|  |  |  |
| --- | --- | --- |
| **Name: Kelly Hiersche** | **Contact Info: kellyhiersche@gmail.com** | **Date: 07/02/2018** |

|  |  |  |  |
| --- | --- | --- | --- |
| **Lesson Title : Understanding Encryption Keys & Breaking them** | **Unit #: 1** | **Lesson #: 1** | **Activity #: 1** |
| **Activity Title: Encryption with Public Key** |

|  |  |
| --- | --- |
| **Estimated Lesson Duration:** | **8 days** |
| **Estimated Activity Duration:** | **4 days (50 minute periods)** |

|  |  |
| --- | --- |
| **Setting:** | **Classroom** |

|  |
| --- |
| **Activity Objectives:** |

I can…

1. Develop essential questions about Cybersecurity and Encryption
2. Present at least one-way math is used in modern encryption
3. Pass secret information using a public key
4. Understand the difference between types of encryption systems

|  |
| --- |
| **Activity Guiding Questions:** |

* What are methods of information encryption?
* What are public and private keys?
* How do you share a public key?

| **Next Generation Science Standards (NGSS)** | |
| --- | --- |
| **Science and Engineering Practices (Check all that apply)** | **Crosscutting Concepts (Check all that apply)** |
| Asking questions (for science) and defining problems (for engineering) | Patterns |
| Developing and using models | Cause and effect |
| Planning and carrying out investigations | Scale, proportion, and quantity |
| Analyzing and interpreting data | Systems and system models |
| Using mathematics and computational thinking | Energy and matter: Flows, cycles, and conservation |
| Constructing explanations (for science) and designing solutions (for engineering) | Structure and function. |
| Engaging in argument from evidence | Stability and change. |
| Obtaining, evaluating, and communicating information |  |

| **Ohio’s Learning Standards for Science (OLS)** |
| --- |
| **Expectations for Learning - Cognitive Demands (Check all that apply)** |
| Designing Technological/Engineering Solutions Using Science concepts **(T)** |
| Demonstrating Science Knowledge **(D)** |
| Interpreting and Communicating Science Concepts **(C)** |
| Recalling Accurate Science **(R)** |

| **Ohio’s Learning Standards for Math (OLS) and/or**  **Common Core State Standards -- Mathematics (CCSS)** | |
| --- | --- |
| **Standards for Mathematical Practice (Check all that apply)** | |
| Make sense of problems and persevere in solving them | Useappropriate tools strategically |
| Reason abstractly and quantitatively | Attendto precision |
| Construct viable arguments and critique the reasoning of others | Look for and make use of structure |
| Model with mathematics | Look for and express regularity in repeated reasoning |

|  |
| --- |
| **Unit Academic Standards (NGSS, OLS and/or CCSS):** |

**F-BFA1b**

|  |
| --- |
| **Materials**: (Link Handouts, Power Points, Resources, Websites, Supplies) |

**Powerpoint (**1.1.1.a)

**Video on social media hacking** (still looking for a good video or going to create my own compilation – will input once I have it) 1.1.1.b

[**Printed/laminated copies of public and private map**](https://classic.csunplugged.org/wp-content/uploads/2014/12/unplugged-18-public_key_encryption_0.pdf) **(pg 194)** 1.1.1.c

**Calculators** (not necessary but will increase the speed of the activity)

|  |
| --- |
| **Teacher Advance Preparation:** |

Read the [PDF](https://classic.csunplugged.org/wp-content/uploads/2014/12/unplugged-18-public_key_encryption_0.pdf) explaining how the public key encryption works to ensure you understand the method of encryption, how to break it, and how to create guiding questions to bring your students through the activity

|  |
| --- |
| **Activity Procedures:** |

(Procedure best outlined by viewing PowerPoint that goes with this activity)

1. Have students take pretest the day before, should only take 15 minutes
2. Big Idea: Data Encryption
3. Hook: Video on social media hacking (tailor to your group of students- I recommend snapchat)
   1. Ask questions like “Has anyone ever had their social media hacked? Do your photos really disappear after 10 seconds? Can anyone “steal” the information you send?”
   2. Show the video
4. Essential Question: Ask students – What do you want to know about data encryption?

\*\*Students will have a sheet where they write their questions – questions they get from their partner and the chosen essential question at the end. This can be done in a notebook as well if it is a graded notebook

* 1. Take 3 minutes to write at least 3 questions about the big idea
  2. Take 3 minutes to share your ideas with a partner, pick at least 2 questions to share with the group
  3. Criteria/Constraints:
     1. Questions cannot be yes/no or one word answers
     2. Questions cannot be easily Googled
  4. Discuss and choose an essential question

1. Do an simple encryption example, outlined in the [PDF](https://classic.csunplugged.org/wp-content/uploads/2014/12/unplugged-18-public_key_encryption_0.pdf): Public Key Encryption from Computer Science Unplugged
   1. You will need supplies for this! (printed public and private keys, if laminated, need expo markers kids can write with)
   2. Class should be broken up into groups of 2. Each person with their own public and private map. Everyone sends a message and everyone decodes a message.
2. Class discussion – How did this encryption method work? How could it be broken? How could it be made more secure? **END OF DAY 1**
3. **START DAY 2** Come back next day with the Challenge: Come up with as many viable ways as possible to mathematically encrypt a message between you and your team.
4. Develop guiding questions:
   1. Use same brainstorming technique as above with altered times if needed
5. Provide students with a research template for them to start answering some of the questions developed
   1. Each student will have to address at least 2 questions
   2. For smaller classes, it may work better to research these questions as a group on the smartboard – student lead Google searches – put 1 trusted student in charge of the Google search – give other students the ability to go off and search other things as they think of it, while the main search is run in front of the class
6. Bring all research together whole group – work on answering the question – how is math used now to encrypt information / what are methods of encrypting / what makes an encryption successful
   1. each group must share 2 things they have learned
   2. Try to lead students to research things like public vs. private keys, symmetric and asymmetric keys, hash functions, Diffie Hellman exchange, double encryption
   3. This can be done by provided a list of websites you recommend students use to gather information
7. Question to contemplate whole class: Can any of the math we have learned be a viable method of encrypting? **END OF DAY 2**

**\*\*If extra time at end of day 1 or 2 students can try to develop their own public and private key that would work from the exercise completed on day 1**

**Formative Assessments:** Link the items in the Activities that will be used as formative assessments.

1. Brainstorming of essential question worksheet
2. Research template to start answering their guiding questions

**Summative Assessments:** These are optional; there may be summative assessments at the end of a set of Activities or only at the end of the entire Unit.

N/A

|  |
| --- |
| **Differentiation:** Describe how you modified parts of the Lesson to support the needs of different learners.  Refer to Activity Template for details. |

Accommodations:

* Simpler patterned encryption maps (available on page 193 of [PDF](https://classic.csunplugged.org/wp-content/uploads/2014/12/unplugged-18-public_key_encryption_0.pdf))
* Adjusted amount of brainstorming time – require 2 questions per person instead of 3
* Give list of websites to use for researching

Extensions:

* If extra time at end of day 1 or 2 students can try to develop their own public and private key that would work from the exercise completed on day 1
* Try and write a procedure for breaking this encryption

|  |
| --- |
| **Reflection:** Reflect upon the successes and shortcomings of the lesson. |

This activity needs to be extended, dependent upon the results of the pretest, which should inform you on your students’ initial knowledge of encryption and hacking. My students could not define the work encryption, which I was not expected. An additional 2 days should be added to the unit, on the discretion of the teacher, to ensure students fully understand the concept of encryption and decryption and have been exposed to various types of encryption systems.

Here are some links that gives some great classic and more complex types of encryption systems:

1. <https://academickids.com/encyclopedia/index.php/Encryption> - good intro the encryption terms

2. <https://www.ams.org/books/mawrld/029/mawrld029-endmatter.pdf> - long but very helpful paper on the connection between math and encryption throughout time

3. <https://www.cerias.purdue.edu/education/k-12/teaching_resources/lessons_presentations/cryptology.html> - great website that explains how to teach various classical encryption systems (cryptographic wheel, enigma machine, Morse code, etc)

Also, my students had more difficulty with the: Public Key Encryption from Computer Science Unplugged activity than I expected. I think it would be important to save this activity until after students have explored other encryption methods, like the enigma machine and shift ciphers, then do a fully worked out example on the board (available in the PowerPoint), before asking them to complete the activity on their own. Color coding the activity would be helpful as well as provided written out steps for students with IEPs or for classes that need more organization.

Finally, I think it is essential to introduce the CBL process before starting this unit. I expected my students to learn new math content, in a new type of lesson (CBL/EDP), in a field (cybersecurity) that they were unfamiliar with. This presented my students with a lot of barriers to success from the start. I believe the lesson would have been expedited and students would have shown more growth and confidence if a mini CBL unit, or multiple, had been taught earlier in the school year, or in previous classes. Also, if students have not completed independent research in your class already, be sure to use a rubric that guides them through the research process. (There is an example rubric on the wiki)