primos**, os números primos p e q são passados para a caixa de diálogo RSA. Ao mesmo tempo RSA módulo N é calculado, também a função Euler phi phi(N).

O próximo passo é determinar a [chave RSA pública](#) e, um número que é coprímo para phi(N). Às vezes não é fácil encontrar tal número. Por esta razão, oferecemos uma pequena dica: o número e = $2^{16}+1 = 65537$ (= 10000000000000001 binário) é na prática sempre coprímo para phi(N).

Clica no botão de comando **Atualizar parâmetros** e a [chave secreta RSA](#) d será calculada a partir do número e.

Agora podes criptografar e descriptografar mensagens.

2. Encriptação ou decodificação de mensagens utilizando o par de chaves RSA

Depois de teres gerado a chave RSA, podes criptografar e descriptografar mensagens.

Vê um exemplo abaixo:

The screenshot shows the 'RSA Demonstration' window. It contains the following sections:

- Options:** Two radio buttons. The first is selected: 'Choose two prime numbers p and q. The composite number N = pq is the public RSA modulus, and phi(N) = (p-1)(q-1) is the Euler totient. The public key e is freely chosen but must be coprime to the totient. The private key d is then calculated such that d = e^-1 mod phi(N)'. The second option is 'For data encryption or certificate verification, you will only need the public RSA parameters: the modulus N and the public key e.'
- Prime number entry:** Two input fields for 'Prime number p' (value: 5) and 'Prime number q' (value: 7). A 'Generate prime numbers...' button is to the right.
- RSA parameters:** Four input fields: 'RSA modulus N' (35, labeled '(public)'), 'phi(N) = (p-1)(q-1)' (24, labeled '(secret)'), 'Public key e' (2^16+1), and 'Private key d' (17). An 'Update parameters' button is to the right.
- RSA encryption using e / decryption using d [alphabet size: 27]:** A section with 'Input as' radio buttons (selected: 'text', unselected: 'numbers') and an 'Alphabet and number system options...' button. Below are three text boxes: 'Input text' containing 'WELCOME', a note 'The input text will be separated into segments of Size 1 (the symbol '#' is used as separator)', and 'Numbers input in base 10 format' containing '23#05#12#03#15#13#05'. Below these is the formula 'Encryption into ciphertext c[j] = m[j]^e (mod N)' and the resulting ciphertext '19#10#17#33#15#13#10'.
- Buttons:** 'Encrypt', 'Decrypt', and 'Close' buttons are at the bottom.

Atividade 2

Os alunos são divididos em dois grupos (um grupo criptografa, o outro descriptografa).

Etapa 1

Atividade para ambos os grupos: a criação de pares de chaves públicas.

Etapa 2

O grupo Criptografia criptografa uma mensagem.

Etapa 3

A mensagem criptografada é enviada para o grupo de decodificação.

Etapa 4

O grupo de decodificação descriptografa a mensagem criptografada.

Atividade 3

O funcionamento do algoritmo RSA será demonstrado em alternativa noutro software de simulação:

- <https://travistidwell.com/jsencrypt/demo/>,
- <https://www.devglan.com/online-tools/rsa-encryption-decryption>
- <https://8gwifi.org/rsafunctions.jsp>

Os alunos podem:

1. Criar chaves RSA
2. Criptografar/Descriptografar e trocar mensagens

Encriptação assimétrica: Assinatura digital — Ficha de trabalho 7



Nome(s) do(s) aluno(s): ____

Nome do grupo: ____ Data: ____

Método

Criar e verificar assinatura digital

A utilização da assinatura digital envolve dois procedimentos: a criação da assinatura e a sua verificação. Em seguida, as ações do remetente e do destinatário são descritas passo a passo, a fim de facilitar a compreensão do mecanismo de criação digital e de assinatura de verificação.

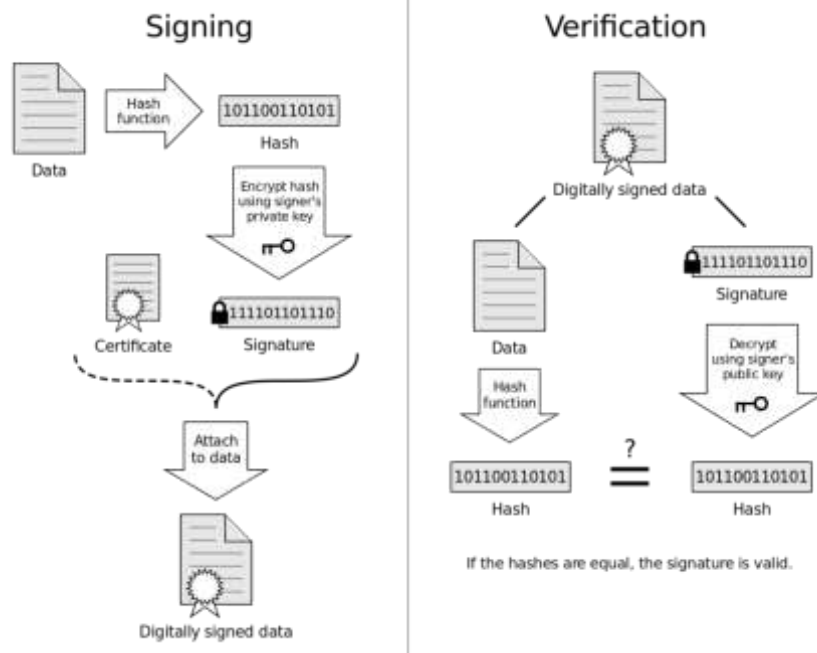
Remetente

1. O remetente usando um algoritmo de hash (Hash unidirecional) cria o resumo da mensagem (digerir mensagem) a ser enviado. Uma série de dígitos de um determinado comprimento será gerada independentemente do tamanho da mensagem.
2. O remetente criptografa o acima usando a chave. A assinatura digital é assim produzida e consiste numa série de dígitos.
3. O resumo encriptado (assinatura digital) é anexado ao texto e a mensagem assinada digitalmente é transmitida através da rede (note-se que a mensagem pode ser encriptada pelo seu remetente com a utilização da chave pública).

Destinatário

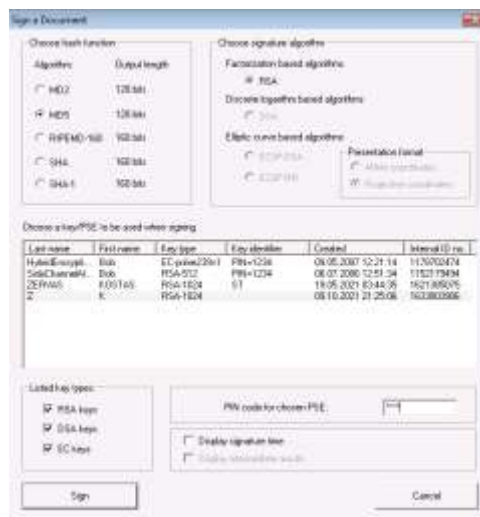
1. O destinatário separa a assinatura digital da mensagem.
2. O destinatário cria o resumo da mensagem aplicando o mesmo algoritmo de hash que o remetente à mensagem recebida.
3. A assinatura digital é descriptografada usando a chave pública do remetente e um resumo da assinatura digital é produzido.
4. A mensagem e os resumos digitais são comparados e, se forem considerados iguais, significa que a mensagem recebida pelo destinatário está intacta. Se, por outro lado, eles são considerados diferentes, então a mensagem enviada foi submetida a mudanças.

O diagrama abaixo ilustra o processo de assinatura (assinatura digital)



Atividade: Pratica o processo de Assinatura Digital com o CrypTool.

1. O par de chaves públicas é criado a partir do menu: Assinatura digital/PKI/Gerar chaves (além disso, PIN é necessário)
2. Em seguida, o texto para criptografia é digitado ou o arquivo a ser criptografado é carregado.
3. O comando Digital Signatures/Sign Document é então escolhido. É necessário especificar
 - a. O algoritmo da função Hash (MD2, MD5 etc.)
 - b. O algoritmo de assinatura (RSA, etc.)
 - c. O par de chaves públicas
4. Assinar



5. Salva o arquivo produzido e envia para os destinatários. Este ficheiro contém:
 - a. A assinatura
 - b. O conteúdo a ser enviado

A equipa que receberá o arquivo contendo a assinatura e o conteúdo pode confirmar a assinatura (que garante que o texto atingiu intacto), escolhendo Digital/assinatura/PKI/Verify Signature

Encriptação assimétrica: Procedimento RSA — Antecedentes matemáticos



Ficha de trabalho 8

Nome(s) do(s) aluno(s): ____

Nome do grupo: ____ Data: ____

Método

O quadro seguinte mostra o procedimento RSA (conhecimento prévio: números primos, poderes)

1	Escolher dois números primos p e q	$p=3$ και $q=11$
2	Computar $N=p \cdot q$	$N=3 \cdot 11=33$
3	Calcular $r=(p-1) \cdot (q-1)$	$R=(3-1) \cdot (11-1)=2 \cdot 10=20$
4	Escolher um número e de tal forma que e e r não têm divisor comum	$e=7$ $e=5$ $r=20$ não têm divisor comum
5	Determinar o número d como $e \cdot d \bmod r=1$	$D=23$ $7 \cdot 23 \bmod 20=161 \bmod 20=1$
6	Publicar e , manter em segredo d	Chave pública $(p,e)=(33, 7)$ Chave privada $(N, d)=(33, 23)$
7	Encriptar a mensagem M : Computar $C=M^e \bmod N$	Por exemplo, $M=2$ $C=2^7 \bmod 33=128 \bmod 33=29$
8	Decifrar C Computar $M=C^d \bmod N$	Decifrar $C=29$ $M=29^{23} \bmod 33=2$ $M=2$

A filosofia do algoritmo é que cálculos em uma direção são fáceis, mas muito mais difíceis em outra direção. O método RSA baseia-se no fato matemático de que é fácil calcular o produto de dois números primos, mas é muito difícil fatorizar este produto, ou seja, encontrar os fatores a partir dos quais ele é formado. Neste caso (se nos limitarmos a pequenos números, é possível com testes calcular a chave d com testes).

Mas quando os números são grandes, a ordem de 200-300 dígitos é extremamente demorada, mesmo com os computadores mais rápidos para calcular d . É «computacionalmente impossível» calculá-lo. A factorização de pequenos números, por exemplo, no nosso exemplo de 33, é fácil. Encontramos «à mão que 33»

produzido multiplicando 3 por 11. Existem também aplicações que podem factorizar números, como a indicada no link <https://www.mathpapa.com/factoring-calculator/>

1	Escolher dois números primos p e q	p= και q=
2	Computar $N=p \cdot q$	N=
3	Calcular $r=(p-1) \cdot (q-1)$	R=
4	Escolher um número e de tal forma que e e e r não têm divisor comum	e=
5	Determinar o número d como $e \cdot d \bmod r=1$	D=
6	Publicar e e, manter em segredo d	Chave pública (N, e)= Chave privada (N, d)=
7	Encriptar a mensagem M: Computar $C=M^e \bmod N$	Por exemplo, $C=2$
8	Decifrar C Computar $M=C^d \bmod N$	Decifrar C

Atividade: Antecedentes matemáticos do método RSA

Escolhe dois números primos p e q e depois aplica o Método RSA.

Podes usar a calculadora do Windows em visão científica para calcular poderes e divisões com mod ou aplicar regras de mod.

Regras de modificação

$$(x+y) \bmod b = x \bmod b + y \bmod b$$

$$(x \cdot y) \bmod b = x \bmod b \cdot y \bmod b$$

Isso torna mais fácil calcular poderes modulo um número

$$(x^{y+z}) \bmod b = (x^y \cdot x^z) \bmod b = (x^y \bmod b \cdot x^z \bmod b) \bmod b$$

Referências

Grimm, R., Kempe, T., Löhr, A., & Scholle, O. (2016). *Informatik* (em inglês). (Schöningh-Schulbuch, 1. Auflage, 4. É o Druck. Paderborn: Schöningh (p. 280-284)

Ejemplo situación de aprendizaje 1: **¡Hablemos a las máquinas!**

Part A. Datos Generales																																					
A.1 Título:	<i>¡Hablemos a las máquinas!</i>																																				
A.2 Autor(es/as):	<i>Manuel Toro Casaucao, IES El Sobradillo</i>																																				
A.3 Resumen:	<i>En esta situación de aprendizaje, el alumnado aprenderá cómo descomponer algoritmos simples de forma secuencial, y aprenderá la manera de poder expresarlos y comunicarlos a través de diagramas de flujo.</i>																																				
A.4 Palabras Clave:	<i>Diagramas de flujo, pensamiento secuencial, robótica, lenguajes de programación.</i>																																				
A.5 Versión:	<i>Borrador</i>																																				
A.6 Fecha:	<i>15/09/2021</i>																																				
A.7 Licencia de Copyright:	<i>Atribución de compartir por igual CC BY-SA</i>																																				
Part B. Datos de aprendizaje																																					
B.1 Curso/s:	<i>4º ESO, edad 15-16 años</i>																																				
B.2 Materia/s:	<i>Tecnología</i>																																				
B.3 Topic(s):	<i>Sistemas de control programables. Robótica.</i>																																				
B.4 Dimensiones del Pensamiento Computacional:	<table border="1"> <tbody> <tr><td>Pensamiento algorítmico (AL)</td><td>✓</td></tr> <tr><td>Abstracción (AB)</td><td>✓</td></tr> <tr><td>Generalización (GE)</td><td></td></tr> <tr><td>Razonamiento lógico (LR)</td><td>✓</td></tr> <tr><td>Coincidencia de patrones (PM)</td><td></td></tr> <tr><td>Descomposición de problemas(PD)</td><td>✓</td></tr> <tr><td>Traducción del problema (PT)</td><td>✓</td></tr> <tr><td>Evaluación (EV)</td><td>✓</td></tr> <tr><td>Representación (RE)</td><td>✓</td></tr> <tr><td>Recopilación de datos (DC)</td><td></td></tr> <tr><td>Representación de datos (DR)</td><td></td></tr> <tr><td>Análisis de datos (DA)</td><td></td></tr> <tr><td>Modelaje (MO)</td><td>✓</td></tr> <tr><td>Simulación(SIM)</td><td>✓</td></tr> <tr><td>Automatización (AUT)</td><td>✓</td></tr> <tr><td>Secuenciación (SE)</td><td>✓</td></tr> <tr><td>Testeo (TE)</td><td>✓</td></tr> <tr><td>Entendimiento de las personas – (UP) /Inteligencia Artificial (AI)</td><td>✓</td></tr> </tbody> </table>	Pensamiento algorítmico (AL)	✓	Abstracción (AB)	✓	Generalización (GE)		Razonamiento lógico (LR)	✓	Coincidencia de patrones (PM)		Descomposición de problemas(PD)	✓	Traducción del problema (PT)	✓	Evaluación (EV)	✓	Representación (RE)	✓	Recopilación de datos (DC)		Representación de datos (DR)		Análisis de datos (DA)		Modelaje (MO)	✓	Simulación(SIM)	✓	Automatización (AUT)	✓	Secuenciación (SE)	✓	Testeo (TE)	✓	Entendimiento de las personas – (UP) /Inteligencia Artificial (AI)	✓
Pensamiento algorítmico (AL)	✓																																				
Abstracción (AB)	✓																																				
Generalización (GE)																																					
Razonamiento lógico (LR)	✓																																				
Coincidencia de patrones (PM)																																					
Descomposición de problemas(PD)	✓																																				
Traducción del problema (PT)	✓																																				
Evaluación (EV)	✓																																				
Representación (RE)	✓																																				
Recopilación de datos (DC)																																					
Representación de datos (DR)																																					
Análisis de datos (DA)																																					
Modelaje (MO)	✓																																				
Simulación(SIM)	✓																																				
Automatización (AUT)	✓																																				
Secuenciación (SE)	✓																																				
Testeo (TE)	✓																																				
Entendimiento de las personas – (UP) /Inteligencia Artificial (AI)	✓																																				

B.5 Enfoques del Pensamiento Computacional :	<table border="1"> <tr> <td>Retoques, experimentación y juego</td> <td>✓</td> </tr> <tr> <td>Creación, diseño y experimentación</td> <td>✓</td> </tr> <tr> <td>Depuración, hallazgo y arreglo de errores</td> <td>✓</td> </tr> <tr> <td>Perseverancia y seguir adelante</td> <td>✓</td> </tr> <tr> <td>Colaboración y trabajo conjunto</td> <td>✓</td> </tr> </table>	Retoques, experimentación y juego	✓	Creación, diseño y experimentación	✓	Depuración, hallazgo y arreglo de errores	✓	Perseverancia y seguir adelante	✓	Colaboración y trabajo conjunto	✓																																				
Retoques, experimentación y juego	✓																																														
Creación, diseño y experimentación	✓																																														
Depuración, hallazgo y arreglo de errores	✓																																														
Perseverancia y seguir adelante	✓																																														
Colaboración y trabajo conjunto	✓																																														
B.6 Contexto temático del proyecto de CompuT:	<table border="1"> <tr> <td>Robótica Educativa o Física Computacional</td> <td colspan="2">✓</td> </tr> <tr> <td rowspan="5">Proyecto de Ciencias computacionales</td> <td>Modelaje/ Simulación</td> <td>✓</td> </tr> <tr> <td>Modelaje Bifocal</td> <td></td> </tr> <tr> <td>Creación o uso de sensores</td> <td></td> </tr> <tr> <td>Matemáticaso Ciencias Computacionales</td> <td>✓</td> </tr> <tr> <td>Otros:....</td> <td></td> </tr> <tr> <td>Datos del proyecto de Ciencia</td> <td colspan="2"></td> </tr> <tr> <td>Historia de la Ciencia y la Tecnología</td> <td colspan="2"></td> </tr> <tr> <td>Juegos Digitales, programas o aplicaciones móviles</td> <td colspan="2"></td> </tr> <tr> <td rowspan="5">Proyectos de Humanidades Digitales</td> <td>Cuentacuentos digital</td> <td></td> </tr> <tr> <td>Ficción Interactiva</td> <td></td> </tr> <tr> <td>Extracción de textos</td> <td></td> </tr> <tr> <td>Algoritmos de uso diario</td> <td></td> </tr> <tr> <td>Otros:....</td> <td></td> </tr> <tr> <td>Proyectos de Inteligencia Artificial</td> <td colspan="2"></td> </tr> <tr> <td>Enfoque de estudio - Proyectos de clase futuros</td> <td colspan="2"></td> </tr> <tr> <td>Experiencias desenchufadas o uso de manipulativos</td> <td colspan="2">✓</td> </tr> <tr> <td>Otros:....</td> <td colspan="2"></td> </tr> </table>	Robótica Educativa o Física Computacional	✓		Proyecto de Ciencias computacionales	Modelaje/ Simulación	✓	Modelaje Bifocal		Creación o uso de sensores		Matemáticaso Ciencias Computacionales	✓	Otros:....		Datos del proyecto de Ciencia			Historia de la Ciencia y la Tecnología			Juegos Digitales, programas o aplicaciones móviles			Proyectos de Humanidades Digitales	Cuentacuentos digital		Ficción Interactiva		Extracción de textos		Algoritmos de uso diario		Otros:....		Proyectos de Inteligencia Artificial			Enfoque de estudio - Proyectos de clase futuros			Experiencias desenchufadas o uso de manipulativos	✓		Otros:....		
Robótica Educativa o Física Computacional	✓																																														
Proyecto de Ciencias computacionales	Modelaje/ Simulación	✓																																													
	Modelaje Bifocal																																														
	Creación o uso de sensores																																														
	Matemáticaso Ciencias Computacionales	✓																																													
	Otros:....																																														
Datos del proyecto de Ciencia																																															
Historia de la Ciencia y la Tecnología																																															
Juegos Digitales, programas o aplicaciones móviles																																															
Proyectos de Humanidades Digitales	Cuentacuentos digital																																														
	Ficción Interactiva																																														
	Extracción de textos																																														
	Algoritmos de uso diario																																														
	Otros:....																																														
Proyectos de Inteligencia Artificial																																															
Enfoque de estudio - Proyectos de clase futuros																																															
Experiencias desenchufadas o uso de manipulativos	✓																																														
Otros:....																																															
B.7 Propósito / Objetivo de la Situación de aprendizaje.	<p><i>Al realizar esta situación de aprendizaje, el alumnado habrá desarrollado conocimientos básicos acerca de la forma en que trabajan los sistemas programables, y comprenderá la necesidad de descomponer la solución a un problema en una secuenciación de pasos simples. También aprenderá una forma eficiente de comunicar estas soluciones a través de diagramas de flujo. De forma transversal, entenderá la importancia de conocer la máquina (hardware) para diseñar la solución (software).</i></p>																																														
B.8 Productos de aprendizaje/ Logros⁴:	<p><i>Téngase en cuenta cómo la situación de aprendizaje puede favorecer el desarrollo general de competencias y habilidades del S. XXI.</i></p>																																														

⁴ Para la formulación efectiva de aprendizaje instruccional el trabajo de Mager, quien alude a la definición del uso de

	B.8.1 Conocimiento (Saber)	<ul style="list-style-type: none"> • Entender la importancia de descomponer la solución a un problema en pasos secuenciales. • Entender la importancia de conocer las capacidades de la máquina (hardware) para diseñar la solución a un problema. • Conocer las reglas de los símbolos básicos de los diagramas de flujo.
	B.8.2 Habilidades (Saber hacer)	<ul style="list-style-type: none"> • Saber descomponer un algoritmo sencillo en pasos secuenciales. • Saber representar algoritmos en diagramas de flujo.
	B.8.3 Actitudes-afectivo (Saber ser)	<ul style="list-style-type: none"> • Reconocer la importancia de las máquinas para resolver problemas del día a día.
B.9 Competencias horizontales . Habilidades del S. XXI	<i>Esta propuesta didáctica crea las condiciones adecuadas para desarrollar habilidades del S. XXI tales como el pensamiento crítico, la resolución de problemas, la creatividad, la comunicación, la colaboración, la curiosidad, la iniciativa, la perseverancia y la adaptabilidad.</i>	
	B.9.1 Aprendizaje y habilidades de innovación:	<p><i>Pensamiento crítico: encontrar soluciones a los problemas. Tienen que buscar las soluciones de cada problema que apareció durante la situación de aprendizaje.</i></p> <p><i>Creatividad: pensar fuera de la caja. Los estudiantes deben ser originales buscando soluciones para los problemas.</i></p> <p><i>Colaboración: el alumnado podrá compartir sus propuestas con el resto para ir perfilando la solución.</i></p> <p><i>Comunicación: expresar las soluciones mediante un lenguaje de diagramas de flujo.</i></p>
	B.9.2 Habilidades de alfabetización digital:	<i>Alfabetización informacional: El alumnado buscará información sobre los distintos lenguajes de programación.</i>
	B.9.3 Habilidades para la vida:	<p><i>Flexibilidad y adaptabilidad, interacción social y cultural transversal, productividad y responsabilidad y liderazgo.</i></p> <p><i>El alumnado adaptará su solución de forma que sea más óptima, corrigiendo errores que se vayan presentando de forma colaborativa con sus compañeros. Siendo responsables críticos con sus resultados.</i></p>
B.10 Métodos de enseñanza modernos:	<p><i>La situación de aprendizaje incluye métodos de enseñanza moderna tales como:</i></p> <p><i>Aprender codificando, ya que el alumnado tendrá secuenciar</i></p>	

acciones observables y criterios mensurables en el desempeño de la evaluación en condiciones específicas, Mager, F. (1975). "Preparing Instructional Objectives". (2nd ed.). Belmont, CA: Fearon. & Mager, F. (1997). "Preparing instructional objectives": Una herramienta Crítica en el desarrollo de la instrucción efectiva. "Atlanta: The Center for Effective Performance". Los verbos podrían seguir la taxonomía de Bloom, véase por ejemplo: <https://tips.uark.edu/blooms-taxonomy-verb-chart/>. Es importante utilizar procesos cognitivos de alto rango.. Anderson, L. W., & Krathwohl, D. R. (2001). "A taxonomy for learning, teaching, and assessing", Abridged Edition. Boston, MA: Allyn and Bacon

	<p><i>soluciones a problemas.</i></p> <p><i>Aprendizaje colaborativo, ya que el alumnado deberá trabajar en equipo para completar la tarea.</i></p>	
B.11 Integración de Pensamiento Computacional en el Currículo:	<p><i>Esta situación de aprendizaje está relacionada con los lenguajes de programación y la solución a problemas de forma secuencial.</i></p>	
B.12 Relación con el Currículo y/ o estándares:	<p><i>Esta situación de aprendizaje está relacionada con el tema de Sistemas de control programables, de la asignatura Tecnología de 4º ESO. También está relacionada con el currículo de Tecnologías de la información y comunicación I y II de 1º y 2º de bachillerato.</i></p>	
B.13. Conocimientos Previos:	<p><i>No requieren conocimientos previos.</i></p>	
B.14. Nivel de dificultad de la situación de aprendizaje:	<p><i>Intermedio</i></p>	
B.15. Escenario social de la situación de aprendizaje:	<p><i>El alumnado tendrá que trabajar en pequeños grupos para completar algunas de las actividades de esta situación de aprendizaje.</i></p>	
B.16 Lugar de la implementación didáctica:	<p><i>Clase o laboratorio de computación.</i></p>	
B.17 Duración:	<p><i>3 x 45' sesiones</i></p>	
B.18 Material educativo, recursos, instrumentos, herramientas y medios de comunicación y difusión:	B.18.1 "Software":	
	B.18.2 "Hardware":	
	B.18.3 Recursos en línea:	<i>https://www.areatecnologia.com/diagramas-de-flujo.htm</i>
	B.18.4 Material educativo convencional:	<i>Pizarra y rotulador. Papel y lápiz.</i>

Part C. Diseño de la Experiencia de aprendizaje

C.1. Actividades- Acción- Argumento- Tabla de secuencia del guión gráfico:	Fase 1.	<i>Entender la secuenciación de problemas.</i>	
	Actividad/Tarea	Descripción/Procedimiento	Duración
	<i>A1.1 Conozcamos el hardware.</i>	<p><i>Se les plantea al alumnado que el docente es un "robot" de última generación con las siguientes capacidades:</i></p> <ul style="list-style-type: none"> <i>- Dar un número de pasos.</i> <i>- Girar un número de grados hacia la izquierda o la derecha.</i> <i>- Detectar si ve la puerta de</i> 	<i>10'</i>

	<p>la clase.</p> <ul style="list-style-type: none"> - Detectar si puede tocar la puerta de la clase. - Abrir la puerta. 	
A1.2 Tenemos un problema.	<p>El alumnado se dividirá en grupos, y se les solicitará que expliquen al docente cómo pueden salir de la clase.</p> <p>NOTA: Normalmente el alumnado planteará soluciones no secuenciales en lenguaje humano, prácticamente en una frase. "Ej: Busca la puerta y sal." Entonces el docente le indicará la necesidad de explicarlo solo realizando las acciones que entiende la máquina.</p>	15'
A1.3 Programemos al docente.	<p>Los distintos grupos diseñarán su solución y la probarán con el docente, realizando las acciones que le indique cada grupo invitando a la reflexión si falla el algoritmo.</p>	20'
Fase 2.	Entender los bucles.	
Actividad/Tarea	Descripción/Procedimiento	Duración
A2.1 No sabemos cómo está.	<p>Ahora se le plantea a los grupos que prueben sus algoritmos, pero el profesor cambiará su posición y/o orientación, viendo que estos ya no funcionan.</p>	10'
A2.2 Diagramas de flujo.	<p>El profesor les explicará las reglas de los diagramas de flujo (opcionalmente se les puede pedir que consulten https://www.areatecnologia.com/diagramas-de-flujo.html)</p>	20'
A2.3 Programamos nuestra solución	<p>El profesor dará un ejemplo de diagrama de flujo con algún error para que el alumnado busque como solucionarlo.</p>	15'
Fase 3.	Programamos	
A3.1 Subimos el nivel.	<p>El profesor pondrá mesas en medio de la clase a modo de obstáculos. Ahora tendrá que salir esquivando los obstáculos. De esta manera el alumnado debe entender que con el hardware anterior no tenemos la posibilidad de</p>	10'

		<p>esquivarlos, así que tendremos un docente 2.0 que tiene una nueva capacidad:</p> <ul style="list-style-type: none"> - Detectar que se ha chocado. <p>Nota: La posición inicial es desconocida.</p>	
	A3.2 Programamos	Cada grupo buscará una solución	20'
	A3.3 Resumen y debate	Se prueban las distintas soluciones, comparándolas y analizando su estructura.	15'
C.2 Evaluación			
	C.2.1 Retroalimentación del alumnado y reflexión.	El alumnado probará y corregirá sus algoritmos.	
C.3 Tarea de casa/ Trabajo con la familia	No es necesario.		
Parte D. Información para el profesorado			
D.1 Adaptación-Modificaciones para la inclusión de todo el alumnado.	Todo el alumnado puede desarrollar esta situación de aprendizaje		
D.2 Extensión	https://code.org/		
D.3 Recursos	https://www.areatecnologia.com/diagramas-de-flujo.htm https://www.youtube.com/watch?v=awhRzotTT0E&list=LLkNaV2CUupBwIEo-n6aT93A		
D.4 Experiencia derivada de la implementación de la situación de aprendizaje	El alumnado tiene un primer acercamiento a los lenguajes de programación y empiezan a entender las distintas estructuras de control. El docente puede cambiar, si lo considera oportuno, la máquina por algún alumno a partir de la fase 2.		
D.5 Relaciones con otras situaciones de aprendizaje.			
D.6 Revisiones del profesorado			
D.7 Evaluación de la situación de aprendizaje	[1=Very Bad – 5=Very Good]		
D.8 Referencias			

Parte E. Anexos

Worksheet 1 – Ejemplo de solución a los problemas planteados FASE I.

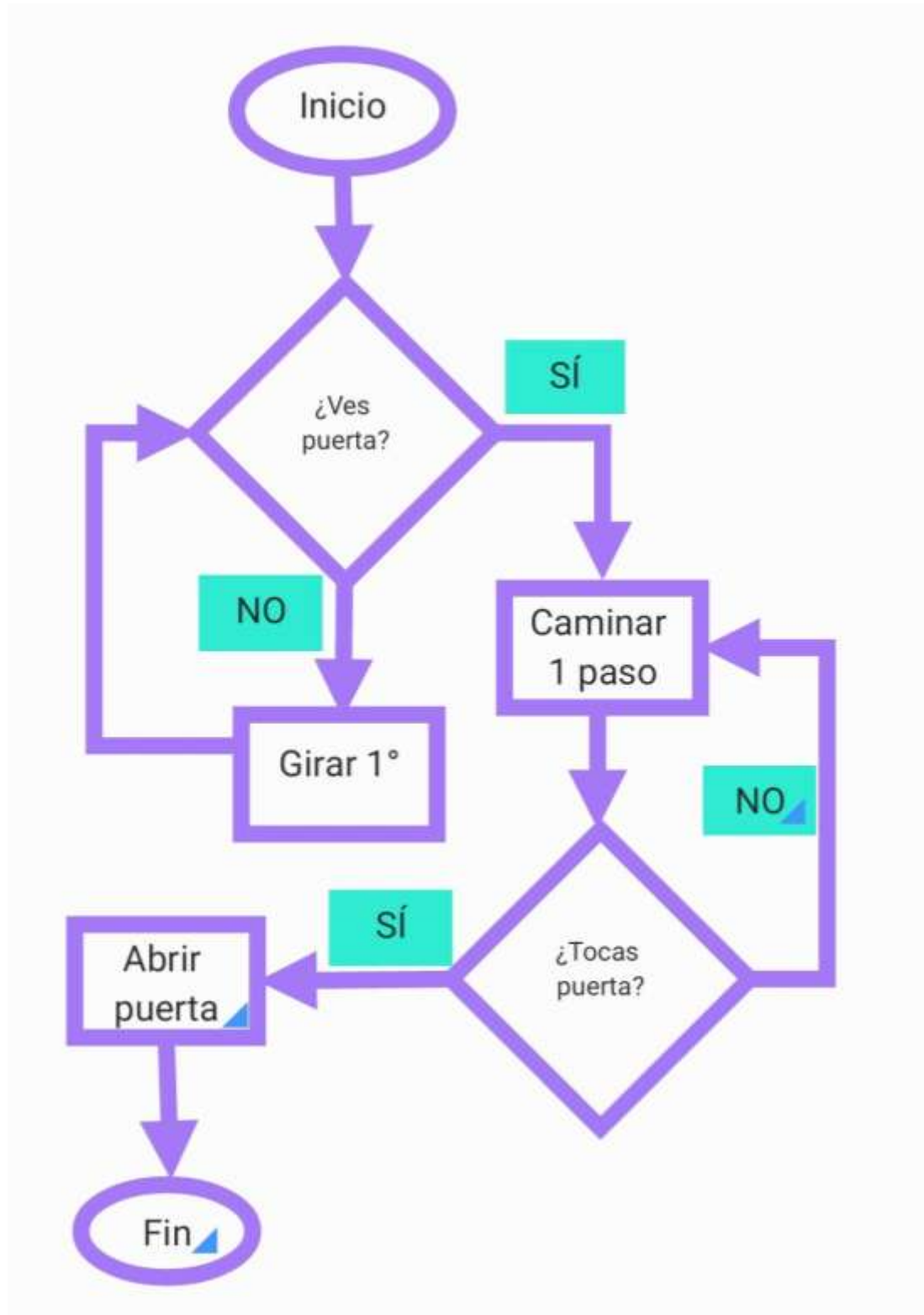
Worksheet 2 – Ejemplo de solución a los problemas planteados FASE II.

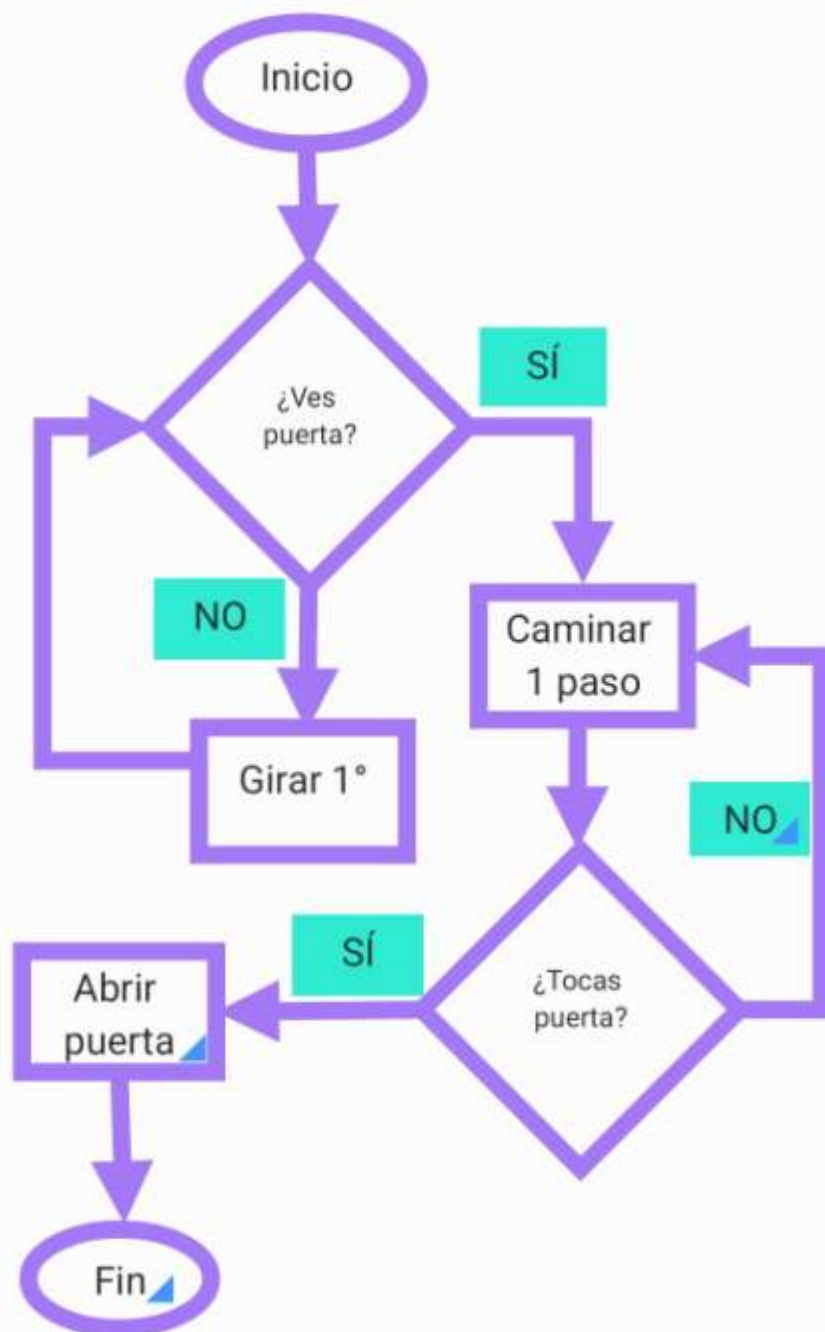
Worksheet 1

Solución de FASE I



Worksheet 2 Solución de FASE II







UNIVERSITY OF THE
AEGEAN



Comput

Computational Thinking at School

Erasmus+ KA201 Project: 2019-1-EL01-KA201-062883