|  |  |  |
| --- | --- | --- |
| **Name: Amanda Sopko** | **Contact Info:** **Amanda.sopko@ih.k12.oh.us** | **Date: 7/02/15** |

|  |  |  |  |
| --- | --- | --- | --- |
| **Lesson Title : What is Cryptography?** | **Unit #:****1** | **Lesson #:****1** | **Activity #:****2** |
| **Activity Title: Secret Vs. Public Keys** |

|  |  |
| --- | --- |
| **Estimated Lesson Duration:** | **7 days** |
| **Estimated Activity Duration:** | **4 days** |

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

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

Students will

1. compare and contrast the pros and limitations of sharing messages privately vs. publicly.
2. use the order of operations to evaluate expressions.
3. use algorithms to substitute values in order to generate a secret key with a partner.

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

* How can I share a private message publicly?
* What algorithms can I use to send private information over a public forum?
* Why is it important to use the order of operations when evaluating algorithms?

| **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):** |

[CCSS.MATH.CONTENT.6.NS.B.2](http://www.corestandards.org/Math/Content/6/NS/B/2/)

Fluently divide multi-digit numbers using the standard algorithm.

[CCSS.MATH.CONTENT.6.EE.A.2.C](http://www.corestandards.org/Math/Content/6/EE/A/2/c/)

Evaluate expressions at specific values of their variables. Include expressions that arise from formulas used in real-world problems. Perform arithmetic operations, including those involving whole-number exponents, in the conventional order when there are no parentheses to specify a particular order (Order of Operations).

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

Diffie-Hellman and RSA Videos

Diffie-Hellman and RSA Practice Worksheet

Engineering Design Notebooks (EDN)

10 boxes with 2 latches (or 1 box for each group of 3)

30 padlocks with keys (or one for each student)

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

1. Prior to the lesson, have students watch the Diffie-Hellman and RSA videos.
2. Put out boxes to there is one box for every group of 3 students.
3. Put 2 locks with corresponding keys in each box.
4. Print off DIffie-Hellman and RSA Practice Worksheets.

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

DAY 1

1. Hook: Box Problem
	1. Arrange groups of three such that two students are sitting across from one another (students A and B) at a table/desk and the third student (E) is sitting between.
	2. Tell students that they must pass a coin from A to B in the box so that E cannot steal the coin.
	3. A and B cannot pass the box directly to each other, it must be passed through E.
	4. Allow groups to complete this task until they can successfully pass the coin without E taking it.
	5. Discuss successful strategies as a whole group.
	6. Have students write their strategies/strategies observed in their EDN.
2. Diffie-Hellman
	1. Introduce Diffie-Hellman and its significance to Cyber Security
	2. Review the video assignment and practice several problems with the students until they feel comfortable using the algorithm.
	3. Give students the Diffie-Hellman applet.
	4. With a partner, have the students work through the problems to discover that after 2 exchanges, both partners will always get the same remainder. Students should record all observations in their EDN.
	5. Conduct a whole group discussion on this phenomena and allow students to respond in their EDNs

DAY 2

1. RSA
	1. Introduce RSA and its significance to Cyber Security
	2. Review the video assignment and practice several problems with the students until they feel comfortable using the algorithm.
	3. Give students the RSA applet.
	4. Allow students to work with a partner and make observations in their EDN.
	5. Discuss solutions as a class.

DAY 3

1. Review the Chinese Remainder Theorem
	1. In their EDNs have students brainstorm ways to use the CRT to authenticate a message.
	2. Allow students to share their thoughts with the class.
2. Conduct a whole class discussion on the pros and cons of using each method. Allow students to make observations in their EDNs.
	1. Allow students to stand in one of three spots in the room depending on the method they think is most secure. Students who are undecided can stand in the middle of the room.
	2. Allow each side to give evidence to support their stance trying to win over students.

DAY 4

1. Revisit Box Problem with Active Attacker
	1. Review the Box Problem.
	2. This time, give person E a lock with key.
	3. Allow students to complete the exchange allowing person E to attempt to steal the coin.
	4. Discuss successful solutions and allow students to respond in their EDN.
2. Man in the Middle Attack
	1. Explain that this is a common attack used by hackers.
	2. Conduct a “Man in the Middle Attack” with the class.
	3. Revisit Diffie Hellman applet. Have students work in groups of 3 and allow interception.
	4. Have students write observations in their EDN and discuss the limitations of protecting a message from a Man in the Middle Attack.
	5. Assign students to research methods to prevent the middle man from stealing their data and write their findings in their EDNs.

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

Class discussion over the Hook.

Diffie-Hellman and RSA Practice work from applets

Diffie-Hellman/RSA Debate

**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.

All work in this lesson is prerequisite to the final “Coin Collection Challenge”. (See Lesson 2, Activity 4)

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

This lesson took more time than expected. The students did not feel comfortable with the exchanges and wanted to spend more time practicing them. I added a short video on modular arithmetic for the students to reference as needed. This can be found on document 1.1.02e. Since the Diffie Hellman Exchange took longer than expected. Only a small group of students were accelerated to learn the RSA Exchange.

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

The video lessons gave the students a good preview to the lesson and helped move the lesson along faster than if I were to teach without the preview. Due to the age and ability level of the students, it took more time for them to fully grasp the Diffie Hellman exchange. As a result, I did not require all students to use the RSA exchange.