|  |  |  |
| --- | --- | --- |
| **Name: Ben Dougherty** | **Contact Info:** **Dougherty.benjamin@gmail.com** | **Date: 10/30/15** |

|  |  |  |  |
| --- | --- | --- | --- |
| **Lesson Title : Cryptography and Ethics** | **Unit #:****1** | **Lesson #:****2** | **Activity #:****4** |
| **Activity Title: Challenge: War Games** |

|  |  |
| --- | --- |
| **Estimated Lesson Duration:** | **7 Days** |
| **Estimated Activity Duration:** | **5 Days** |

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

|  |
| --- |
| **Activity Objectives: Students will use the cryptographic knowledge and ability they have developed throughout the unit to participate in a Cryptographic Scavenger Hunt.** |

|  |
| --- |
| **Activity Guiding Questions:** **How do we communicate securely with our team?****How can we break encoded messages?** |

| **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 New Learning Standards for Science (ONLS)** |
| --- |
| **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)** |

| **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, ONLS and/or CCSS):** |

HS.A.SSE.2 - Use the structure of an expression to identify ways to rewrite it.

HS.A.CED.2 - Create equations in two or more variables to represent relationships between quantities; graph equations on coordinate axes with labels and scales.

HS.A.REI.10 - Understand that the graph of an equation in two variables is the set of all its solutions plotted in the coordinate plane, often forming a curve (which could be a line).

HS.F.IF.1 - Understand that a function from one set (called the domain) to another set (called the range) assigns to each element of the domain exactly one element of the range. If f is a function and x is an element of its domain, then f(x) denotes the output of f corresponding to the input x. The graph of f is the graph of the equation y = f(x).

HS.F.BF.1.a.b.c - Write a function that describes a relationship between two quantities.

HS.F.BF.4.b.c - Find inverse functions.

HS.F.LE.5 - Interpret the parameters in a linear or exponential function in terms of a context.

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

Envelopes

Encoded Clues

Vigenere Square

Blank Caesar Cipher Aids

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

Enlist the assistance of other staff and faculty in the building to have someone present at each station.

Write clues to take teams to each station, and encrypt them using a variety of methods (Vigenere, Caesar, Affine, RSA, etc.).

Run copies of the encrypted clues and place them in envelopes.

Determine a “route” for each team, and organize each team’s clue envelopes accordingly.

On the day of the scavenger hunt, make sure that each volunteer for each station knows his/her role and has the appropriate clue envelopes and supplies for their stations.

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

For the scavenger hunt, students proceed through a series of stations, with a different task to complete at each station before they can proceed to the next.

Students begin the classroom, and each team must successfully complete a Diffie-Hellman exchange with the teacher to get the clue to take them to their second station.

I setup the team routes so that different teams did different stations in different orders to keep them all guessing. Here are the stations I used:

1) Diffie-Hellman exchange with teacher in starting classroom

2) Decipher Vigenere Cipher given the key-word

3) Break a Caesar Cipher

4) Break an Affine Cipher

5) Given a list of five different functions, find the inverse function of at least three of the five.

Once the team completed the task at each station, they received their clue to move to the next station. The scavenger hunt ended back in the classroom. The first team to complete the scavenger hunt and return to the classroom won.

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

Throughout the scavenger hunt, students will be testing different decryption strategies, and evaluating whether those strategies are working or not. The formative feedback is embedded in the activity of decrypting.

**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.

None

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

Students are given a copy of a Vigenere Square to help them in their decryption

Students are also given a blank Caesar Cipher aid to help them in their decryption

In designating the teams, students who have displayed stronger decryption skills are matched with students who have struggled more with decryption

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

Two students suggested a challenge for this unit before I could even begin to implement the challenge I had originally planned. Their idea was a kind of cryptographic scavenger hunt. They brought the idea up in class one day, and the rest of the students seemed excited about the idea. So, I decided to set aside the challenge I had designed for this unit, and build a challenge around their idea instead. The advantage to this was that there was a lot of “buy-in” from the students because it was their idea. The disadvantage was that I had to design a new challenge for the unit on short notice and set it up quickly. Ultimately though, I think this was a very positive change. Students used the Engineering Design Process at each stop along the scavenger hunt.

All students had to begin their scavenger hunt by successfully completing a Diffie-Hellman exchange with me to get their first clue. The locations were mixed up for each team, so teams were going in different directions, and didn’t really know whether they were ahead or behind of other teams. At each station, students received an enciphered message, and they had to decrypt the message to figure out where to go for their next stop on the scavenger hunt (to find their next clue). At each stop on the scavenger hunt students had to gather information about the enciphered message, they brainstormed possible decryption methods based on what kind of encryption they suspected was used on the message, and then they attempted their decryption solution, if it worked, they got the clue and moved on, if it didn’t, they had to refine their solution, and try a different decryption method. Throughout the scavenger hunt, students decrypted Caesar ciphers, Affine ciphers, Vigenère ciphers, and RSA ciphers. There was also one stop where the team was given a list of five functions, and they had to correctly compute the inverse of three of the five functions to get their clue for their next stop.

Ultimately, I would say that this modified challenge was a success. Students were very engaged in it. They used all the cryptographic and mathematical skills we had been building throughout the unit to accomplish a task. Although they could not refine their performance on the scavenger hunt as a whole, there was ample refining of solutions at each stop as teams worked to break the codes. The competitive nature of the task appealed to most of the students. I was surprised that the team that “won” the scavenger hunt was not the team with the students who seemed to do the best throughout the unit. The team that won, was the team that worked the best together as a team.