WEEK 2 SCHEDULE

(1) **Monday**
- New teams.

(a) Morning Activity 1. Euclidean Algorithm and Bezout numbers.
(b) Morning Activity 2. Autokey and Substitution ciphers.
(c) Morning activity 3. Different bases if we have time.
(d) Afternoon Computer Lab. Implement general substitution cipher. Make tools to help with decryption of general substitution ciphers. If time, also do autokey.

(2) **Tuesday**
- Classical cipher review.

(a) Morning Activity 1. Numbers in different bases. Base 26 will be particularly important for us.
(b) Morning Activity 2. Make your own classical Cipher (some discussion of historical ciphers). Practice encrypting and decrypting with it.
(c) Discrete Log / primitive root and generators (if time).
(d) Afternoon Computer Lab. Games. If time, implement your own team's ciphers.

(3) **Wednesday**

(a) Morning Activity 1. Primitive roots / generators. Explicitly stated (if we didn't already do it).
(b) Morning Activity 2. Diffie-Hellman idea. First attempt. Introduction to asymmetric ciphers.
(c) Morning Activity 3. Euler Phi (if time).
(c) Afternoon Computer Lab. GCDs and Bezout numbers.

(4) **Thursday**

(a) Morning Activity 1. Euler Phi. Look for patterns. List of patterns.
(b) Morning Activity 2. ElGamal. Practice by hand. Cryptographic/digital signatures.
(c) Morning Activity 2. Scavenger Hunt #2.
(d) Afternoon Computer Lab. Implement strings to numbers and numbers to strings. (Implement your team's own classical cipher - if you can). Implement some factoring.