INTRODUCTION TO CRYPTOGRAPHY

SAFETY > 4.2 PROTECTING PERSONAL DATA AND PRIVACY

TARGET GROUP	AGE GROUP	PROFICIENCY LEVEL	FORMAT	COPYRIGHT	LANGUAGE
All, Job seekers, School drop outs, Students (secondary school)	Adults, Elderly citizens, Teenagers	Level 1	Activity sheet	Creative Commons (BY-SA)	English, French

This workshop helps participants to understand how messages can be encrypted. It also introduces them to a useful tool known as cryptii. Cryptii is a website that uses various ways to encrypt our messages when necessary.

General Objective	Knowledge acquisition
Preparation time for facilitator	less than 1 hour
Competence area	1 - Information and data literacy
Time needed to complete activity (for learner)	1 - 2 hours
Name of author	Salomé Hurel
Support material needed for training	Computers - Internet connection - Projector
Resource originally created in	French

WORKSHOP DIRECTIONS

1 Introduction

This workshop is conducted via a treasure hunt in which participants will need to use a simple tool to decode a message. This will lead them to a website where they will find a true encrypted mystery (still unsolved to this day). During the game, participants will learn about various simple notions of encryption through an online tool called Cryptii. The URL of the mysterious message is divided into three parts, each one encrypted through a different method:

- Backwards lettering
- Caesar cypher
- Morse

Participants will need to break the code using cryptii.

Facilitation tips: This activity is a pretext for explaining how to protect personal data – particularly messages transmitted – by encrypting it, and the reasons for doing it. To complement this, refer to these workshops: 'Personal Data' and 'Cryptography' (in progress).

2 What is cryptography?

Cryptography is a coding system for hiding messages from outside view. Only those knowing the method for decoding a message are able to read it. The method used is often a secret shared between the sender(s) and the receiver(s) of a message (the number of shifted characters for example).

3 Cryptii presentation

Cryptii is a site that codes and decodes sentences using various methods. You can now showcase types of decryption that are easy to learn:

1. Reversing the order of the letters of a message
2. Caesar cipher
3. Morse

Go to https://cryptii.com You only have to use the simple homepage interface when presenting to participants:

- On the left of the page is the text to be decoded
- In the centre, the choice of decoding method (here Enigma machine)
- On the right, the result of decryption

To start, quickly present the Caesar cipher also known as shift cipher. This method is named as such since it is said that this how Julius Caesar encoded his secret communications. Do not go into detail in explaining how this works – the objective just after this is for the participants to discover the workings of this themselves. For this, on Cryptii, click on 'Enigma machine' in orange. The selection window will open – choose Caesar cipher. Caesar cipher will now become the encoding method. To help participants understand this, type the word 'absolutely' in the left-side module and move the shift gauge in the centre to 0 using – or +. At 0, the word will remain the same – it will not be coded. Click once on the – and 'absolutely' is now encrypted! But how? Leave 3-5 minutes for your group to reflect. Explanations: The Caesar cypher is simple: we shift each letter of message by one or several positions in the alphabet. With the gauge at 1, we get this decryption system: b = **a** c = **b** t = **s** p = **o** m = **l** v = **u** u = **t** f = **e** m = **l** z = **y** To read this code you simply need to shift the letters. Show the site https://www.dcode.fr/caesar-cipher on which breaks Caesar ciphers digitally. If you type an encrypted word or phrase into the decoder, a program will attempt every shift possible and display them in the left-hand column. All you then have to do is find the coherent result in order to reveal the hidden message.

4 Progression

Once the functioning of Cryptii is explained, give the encoded URL to participants. To access the secret message located at this address, the group will need to decode one by one the 3 parts of the URL. Depending on the level and the number of participants, do one of the following:

- Divide them into groups and organise a race – the first group to decrypt the address and who finds the message wins
- Let them do the exercise individually

Once they are ready: Write the encrypted code on the board:

gro.euqiremunudsruegayov.sptth://dw-jvualua/bwsvhkz/2020/—– …–/ .-.. . – – .-. . -.. ..- –.. — -.. .. .- -.-. .-.-.- .— .-. –.

Once decoded, this URL is revealed:

https://www.digitaltravellers.org/wp-content/uploads/2020/03/1457972964.jpg

It was encrypted in 3 different ways. Each group will therefore guess what method was used for each part. To make is easier, make it explicit before the beginning that the URL was indeed encoded in 3 different parts, each time using a different encoding system.

Part 1: The first part of the URL was encrypted using the Reverse method. Once encrypted, we get:

gro.euqiremunudsruegayov.sptth://

Ask participants to use Cryptii to decode this part. If this is taking up all your time, drop the hint that since it's a website URL it begins with https://. Big clue!

Part 2*:* The second part of the address is wp-content/uploads/2020 This was coded using a Caesar cipher. Once decoded (shifted 7 places), we get:

dw-jvualua/bwsvhkz/2020/

Hint (SHHHH): go to https://www.dcode.fr/chiffre-cesar, paste the code and select 'DECRYPT CAESAR CODE'. Now check each result on the left-hand column.

Part 3*:* For the filename 03/Lettreduzodiac.jpg, we wanted to use Morse code more for historical reasons that for the challenge and to demonstrate that a letter can be replaced by a sign or symbol. The result in Morse:

—– …–/ .-.. . – – .-. . -.. ..- –.. — -.. .. .- -.-. .-.-.- .— .-. –.

Once decoded, participants will be able to enter the URL into the browser. This letter is a real one written by the mystery serial killer known as the Zodiac killer who has never been identified to this day. This letter indicates that by decrypting its cipher, the writer's identity would be found. The FBI were unsuccessful and so the letter was made public so anyone could have a go at it. It has yet to be solved. In fact, at one point, the killer sent another coded message to the press and saw it quickly solved by a couple who would often do coded puzzles in magazines.