Tom Leighton and Ankur Moitra

Problems for Recitation 5

The RSA Cryptosystem

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

(a) Generate two distinct primes, p and q. Since they can be used to generate the secret key, they must be kept hidden.

(b) Let $n = pq$.

(c) 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.

(d) Compute d such that $de \equiv 1 \pmod{(p-1)(q-1)}$. This can be done using the Pulverizer.
The *secret key* is the pair (d, n). This should be kept hidden!

Encoding Given a message m, the sender first checks that $\gcd(m, n) = 1$.[1] The sender then 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:

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

[1]It would be very bad if $\gcd(m, n)$ equals p or q since then it would be easy for someone to use the encoded message to compute the secret key If $\gcd(m, n) = n$, then the encoded message would be 0, which is fairly useless. For very large values of n, it is extremely unlikely that $\gcd(m, n) \neq 1$. If this does happen, you should get a new set of keys or, at the very least, add some bits to m so that the resulting message is relatively prime to n.

1 Let's try out RSA!

(a) Go through the **beforehand** steps.

- Choose primes p and q to be relatively small, say in the range 10–40. In practice, p and q might contain hundreds of digits, but small numbers are easier to handle with pencil and paper.
- Try $e = 3, 5, 7, \ldots$ until you find something that works. Use Euclid's algorithm to compute the gcd.
- Find d (using the Pulverizer).

When you're done, put your public key on the board labeled "Public Key." This lets another team send you a message.

(b) Now send an encrypted message to another team using their public key. Select your message m from the codebook below:

- 2 = Greetings and salutations!
- 3 = Yo, wassup?
- 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.

(c) Decrypt the message sent to you and verify that you received what the other team sent!

Try to send at least two messages and to decode at least one received message.

2 Cracking RSA

$\phi(n)$ is the number of positive integers less than n that are relatively prime to n. In particular, if $n = pq$ for primes p, q, then $\phi(n) = (p - 1)(q - 1)$. This is referred to as Euler's totient function.

(a) Just as RSA would be trivial to crack knowing the factorization into two primes of n in the public key, explain why RSA would also be trivial to crack knowing $\phi(n)$.

(b) Show that if you knew n, $\phi(n)$, and that n was the product of two primes, then you could easily factor n.

3 Sending signed messages

Suppose Alice and Bob are using the RSA cryptosystem to send secure messages. Each of them has a public key visible to everyone and a private key known only to themselves, and using RSA in the usual way, they are able to send secret messages to each other over public channels.

But a concern for Bob is how he knows that a message he gets is actually from Alice—as opposed to some imposter claiming to be Alice. This concern can be met by using RSA to add unforgeable "signatures" to messages. To send a message m to Bob with an unforgeable signature, Alice uses RSA encryption on her message m, but instead of using Bob's public key to encrypt m, she uses her own *private* key to obtain a message m_1. She then sends m_1 as her "signed" message to Bob.

(a) Explain how Bob can read the original message m from Alice's signed message m_1. (Let (n_A, e_A) be Alice's public key and d_A her private key.

(b) Briefly explain why Bob can be confident, assuming RSA is secure, that m_1 came from Alice rather than some imposter.

(c) Notice that not only Bob, but *anyone* can use Alice's public key to reconstruct her message m from its signed version m_1. So how can Alice send a secret signed message to Bob over public channels?

(d) Given the public key (5, 1073), and the encrypted message 33, what is the original message?

4 Dressed to the nines.

Give a proof by induction that $10^k \equiv 1 \pmod 9$ for all $k \geq 0$. Why is a number written in decimal evenly divisible by 9 if and only if the sum of its digits is a multiple of 9?