|  |  |  |
| --- | --- | --- |
| **Name: James Prugh** | **Contact Info:** | **Date:7/15/16** |

|  |  |  |  |
| --- | --- | --- | --- |
| **Lesson Title : Modular Arithmetic** | **Unit #:** | **Lesson #2:** | **Activity #:3** |
| **Activity Title: Modular Arithmetic** |

|  |  |
| --- | --- |
| **Estimated Lesson Duration:** | **1 day** |
| **Estimated Activity Duration:** | **1 day** |

|  |  |
| --- | --- |
| **Setting:** | **High school classroom** |

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

1. Students will learn modular arithmetic and use it to generate a shared key using the Diffie-Hellman algorithm.

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

1. What is modular arithmetic?
2. What is clock arithmetic? What does it have to do with encryption? What does it have to do with internet security?

| **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):** |

[CCSS.MATH.CONTENT.HSF.BF.A.1.B](http://www.corestandards.org/Math/Content/HSF/BF/A/1/b/)

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

<https://docs.google.com/viewer?a=v&pid=sites&srcid=ZGVmYXVsdGRvbWFpbnxqYW1lc3BydWdoMjAxNnxneDo0NTg5ZmY5NGQ0YTcxNDI2>

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

Bring in analog clock.

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

Students will be divided in groups of 4 and given questions to work on.

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

**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.

|  |
| --- |
| **Differentiation:** More difficult questions were posed to the students with prior experience in modular arithmetic |

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

I had assumed that students had some experience with clock arithmetic, but I was wrong. This was a bit more difficult than expected, and some students had a hard time getting their mind around a number system with a base other than 10. Once the Diffie-Hellman algorithm was introduced and we discussed the significance of modular arithmetic, the interest level picked up and the activities went well.