|  |  |  |
| --- | --- | --- |
| **Name: Ben Dougherty** | **Contact Info:** **Dougherty.benjamin@gmail.com** | **Date: 10/5/15** |

|  |  |  |  |
| --- | --- | --- | --- |
| **Lesson Title : Introduction to Cryptography and the Mathematics of Cryptographic Systems** | **Unit #:****1** | **Lesson #:****1** | **Activity #:****2** |
| **Activity Title: Public Key (Asymmetric) Cryptography** |

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

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

|  |
| --- |
| **Activity Objectives:**1. **Students will be able to describe the difference between symmetric and asymmetric cryptographic systems.**
2. **Students will be able to use the Diffie-Hellman Key Exchange protocol to establish a secure channel with another party.**
3. **Students will use modular arithmetic to encrypt and decrypt messages.**
 |

|  |
| --- |
| **Activity Guiding Questions:**1. **What is the difference between symmetric and asymmetric key encryption systems?**
2. **Can two users establish a shared secret when communicating over an open channel?**
3. **Are asymmetric cryptographic systems breakable? If so, how?**
 |

| **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) |

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

Select values for g and p to simulate a Diffie-Hellman exchange (g=7 and p = 37). Select your own “b” value, and calculate your public key (33 in the example below).

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

Day 1:

When students walk into class the following instructions will be on the board:

Warm-up: Follow the instructions below using a calculator where needed:

1. Select a secret whole number (we’ll call this your “a”)
2. Raise the number 7 to the power of your secret number (“a”)
3. Divide the result of step 2 by 37, and record the REMAINDER. This is your special number.
4. Write your special number (the result of step 3) next to your name on the board.
5. Take Mr. Dougherty’s special number (33), raise it to the power of your secret number (“a”).
6. Divide the result of step 5 by 37, and record the REMAINDER. This is your second secret number (“s”).
7. Keep your first and second secret numbers private!

You can use this time to take attendance or whatever else you need to do. Also, as students write their “special” numbers up on the board, you can plug them into the Diffie-Hellman algorithm to get your shared secret with each student.

Start class with a Q&A session reviewing what you’ve covered so far with secret key encryption, substitution ciphers, function inverses, and the pros and cons of using these. Through the Q&A, lead students back around to the idea that a secret key (symmetric) requires a prior exchange of knowledge (a shared secret), and this is a problem when communicating at a distance over an open channel. Ask students if they still have their two secret numbers. Ask them if they would be impressed if you could tell them their second secret number (“s”) from step 6. Use the results of the Diffie-Hellman algorithm on their “special numbers” that they wrote on the board to “WOW” them by telling them their second secret number (“s”). Ask them if they’d like to know how you did that; presumably you will have sufficiently “WOW”ed them enough that they will want to know the trick. This opens the door to explain Diffie-Hellman.

Explain that the “special” number they wrote next to their names is their “public key”. Pair students up and have them run the Diffie-Hellman algorithm (steps 5-6) on their partner’s public key, and see if they get the same result. This would be a good place to introduce ideas of modular arithmetic and remainders. Also the identities:

$$\left(g^{a}mod p\right)^{b} mod p=\left(g^{b}mod p\right)^{a} mod p$$

$$g^{ab}mod p= \left(g^{a}mod p\right)^{b}mod p$$

Bring class back together for more Q&A:

So, you can establish a shared secret key with someone, what can you do with that? What good is that?

Hopefully someone comes up with the idea of using the shared secret as the numerical offset in a Caesar cipher. Have the pairs pass a message using a Caesar cipher with their shared secret as the Caesar cipher offset (use Diffie-Hellman Exercise Handout).

For homework have students come up with a plan for how an interceptor between the communicating parties could disrupt the security of Diffie-Hellman.

Day 2:

Start class off by having students present their plans to disrupt Diffie-Hellman. Put two random students as the sender and receiver; put the student with the plan between them as the interceptor, and let them try to disrupt the exchange. After a few attempts, introduce the concept of “man-in-the-middle” attacks, particularly the reflection attack. After you show this to the students (or they figure it out themselves), break them into groups and have them try to figure out how to thwart the MITM attack.

Ideally, students will arrive at the idea of needing authentication. We’ll use this as a way to introduce RSA Encryption.

Present instructional component on asymmetric key cryptography and RSA. This includes an activity for students to practice RSA encryption and decryption via a shared Google Document.

Special note to teacher: encrypt a silly or appropriately teasing comment using a student’s public key and put it on the Google Doc using another student’s name before the next class. (You can enlist a student as a co-conspirator in this plan.)

Day 3:

Open class by reviewing the RSA exercise from the previous day. Say you want to use an example from our Google Document. Pull up the Google document and pick the message that you planted there the previous day. Use the student’s private key to decrypt the message, and then chastise the student whom you impersonated for putting a slightly “negative” message up. That student will hopefully protest that it wasn’t them (you could inform this student ahead of class what you’re doing), which brings up the issue of someone impersonating someone else, and how, on an open channel, can we really be sure we’re talking to the person we think we are. At this point, I would tell the whole class that I had posted the message impersonating the student to illicit the conversation about authentication.

Present authentication PowerPoint, and have students send RSA encrypted messages with authentication per the instructions in the PointPoint. During the exercise, try to post fake messages to various students posing as other students so they can see what happens when a message does NOT authenticate!

Once everyone has practiced RSA authentication, group students and have them brainstorm ways to break RSA encryption. Give them the RSA Code Breaking Exercise for homework.

Day 4:

Begin class with a Q&A session to lead students toward the weaknesses of RSA. Lead students to the idea that “n” (the modulus) is a composite of two primes. If someone can find the primes p and q, then they can find (p-1)\*(q-1), and they already know your “e”, so they can solve (ex-dy=1) for a whole number solution that will decrypt.

See if anyone got this, and see if they broke the code. If they did, let them explain their process. If no one got this, then put students into groups and let them work on breaking this code using this method. Also have groups come up with a plan to prevent this attack.

Students may also realize that knowing the public key they can encrypt the alphabet using the receiver’s key and do a backwards lookup from the ciphertext back to the plaintext through such a table. Have them derive methods for preventing this attack as well.

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

The Diffie-Hellman exercise handout

The Google documents listed in the RSA activities

The RSA Code Breaking Exercise

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

Students who had difficulty with the modular arithmetic were given extra help, and when creating groups, students who had a stronger grasp of modular arithmetic were spread throughout the groups to support those students who were still struggling to grasp the concepts.

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

This lesson was much more difficult than I expected. Students grasped the concept of basic modular arithmetic relatively quickly. However, the deeper understanding of the special properties of modular arithmetic when combined with raising numbers with exponents took them longer than I expected to wrap their minds around; even at the end of the lesson, some students didn’t really get what was going on there (as the post-assessment data showed). Despite the fact that the mathematics of asymmetric encryption were the most challenging in the unit, and students across the board struggled with the technical details as well as the concepts, students did seem very interested in the ideas, and they thought it was cool to see how modern encryption is handled through the internet with different parties using public and private keys to both encrypt as well as authenticate. It was a real eye-opener for the students, and they seemed to genuinely enjoy “pulling back the curtain” on the encryption that they make use of on a daily basis through their cell phones and internet usage.

Next time, I will start the lesson with more of the “high-level” conceptual understanding of how asymmetric encryption and authentication work (making use of some good videos I found on YouTube), before diving into the more technical aspects of the mathematics. I did a lot of this too late, after students had gotten bogged down in the technical mathematics, and some students lost interest because of this. I will also plan more time for this portion of the unit in the future, as it took much longer than I expected to convey all of this, and to let students grapple with it.