|  |  |  |
| --- | --- | --- |
| **Name: Kelly Hiersche** | **Contact Info:** [**kellyhiersche@gmail.com**](mailto:kellyhiersche@gmail.com) | **Date: 7/2/18** |

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

|  |  |
| --- | --- |
| **Estimated Lesson Duration:** | **8 days** |
| **Estimated Activity Duration:** | **5 days (50 minute periods)** |

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

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

1. Students will view logs as the inverse of exponents – use log to figure out the hidden exponent
2. Students will understand the difference between logs and roots
3. Students will understand how private keys are needed for encryption
4. Students will be able to use exponent rules for encrypting information
5. Students will understand the basics of modular arithmetic

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

1. What is the Diffie-Hellman exchange?
2. How are exponent rules used to encrypt information?
3. Does math create a secure way to encrypt information?
4. How does modern computational power affect the effectiveness of encryption techniques?

| **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-LEA4** Construct and compare linear, quadratic, and exponential models and solve problems: For exponential models, express as a logarithm the solution to *abct*= *d* where *a*, *c*, and *d* are numbers and the base *b* is 2, 10, or *e*; evaluate the logarithm using technology.

**N-RNA1-2** Extend the properties of exponents to rational exponents

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

PowerPoint explaining the Diffie-Hellman

Worksheet – practice log as inverse of exponents / practice using exponent rules (to be made)

Worksheet – using modular arithmetic & exponent rules to complete Diffie-Hellman

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

Read [this](http://www.cimt.org.uk/resources/topics/art003.pdf)

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

**Day 1/2**

1. Review exponent rules (students should already know product rule, quotient rule, power rule, expanded power rule)
2. Go through PowerPoint which leads students to see how you can use the log if you don’t know what power a number was raised too.
3. Give worksheet where they can practice taking the log to find the missing exponent
4. END CLASS – with a discussion on how the fact that a log exists makes this an insecure method of encrypting data – even high schoolers can break it

**Day 3/4**

1. Use PowerPoint to cover Diffie-Hellman with modular arithmetic example
   1. Be sure to discuss why it is difficult to undo modular arithmetic – no set inverse function
   2. Start talking about using inverses to crack codes
2. Students complete worksheet in teams with modular arithmetic to create a shared key
3. END CLASS – discuss why it is difficult to break the Diffie-Hellman when you include modular arithmetic / discuss whether it is better to have a secret key or public key? (difference between activity 1 and 2)

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

Worksheet - Diffie-Hellman Exchange by taking the log

Worksheet – Diffie-Hellman with modular arithmetic

**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

* Include extra examples / more steps in worksheet
* Have worksheet only deal with mod12 so students can use clock model to find the remainder (or have blank clocks w/ right # of blanks for students to fill in to practice modular arithmetic

Extension

* Come up with two possible inputs that would both satisfy the Diffie-Hellman modular example from the PowerPoint
* Explain why modular arithmetic is good for created a shared key

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

This was the best activity of the unit. Students really grasped the math concepts of logs and exponents, especially understanding them as inverses. I found a lot of success in teaching the lesson to explain how logs can help solve for a missing exponent, and then allowing the students to teach the lesson back, either to each other in small groups or allowing one student to go up to the board and teach the lesson again. The repetitive nature and real world context of “breaking an encryption” made this a memorable activity for the students.

I would do this unit with larger missing exponents though, like 4^45 or 3^102, instead of introducing with 4^3, because then I don’t think students see the value in the log, and believe a guess and check method is just as strong.

Finally, I did not have time to complete the modular arithmetic portion of this example. I do believe that it is vital to their encryption understanding and can also help them be better math thinkers, but it was not directly tied to Algebra II concepts, and I was dealing with a lot of illness, both on my students’ end and my end, so it got cut. Therefore, I do not have reflections, but I welcome any thoughts that you have after trying the unit yourself!