SPCS CRYPTOGRAPHY
HOMEWORK 8

Please try all the unmarked problems. #, ⋆ problems are both optional, with ⋆ problems being harder. 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 10.5 - 10.6; Chapter 11.1, Chapter 12.1-12.2

1. Recall that Euler's phi function $\phi(n)$ is the function defined by

   $$\phi(n) = \text{ number of positive integers up to } n \text{ that are relatively prime to } n$$

   Equivalently, $\phi(n)$ is the number of elements of $(\mathbb{Z}/n\mathbb{Z})^*$.
   (a) Compute the values of $\phi(9), \phi(15), \phi(28)$.
   (b) If we let n have prime factorization $p_1^{e_1} \cdots p_k^{e_k}$, write down a formula for $\phi(n)$ in terms of $p_1, \cdots, p_k, e_1, \cdots, e_k$. In particular, it means that one can compute $\phi(n)$ quickly if we know the factorization of n.
   ⋆ (c) Prove *Euler's totient function theorem*,

   $$a^{\phi(n)} \equiv 1 \bmod n \text{ for all integers } a \text{ satisfying } gcd(a, n) = 1.$$

   (Hint: Mimic the proof of Fermat's little theorem. Instead of looking at all the multiples of a, just look at the multiples ka with $gcd(k, n) = 1$.)

2. Using Euler's totient function theorem, or Chinese remainder theorem, or otherwise, compute
   (a) $7^{26} \bmod 72$.
   (b) $3^{48} \bmod 112$.

3. Alice wishes to communicate with Bob using RSA. Suppose that Bob chooses $p = 3701$, $q = 7537$, $n = pq$ and $e = 443$.
   (a) What is his private key d?
   (b) Alice wishes to send the message $m = 11034007$. What is her ciphertext?
   (c) Alice sends another message, and his ciphertext is c = 3003890. What was her plaintext message?

4. A deck of 52 cards is shuffled and the top eight cards are turned over.
   (a) What is the probability that the king of hearts is visible?
   (b) A second deck is shuffled and its top eight cards are turned over. What is the probability that a visible card from the first deck matches a visible card from the second deck?

5. Factorize the following numbers using Pollard's ρ method, using the polynomial $f(x) = x^2 + 1$. You can also use other polynomials, but specify them if you do so.
   (a) 8051
   (b) 140299

6. Can you use RSA for key exchange? In other words, if Alice and Bob must agree on a secret key for further communication through a public channel, can they use RSA to do it?

7. Eve knows that Bob is using RSA system. In particular, she knows the public key (n, e) Bob published, where $n = pq$ is a product of two large primes. Through espionage, Eve discovers $\phi(n) = (p-1)(q-1)$.

How can she recover p, q and Bob's private key d?

8. Bob publishes his public key (n, e). Suppose that Eve tricks Bob into telling her his private key d. Does this help her find the factorization of n?