Problems for Recitation 5

1 RSA: Let's try it out!

You'll probably need extra paper. *Check your work carefully!*

1. As a team, go through the **beforehand** steps.

   (a) Choose primes p and q to be relatively small, say in the range 5-15. In practice, p and q might contain several hundred digits, but small numbers are easier to handle with pencil and paper.

   (b) Calculate $n = pq$. This number will be used to encrypt and decrypt your messages.

   (c) Find an $e > 1$ such that $\gcd(e, (p-1)(q-1)) = 1$.
   The pair (e, n) will be your *public key*. This value will be broadcast to other groups, and they will use it to send you messages.

   (d) Now you will need to find a d such that $de \equiv 1 \pmod{(p-1)(q-1)}$.

   - Explain how this could be done using the Pulverizer. (Do not carry out the computations!)
   - Find d using Euler's Theorem given in yesterday's lecture.
     The pair (d, n) will be your *secret key*. Do not share this with anybody!

   When you're done, write your public key and group members' names on the board.

2. Now ask your recitation instructor for a message to encrypt and send to another team using *their* public key.

   The messages m correspond to statements from the codebook below:

   2 = Greetings and salutations!

   3 = Wassup, yo?

   4 = You guys are slow!

   5 = All your base are belong to us.

   6 = Someone on *our* team thinks someone on *your* team is kinda cute.

   7 = You are the weakest link. Goodbye.

3. **Encode** the message you were given using another team's public key.

4. Now **decrypt** the message sent to you and verify that you received what the other team sent!

5. Explain how you could read messages encrypted with RSA if you could quickly factor large numbers.

RSA Public-Key Encryption

Beforehand The receiver creates a public key and a secret key as follows.

1. Generate two distinct primes, p and q.
2. Let $n = pq$.
3. Select an integer e such that $\gcd(e, (p-1)(q-1)) = 1$.
   The *public key* is the pair (e, n). This should be distributed widely.
4. Compute d such that $de \equiv 1 \pmod{(p-1)(q-1)}$.
   The *secret key* is the pair (d, n). This should be kept hidden!

Encoding The sender encrypts message m to produce m' using the public key:

$$m' = \text{rem}\,(m^e, n)$$

Decoding The receiver decrypts message m' back to message m using the secret key:

$$m = \text{rem}\,((m')^d, n).$$