Securing Cyberspace

Ben Dougherty
Purcell Marian High School, Mathematics 11-12

Securing Cyberspace

- Cryptography
  - Symmetric vs. Asymmetric Keys
  - Substitution Ciphers
  - Chinese Remainder Theorem
  - Diffie-Hellman Key Exchange

A password is like a toothbrush
- Choose a good one
- Don't share it with anyone
- Change it occasionally

- Mathematics
  - Modular Arithmetic
  - Linear Models
  - Function Inverses

Password + Proof = Access
? + Is that you? = Success!

- Cryptographic Pedagogy
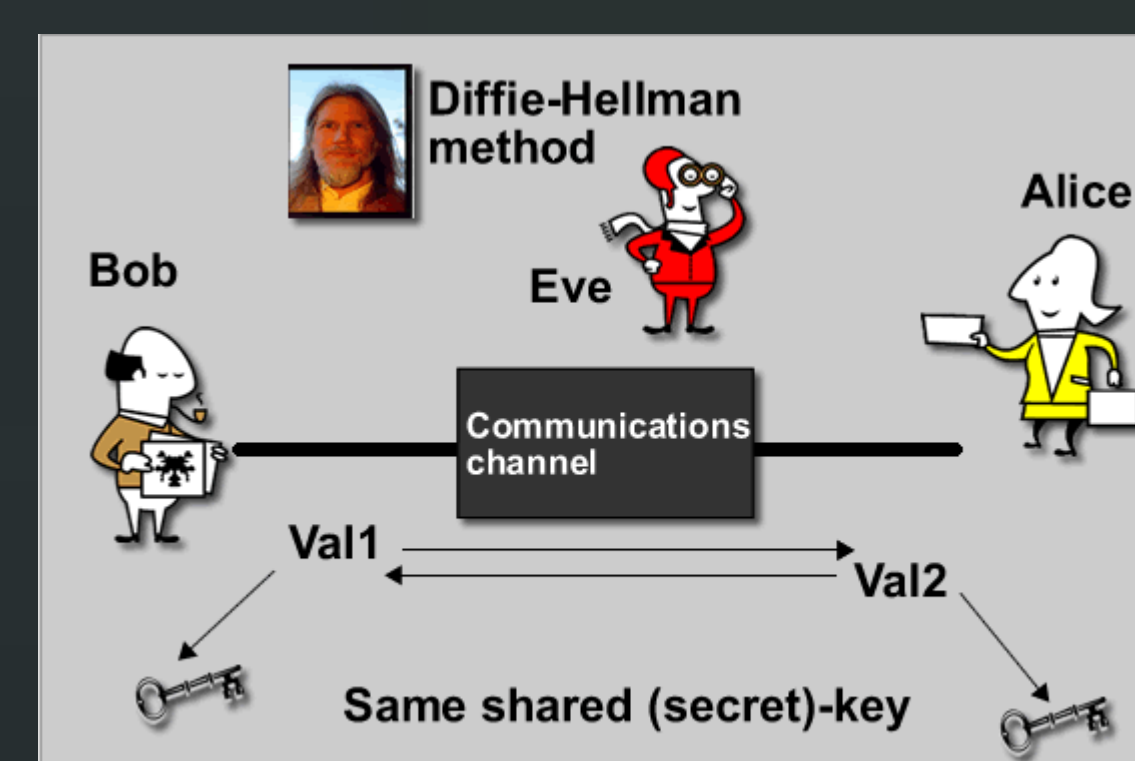 - Interactivity
  - Hands-on Activities
  - Games

How can this be brought into the classroom?

Students will explore the math and history behind cryptography

Students will experiment with different cryptographic systems

Diffie-Hellman method
Bob   Eve   Alice
Communications channel
Val1   Val2
Same shared (secret)-key

Students will experiment with different code breaking techniques

Students will use their code making and breaking skills to design their own cryptographic protocols
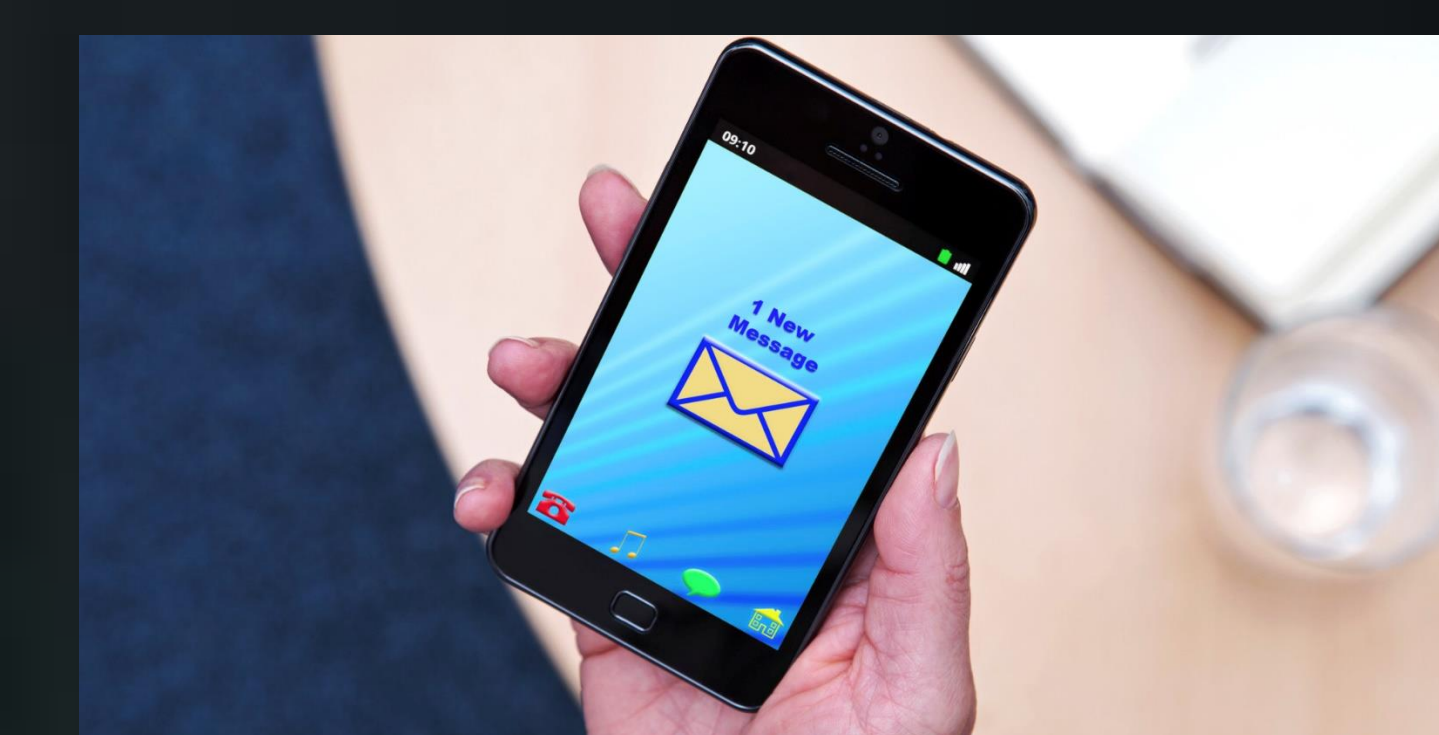
- Challenge
  - Formulate
  - Compute
  - Validate
  - Interpret
- Report
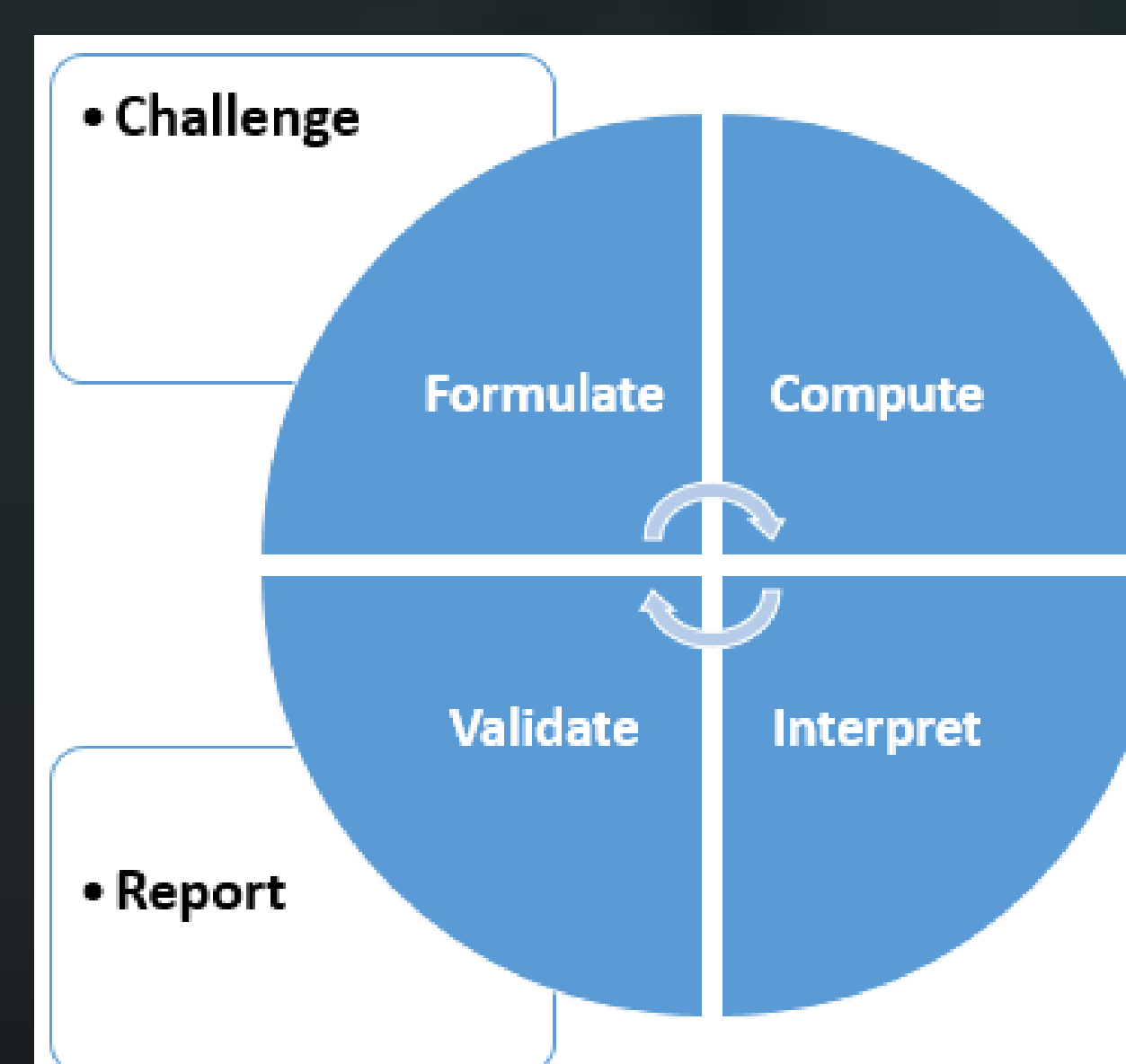
Why should I care about cryptography?

Is your data safe?

Who's reading your messages?

Is our nation vulnerable to cyber attacks?

Kara T on Artem
It was so cheesy to fall for my dancer P10

A perfect storm' of cyber attacks

How can we protect ourselves?