SPCS CRYPTOGRAPHY
HOMEWORK 9 (OPTIONAL)

Spend time on your project first - just do the ones in this p-set that interest you. You are strongly encouraged to work in groups, but you have to write up the solution on your own.

Reference for today's lecture: Chapter 12.2-12.4; For $p-1$-method, see `https://math.berkeley.edu/~sagrawal/su14_math55/notes_pollard.pdf`

1. Compute the number of B-smooth number from 2 to X (inclusive):
   (a) $X = 25$, $B = 3$.
   (b) $X = 35$, $B = 5$.

2. If n is B-power smooth, prove that it is also B-smooth. Is the converse true?

3. Use $p-1$ method to factorize
   (a) 1739.
   (b) 220459.

\# 4. For each of the following numbers n, compute the values of

$$n + 1^2, n + 2^2, n + 3^2, \cdots,$$

as we did in class, until you find a value $n + b^2$ that is a perfect square a^2. Then use the values of a and b to factor n.
   (a) $n = 53357$.
   (b) $n = 34571$.

5. Use the quadratic sieve/Dixon's method to factor the following numbers.
   (a) $n = 61063$. Hint:

$$1882^2 \equiv 270 \mod 61063 \quad \text{and} \quad 270 = 2 \cdot 3^3 \cdot 5$$
$$1898^2 \equiv 60750 \mod 61063 \quad \text{and} \quad 60750 = 2 \cdot 3^5 \cdot 5^3$$

   (b) $n = 52907$. Hint:

$$399^2 \equiv 480 \mod 52907 \quad \text{and} \quad 480 = 2^5 \cdot 3 \cdot 5$$
$$763^2 \equiv 192 \mod 52907 \quad \text{and} \quad 192 = 2^6 \cdot 3$$
$$773^2 \equiv 15552 \mod 52907 \quad \text{and} \quad 15552 = 2^6 \cdot 3^5$$
$$976^2 \equiv 250 \mod 52907 \quad \text{and} \quad 250 = 2 \cdot 5^3$$

\# 6. Prove that n is B-power smooth if and only if n divides the least common multiple of $1, 2, \cdots, B$.

7. Suppose Bob leaks his private key d to Eve. Instead of choosing a new n, he decides to choose a new public key e thus a new private key d, but with the same value of n. Is this safe? (That is, can Eve decrypt messages now?)

8. Alice and Bob are such good friends that they choose to use RSA with the same n, but their public keys e and f are different, and indeed, they are relatively prime. Charles wants to send the same message m to Alice and Bob. If Eve intercepts both of his messages, how can she recover the plaintext message m?

⋆ 9. A *multiplicative function* $f : \mathbb{N} \to \mathbb{R}$ is a function such that whenever $gcd(a, b) = 1$, we have $f(a)f(b) = f(ab)$. We said in class that Euler's ϕ function is one such example.
   (a) Prove that Euler's ϕ function is multiplicative.
   (b) The *divisor function*, $d(n)$, counts the number of divisors of n. For example, 3 has two divisors 1 and 3, so $d(3) = 2$. 12 has 6 divisors: 1,2,3,4,6,12, so $d(12) = 6$.
   Prove that $d(n)$ is multiplicative.
   (c) Find a formula for $d(p^e)$ for a prime p and positive integer e. Deduce a formula for $d(n)$, in terms of the prime factorization of $n = p_1^{e_1} \cdots p_k^{e_k}$.
   (d) The *Mobius function*, $\mu(n)$ is defined as follows.

$$\mu(n) = \begin{cases} 0 & \text{if } n \text{ is divisible by square of a prime} \\ (-1)^r & \text{if } n \text{ is the product of } r \text{ distinct primes} \end{cases}$$

   Prove that $\mu(n)$ is multiplicative.

⋆ 10. Here is another example of a public key cryptosystem. Bob chooses two large primes p and q and he publishes $n = pq$. It is assumed that n is hard to factor. Bob also chooses three random numbers g, r_1, and r_2 modulo n and computes

$$g_1 \equiv g^{r_1(p-1)} \bmod n \text{ and } g_2 \equiv g^{r_2(q-1)} \bmod n.$$

His public key is the triple (n, g_1, g_2) and his private key is the pair of primes (p, q).

Alice wants to send the message m to Bob, where m is a number modulo n. She chooses two random integers s_1 and s_2 modulo n and computes

$$c_1 \equiv m g_1^{s_1} \bmod n \text{ and } c_2 \equiv m g_2^{s_2} \bmod n.$$

Alice then sends the ciphertext (c_1, c_2) to Bob.

Decryption is extremely fast and easy. Bob uses the Chinese remainder theorem to solve the pair of congruences

$$\begin{cases} x \equiv c_1 \bmod p \\ x \equiv c_2 \bmod q \end{cases}$$

   (a) Prove that Bob's solution x equals Alice's plaintext m.
   (b) Explain why this cryptosystem is not secure.