CS 70 Discrete Mathematics and Probability Theory
Fall 2013 Vazirani RSA Practice

1. **Euler and Little Fermat**

   (a) What is $7^{3,000,000,000}$ mod 41? Justify your answer.

   (b) What is $2^{3^{2,001}}$ mod 47? Show your work. (Note that a^{b^c} means $a^{(b^c)}$, not $(a^b)^c$.)

   [Hint: Use the theorems alluded to in the title of this problem.]

2. **Fermat's Little Theorem**

   Fermat's Little Theorem states that, if p is prime, then for any $a \in \{1,2,\ldots,p-1\}$, $a^{p-1} = 1 \bmod p$.

   (a) Prove Fermat's Little Theorem. [HINT: Show that the set of $p-1$ numbers $\{a\cdot 1, a\cdot 2, \ldots, a\cdot(p-1)\}$ are all distinct and non-zero mod p. Then multiply them together.]

   (b) Suppose you wish to use a triple prime analog of RSA. Let $N = pqr$, where p,q,r are primes. Suppose that $gcd(e,(p-1)(q-1)(r-1)) = 1$. Show that $E(x) = x^e \bmod N$ is a bijection. What is the decryption key?

3. **RSA**

   Show how to determine p and q given N and $\varphi(N) = (p-1)(q-1)$. (In other words, given N and the value $\varphi(N) = (p-1)(q-1)$, it is possible to factor N efficiently. This shows that determining $\varphi(N)$ is "as hard as factoring.")

4. **RSA**

   In this problem you play the role of Amazon, who wants to use RSA to be able to receive messages securely.

   (a) Amazon first generates two large primes p and q. He picks $p = 13$ and $q = 19$ (in reality these should be 512-bit numbers). He then computes $N = pq$. Amazon chooses e from $e = 37, 38, 39$. Only one of those values is legitimate, which one? (N,e) is then the public key.

   (b) Amazon generates his private key d. He keeps d as a secret. Find d. Explain your calculation.

   (c) Bob wants to send Amazon the message $x = 102$. How does he encrypt his message using the public key, and what is the result?

   (d) Amazon receives an encrypted message $y = 141$ from Charlie. What is the unencrypted message that Charlie sent him?

5. **Squaring**

   In practical implementations of RSA, it is common to use $e = 3$ as the public exponent, because this provides performance enhancements.

   Could we use $e = 2$ for RSA encryption? Why or why not?

6. **Easy RSA**

   In class, we said that RSA uses as its modulus a product of two primes. Let's look at a variation that uses a single prime number as the modulus. In other words, Bob would pick a 1024-bit prime p and a public exponent e satisfying $2 \leq e < p-1$ and $\gcd(e, p-1) = 1$, calculate his private exponent d as the inverse of e modulo $p-1$, publish (e, p) as his public key, and keep d secret. Then Alice could encrypt via the equation $E(x) = \mod(x^e, p)$ and Bob could decrypt via $D(y) = \mod(y^d, p)$.

   Explain why this variation is insecure. In particular, describe a procedure that Eve could use to recover the message x from the encrypted value y that she observes and the parameters (e, p) that are known to her. Make sure to justify why Eve could feasibly carry out this procedure without requiring extravagant computation resources.

7. **OpRSA**

   Anonymous is running a website and needs to be able to securely receive information from people with something interesting to say about a certain potential target. Your job is to help them set up a crypto-system to accomplish this task.

   (a) Anonymous first generates two large primes, p and q. They pick $p = 13$ and $q = 19$ (though in reality these should be 512-bit numbers). They then computes $N = pq$. Anonymous chooses e from $\{37, 38, 39\}$. Only one of these values is legitimate; which one? (N, e) is then the public key.

   (b) Anonymous needs to generate a private key, d, which will be kept as a secret. Help Anonymous find d and explain your calculation.

   (c) Brain wants to send Anonymous the message $x = 102$. How does he encrypt his message using the public key and what is the result?

   (d) Anonymous receives the encrypted message $y = 141$ from Candy, another informant. What is the unencrypted message that Candy sent?

   (e) Try encrypting several other messages (you're free to choose, as long as they're valid). Do you see anything wrong with this crypto-system? (In the real world, Anonymous is a lot smarter than this.)

8. **Because the Moth just doesn't cut it**

   Gandalf the Grey (a good wizard) wanders about on his merry adventures but frequently runs into some troubles with goblins and orcs along the way. Always being the well-prepared wizard that he is, Gandalf has enlisted the service of the Great Eagles to fly him out of sticky situations at a moment's notice. To do this, he broadcasts a short message detailing his dilemma and a nearby eagle will come to his aid.

   While this is all well and good, Saruman the White (an evil wizard) wants in on this eagle concierge service. The eagles can no longer trust just any distress call they receive! Gandalf needs you (a cryptography master) to help him devise a simple scheme that will allow the eagles to verify his identity whenever he broadcasts a message out. Not only that, but the eagles need to know when the message they receive from Gandalf has been tampered with.

   Once you have devised this scheme, Gandalf will tell it to the eagle lord Gwaihir, who will relay it out to the rest of the world (they are loudmouths so they can't keep a secret).

   To summarize:

   (a) Gandalf broadcasts a message m to all of Middle-Earth.

(b) He is able to attach to the message an extra piece of information s that verifies his identity (i.e. cannot be forged) to whomever receives it.

(c) If the message has been modified in transit, recipients of the modified message should be able to detect that it is not original.

(d) Everyone in Middle-Earth knows the scheme (i.e. the algorithm itself is not a secret)

Your job in this problem is to devise an algorithm (like RSA) that meets the above criteria. In your answer, you should formally prove that Gandalf's messages can be successfully verified. You do not need to formally prove (though it should still be the case) that it is difficult to forge/tamper with messages, but you should provide some informal justification.