1) History of Encryption

Julius Caesar's Cipher (c. 58-50 BCE):

Simple substitution cipher, now famously known as the Caesar Cipher, to secure military communications during his campaigns.

A → C
B → F

2) What is a cypher

What are two things we need if you want a secret code?

1. Hard for enemies to read
2. Easy for friends to read

How can we address point 1?

Need a Key to read it

How can we address point 2?

Only give friends Keys

Go to your stations and try to come up with *(not necessarily math related)* methods to create secret messages.

3) How can we use Prime Factorization to encrypt?

Computer run on math. How can we create digital cyphers using math?

For a math method to be good for encryption is must be _____easy_____ to solve one way, and _____hard_____ to solve another.

What are complicated maths?

Finding the prime factors of a number

What are simple maths?

Multiplication & division

Go to your stations and attempt to come up with a math problem that easy to solve one way, and difficult to solve another.

Hint: If you give a friend a piece of information, does it make Prime Factorization easier?

Can PF easier if you know the factors even if you don't know their power

$176 = 2^4 \times 11^1$