Overview of where we are in the semester:

- **Data Exchange:** AES is a secure way to exchange messages
  Symmetric encryption scheme that requires a shared private key
- **Question:** How do you exchange the private key to begin with?
  Must use an public key (i.e. asymmetric) scheme, like DHKE or RSA

Diffie-Hellman Key Exchange in $\mathbb{F}_p^*$

- Security depends on the DHP being hard to solve
- If can solve the DLP $g^x \equiv h \mod p$ then can solve DHP
  - Shank's: collision algorithm, potentially requires large amount of storage
  - Pollard's ρ: collision algorithm that uses $\mathcal{O}(1)$ storage
  - Pohlig-Hellman: Breaks DLP into smaller DLP's based on factors of $\text{ord}(g)$
    - Use Shank's or Pollard's ρ to solve smaller DLPs
    - Use Chinese Remainder Theorem to reassemble into solution of larger DLP
    - Reduces security of DLP to level of security based on largest factor of $\text{ord}(g)$
- Motivation for finding elements g of large prime order q in $\mathbb{F}_p$
  Exercise 1.33 gives method to find these elements with very high probability
- Still need to know how to find large primes p where $p - 1$ has large prime factor q

Recall RSA

- **Alice – Key Creation**
  - Choose secret primes p and q, form $N = pq$
  - Choose exponent e with $\gcd(e, \phi(N)) = 1$
  - Compute private $d \equiv e^{-1} \mod \phi(N)$ using EEA or Fermat's Little Theorem
  - Publish (N, e)
- **Bob – Encrypt plaintext** $m \in \mathbb{Z}_N$
  - Use Alice's public key (N, e) to compute $c \equiv m^e \mod N$
  - Send ciphertext c to Alice
- **Alice – Decrypt ciphertext** c
  - $c^d \equiv m^{de} \mod N \equiv m \mod N$

Security of RSA

- (N, e) are public information
- If can figure out $\phi(N) = (p-1)(q-1)$, then easy to find private key d
- Security of RSA depends upon it being hard to factor $N = pq$
- How do we find large primes p and q?

1. Find a Miller-Rabin witness for $n = 2465$.
   Perform this calculation by hand, although you can use your favorite computing device for modular arithmetic.

2. Show that $n = 2^{1341} - 19$ is composite by finding a Miller-Rabin witness.
   The Mathematica notebook posted for today may be useful.

3. Find a Miller-Rabin witness for $n = 2^{1279} - 1$

4. Your goal is to find a 20-bit pseudoprime number n
   (a) How many 20-bit numbers do you expect that you will need to pick, on average, before finding a prime?
   (b) Use today's Mathematica notebook to find a 20-bit pseudoprime.
   How confident are you that your n is a pseudoprime?

   You may use Mathematica's RandomInteger[ ] command, but NOT the RandomPrime[ ] command. That would be cheesy.