



PASSWORD CRACKING (THURSDAY PM)

Lesson Description: This activity gives students insight into how garage doors evolved into the modern utilities we use today. Students attack the vulnerabilities present in various renditions

This activity gives an introduction to cracking passwords. By the end of the activity, students should be able to recognize that passwords can be cracked reasonably quickly and easily, and have a better understanding of what adversaries do when approaching a password-cracking problem. The activities are organized into easy, medium, and hard sections, each with two passwords to crack. Each difficulty has one password-cracking problem where some background information about the person using the password is given, and they must deduce what the password is given that background information. The other problem for each difficulty is decoding a password that's gone through some sort of cipher or encoding.

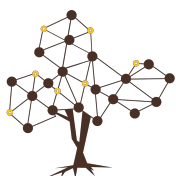
The set-up for the microbits is simple, each of the microbits just needs to listen for the correct password, and show a "secret message" when it receives the correct password. Each microbit should be at its own station, and a paper with the instructions for each microbit should be at each respective station. To fully complete the activity, students will show an instructor all of the secret messages.

Prerequisite Knowledge: Students are expected to know how to operate the micro:bit (use the buttons and understand read the display).

Length of Completion: The lesson should take 1 hour to 1.5 hours.

Level of Instruction: This lesson is intended for high school and middle school students.

Applicable First Principles &/or Concepts:



Defense in Depth

Confidentiality

Think Like an Adversary

Integrity

Resources that are Needed:

1. Micro:bits (1 for each difficulty: 3)
2. Cipher wheel
3. Paper with instructions

LEARNING OUTCOMES

Novice Group Learning Outcomes:

- Recognize that a badly crafted password is one that is based on personally relevant information like a name or birthday.
- Explain what a cipher is
- Explain how a cipher wheel encodes a line of text
- Design more secure passwords
- Understand how to securely store passwords on some form of local storage (text document, paper) by using ciphers as a method of simple encryption that can be done by hand.

Intermediate Group Learning Outcomes:

- Understand the differences in complexity between ciphers and how it affects the security of a message

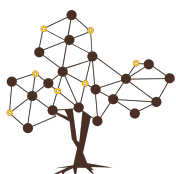
Expert Group Learning Outcomes:

- Being able to create your own cipher
- Explain why a cipher is important for wireless communication

LESSON DETAILS

Assessment: None

Extension Activities: Building one's own cipher and creating a message with that cipher, Creating an alphabet whose characters correspond to the one's in the English alphabet.



Differentiated Learning Opportunities:

Novice: A set of information is presented about an individual and based on that information you have to guess a password.

Intermediate: A simple cipher wheel is used to decrypt some information

Expert: A micro:bit is loaded with depictions of foreign or alien characters that correspond to characters in the English alphabet and this micro:bit is used to determine a message written in these alien characters.

LESSON

Lesson 1 Details:

Warm Up: Students are given a set of scrambled words and using the definitions of those words are asked to put the letters of these words in the correct order. This gets students used to working with the characters of a word.

Lesson: Students work together or at their own pace in an attempt to identify the passwords of a set of individuals, uncover the meanings of words encrypted with ciphers. Prior to the student engaging with the activities, a brief lesson about each station is given which describes the how a student can figure out how to use the tools or information provided to come to a conclusion but does not give away the exact formulations behind the ciphers or exactly how the provided background information relates to the password. The best way to do this would be to go through a simple example. Further those that first complete all difficulties of the activity should work to instead of decrypt ciphers encrypt them and gain practice or maybe make their own form of cipher.

