|  |  |  |
| --- | --- | --- |
| **Name:James Prugh** | **Contact Info:** | **Date:7/18/16** |

|  |  |  |  |
| --- | --- | --- | --- |
| **Lesson Title : Number Theory and Encryption** | **Unit #:** | **Lesson #:2** | **Activity #:4** |
| **Activity Title:** |

|  |  |
| --- | --- |
| **Estimated Lesson Duration:** | **2 90-minutes blocks and 1 50-minute class period** |
| **Estimated Activity Duration:** |  |

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

|  |
| --- |
| **Activity Objectives: Students will use number theory with basic methods of encryption to securely send and receive messages.** |

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

What are the different ways I can encrypt my message?

What if my message in intercepted?

How can my partner and I establish a shared key?

Do I have to share my private key with my partner?

| **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.LE.A.1](http://www.corestandards.org/Math/Content/HSF/LE/A/1/)

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

<https://docs.google.com/viewer?a=v&pid=sites&srcid=ZGVmYXVsdGRvbWFpbnxqYW1lc3BydWdoMjAxNnxneDo3ZjBlNGFiOWY1ZjUxNWY1>

<https://docs.google.com/viewer?a=v&pid=sites&srcid=ZGVmYXVsdGRvbWFpbnxqYW1lc3BydWdoMjAxNnxneDoyNDA4ZGVmMWFiZTNkODU1>

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

Class homework assignment on binary coding that will be assigned the previous class period.

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

Students are divided into groups of four. They will be introduced to the challenge as follows:

Cincinnati has been awarded an NBA franchise. You have been named vice president in charge of marketing. Your first responsibility is to choose a color for our team and send it to your partner. Be especially careful, for this is confidential information.

First iteration –

Step 1: choose a color

Step 2: use a substitution cipher to convert to numbers (substitution cipher)

Step 3: convert to binary

Step 4: send message

Debrief

Second iteration -

Step 1: choose a color

Step 2: use a substitution cipher to convert to numbers

Step 3: use the key for a shift (shifted substitution with key)

Step 4: convert to binary

Step 5: send message

Debrief

Third iteration -

Step 1: choose a color

Step 2: use a substitution cipher to convert to numbers

Step 3: use the key for a shift

Step 4: convert text to binary (shifted substitution with key and padding)

Step 5: apply padding

Step 6: send message (10 characters)

Debrief

Fourth iteration -

Step 1: choose a color

Step 2: use a substitution cipher to convert to numbers

Step 3: convert text to binary (shifted substitution with key, padding, and ex or)

Step 4: apply padding

Step 5: ex or

Step 6: send message (10 character)

Debrief

Introduce RSA

Why?

Authentication

Less communication is needed

The 4 iterations will take approximately 2 block periods. The RSA lesson will take 1 regular class day.

Notes: students should identify the vulnerabilities in sending “red” (just 3 letters), “green” (double letter), or blue/pink (4 letters). That limits them to yellow, purple, orange, turquoise, etc.

After the lesson on RSA, students are asked to read the article attached below. A quiz will follow the next day, and the answers will be encrypted using shifted substitution with key, padding, and ex/or.

<http://www.nationalcybersecurityinstitute.org/hactivism-terrorism-crime-and-espionage/ethics-in-cyber-security/>

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

A checklist will indicate the progress of each group based on different number theory concepts used in each iteration.

**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.

Each group will share out in a class discussion following the activity

|  |
| --- |
| **Differentiation:** The activity can be done using one of four methods, ranging from basic to more elaborate. Grouping will be based on ability, with the expectation that a top group would use a more difficult method of encryption. |

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

The two groups chose different challenges, despite the guiding questions. Each challenge employed the same encryption techniques, so this was not a problem. One group chose to encrypt a true statement about a teacher in our school and hide it in a classroom. An encrypted message was written on the board that led a group to the hidden statement. The other group chose to encrypt a press release about one of our teachers going into space.

In each case, students used a shifted Caesar cipher, binary code, and mono alphabetic substitution.

The challenges went well, but the timing could have been better. They were scheduled for the days leading up to Thanksgiving break. We could have use another day for the decryption of the messages, but we were up against the break and I had planned on introducing the next chapter in the text once we returned from break. As it was, students took the messages home and worked on the decryption on their own.