|  |  |
| --- | --- |
| **Title** | The Secrets of Cryptography – Treasure Hunt |
| **Key words** | Encrypting and decrypting, Ceasar cipher, visual cryptography, Enigma, treasure hunt |
| **Short description** | Within this activity students are introduced to the theory of cryptography, as well as to some ways of encrypting used throughout the history: Caesar cipher, visual cryptography, public key cryptography.  The activity is designed as Treasure Hunt game. Students work individually or in groups and they solve the riddles. Teacher helps if necessary. Students study the materials and get enough information to do all the tasks. Group work is encouraged, along with critical thinking and reading comprehension.  There are two versions of the activity: a simple and a complex one.  In the complex version students learn the ways of encryption with the help of Enigma.  Activity can be further extended in Art classes (making of the visual criptography of an image) and in IT lessons. |
| **IT tools** | Micro:bit, Maqueen, 3d print |
|  |  |
| **Fields (select)** | **A1: Math**  A2: Science  A3: Art  A4: Music  A5: P.E.  A6: Mother tongue  A7: Foreign language  Other:  A8: IT  A9: Civic education |
| **Themes (for each selected field)** | A1: dividing with remainder, prime numbers |
|  |
|  |
|  |
| **Expected prior knowledge** |  |
| **Expected learning outcomes** | * Uses natural numbers up to 10,000 to describe and display quantity and order. * Adds and subtracts in a set of natural numbers up to 1,000 * Multiplies and divides natural numbers up to 1,000 by single digits using long multiplication * Applies four computational operations and relationships between numbers in problem situations. * Solves tasks with one unknown member by writing the letter as a number |
| **Expected duration** | 45-60 minutes |
| **Preparation of activities** | 1. Teacher can deepen his knowledge of cryptography, if necessary. (<https://web.math.pmf.unizg.hr/~duje/kript/osnovni.html>)   Preparation of the material is necessary. Materials are available at: <https://inamath.uniri.hr/treasure-hunt/>   1. The riddles (tasks) booklet for the Treasure hunt includes decrypting tasks, using various methods of decryption (Caesar cipher, visual cryptography – foil, public key cryptography at micro:bit) 2. Preparation of the foil set for visual cryptography (two foils overlap and thus reveal a picture): foils should be printed, using transparency sheets for the overhead projector. 3. 5 micro:bits should be prepared in the following way: four „fake” micro:bits are necessary (with prepared code Microbit\_false.hex) and four labels should be attached to them (5 petals flower, empty circle, five-pointed star, a sad smiley face) and one „real” micro:bit (with prepared code Microbit\_real.hex) with the label with a black square. 4. Preparation of the Treasure hunt path to end the activity. Those are the parts of the road and a plan of the neighborhood that will be composed of pieces of paper or made in 3D printer (<https://www.tinkercad.com/things/8ayryvLRFLL> ), I.e. a neighborhood from the scenario Math Ride (on the link <https://inamath.uniri.hr/math-ride/> you need to download GeoGebra files: voznja, voznjaT, voznja kut i voznja ravno; and print them in order to get parts of the road). A small piece of paper (or an envelope) should be placed on each crossroads and something should be written on it (using the invisible UV marker) A message (ex. Good job!) should be written in the field CILJ (The end).   A picture containing calendar  Description automatically generated   1. A car toy for kids to steer (manually, according to instructions) or to program Maqueen according to the prepared codes: *microbit-DaljinskiZaMacqeen6* and *microbit-MacqeenPlusCTKPapir23*  from the page <https://inamath.uniri.hr/math-ride/> 2. Instructions and description: the process of cryptography, Caesar cipher, Enigma, cryptography with the help of Micro:bit 3. Tasks booklet for the advanced version 4. Preparation of Enigmas (for advanced version): <https://www.thingiverse.com/thing:5793033> |
| **Detailed description of activities** | 1. This activity can be done after the scenario The Secrets of Cryptography, but it can also be done independently for students to learn about cryptography through a game.   1. Treasure hunt – a basic version (45 min)   Students work in four groups. In this case, four sets of foils and four sets of Micro:bits should be prepared and placed on four separate tables. Each group gets one booklet with riddles:    Having completed the 3rd clue with the help of Micro:bit, a group gets to the table with the path and the car (or Maqueen). Following the instructions they found, they should reach the finish field that has a message (Good job!, for example). If they made a mistake, the students go back to their seats and try to find the mistake and/or start again.   1. Treasure hunt – advanced version (60 minutes)   CLUE 1  Caesar encrypted an alphabet letter by replacing it with the letter 3 positions down in the alphabet. Guess a number less than 10 and discover a secret message: YTRNRFLNSJIYMWJJSZRGJWXQCCQQC  CLUE 2  Listen carefully to what Caesar says, lock the enigma, it will tell you what to do next.  OVDIDZPYOSDCYIUHTBDK  CLUE 3  Put the transparencies together to figure out the secret key.  CLUE 4  Transparencies help you choose the right Micro:bit. Unlock it and discover the robot's path to the treasure: EBEJBEE.  CLUE 5  Run me and follow the path, and when the path disappears, listen to what the Micro:bit tells you (L: left, R: right, S: straight). |
| **Extension activities** | 1. Students get to know the procedure of making visual cryptography foils (<https://www.101computing.net/visual-cryptography/> ) and they can make visual cryptography foils in Art class or within lesson on the geometrical shapes. 2. In IT classes students can change and/or make an encrypting / decrypting program in Micro:bit and change / make the program for micro:Maqueen. They can also make a path in the program GeoGebra (paper path) or in Tinkercad (3d printed path). |
| **Additional notes** |  |
| **Authors** | Bojan Crnković, Vedrana Mikulić Crnković, Ivona Traunkar (Faculty of Mathematics, University of Rijeka) |