The Mathematics of Cryptography and Cyber Security

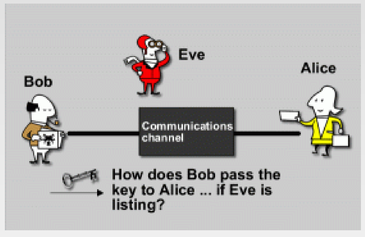
Amanda Sopko
Indian Hill Middle School, Mathematics/STEM

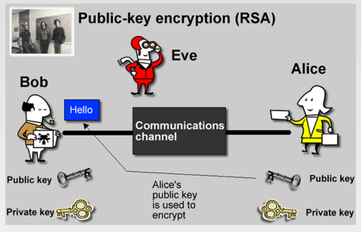
RET is funded by the National Science Foundation, grant # EEC-1404766

What is Cryptography?

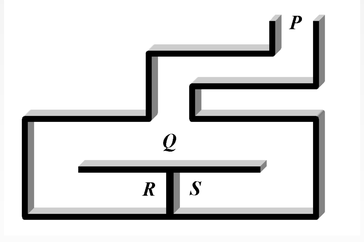
Cryptography comes from the Greek words *cryptos* meaning hidden and *graphos* meaning writing. Therefore, cryptography is the study of hidden or secret writing.

Diffie-Hellman and RSA exchanges help us send messages by encrypting then decrypting data.



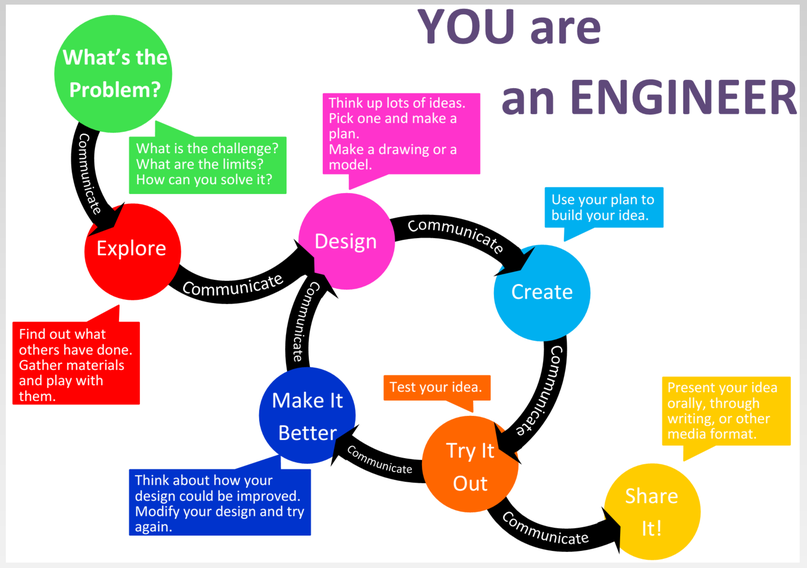


Cryptographers and Cryptanalysts have put protocols, such as Zero Knowledge Proof, in place to authenticate messages.



Cryptographers and Cryptanalysts have put protocols in place to ensure message integrity.

How will we approach this topic?



Questions?

Can you define a problem?

Can an engineer help solve this problem?

Are you part of the solution?

Why should I care about cryptography?

Who reads your text messages?

Are your emails ONLY going to the intended recipients?

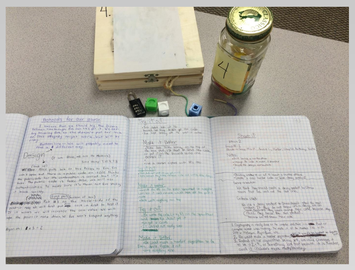
The Mathematics of Cryptography and Cyber Security

Amanda Sopko
Indian Hill Middle School, Mathematics/STEM

RET is funded by the National Science Foundation, grant # EEC-1404766

Big Idea/Challenge

Big Idea: How can we use mathematics to safely send and receive messages that are confidential, unmodified, and received from and by the intended person?



Challenge: Use cryptographic methods to develop a set of protocols to encrypt the combination of your locked box in order to safely pass coins to your teammates through a third party attacker.

Unit Structure

Essential Questions (written by students):

- What is cryptography?
- How can I keep messages safe?
- What are the different types of encryption?
- How can I communicate a key for my code?
- How do I know if my code is strong?

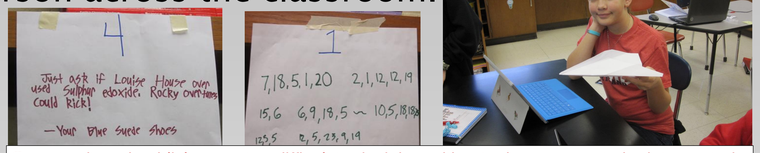
Standards:

CCSSMATH CONTENT: 6.NS.B.2, 6.EE.A.2.C, 7.EE.B.4, 7.SP.C.5
CCSS.ELA-LITERACY: RI.6.1, W.6.1

Objectives: Students will apply what they know about the order of operations and the division algorithm to develop cryptographic protocols to safely send secure messages.

Unit Activity Implementation

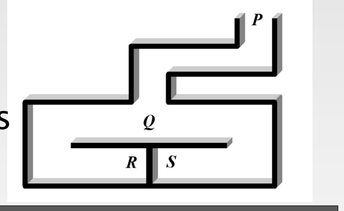
Hook: Students experimented with a variety of methods for sending messages intended for one person across the classroom.



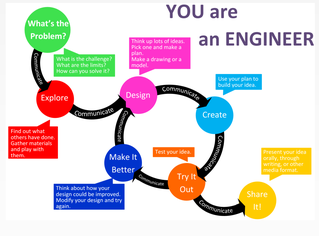
Secrets shared publicly were too difficult to decipher without a key or easy to be intercepted.

Diffie-Hellman Exchange/Man in the Middle Attack: Students sent messages through a third party in locked boxes with each person having a unique key/lock.

Ali Baba's Cave: Students experimented with and discussed methods for authentication.

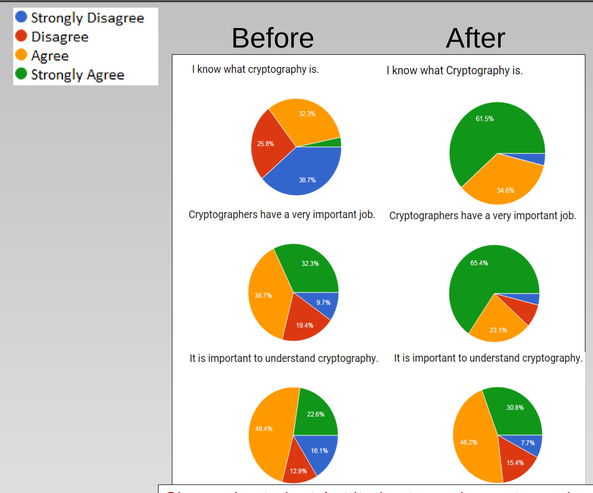


Engineering Design Process

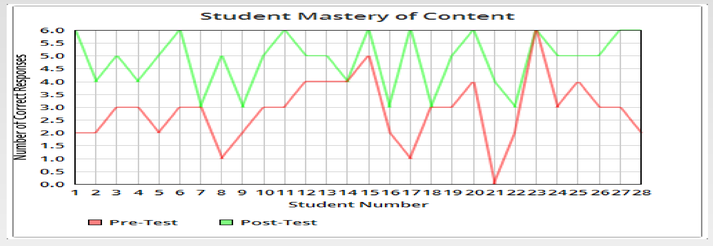


Students worked in teams to research, develop, evaluate, and share cryptographic protocols. They considered the risks associated with their choices and interpreted their learning via class blog and Engineering Design Notebooks throughout the unit.

Student Work and Results



Change in students' attitudes towards cryptography.



Reflection and Conclusion

- Increased engagement in the field of cryptography as well as mathematics.
- Increased mastery of the content standards.

A.C.S.

- Students worked in teams as cryptographers and cryptanalysts to complete the challenge.
- Met a member of the NSA and experiment with code cracking.
- Worked with a UC professor working in this field.
- Recognized the need for cryptography in everyday life.