# 1   RSA Warm-Up

Consider an RSA scheme modulus $N = pq$, where $p$ and $q$ are distinct prime numbers larger than 3.

(a) Recall that $e$ must be relatively prime to $p-1$ and $q-1$. Find a condition on $p$ and $q$ such that $e = 3$ is a valid exponent.

(b) Now suppose that $p = 5$, $q = 17$, and $e = 3$. What is the public key?

(c) What is the private key?

(d) Alice wants to send a message $x = 10$ to Bob. What is the encrypted message she sends using the public key?

(e) Suppose Bob receives the message $y = 24$ from Alice. What equation would he use to decrypt the message?

# 2   RSA with Multiple Keys

Members of a secret society know a secret word. They transmit this secret word $x$ between each other many times, each time encrypting it with the RSA method. Eve, who is listening to all of their communications, notices that in all of the public keys they use, the exponent $e$ is the same. Therefore the public keys used look like $(N_1, e), \ldots, (N_k, e)$ where no two $N_i$'s are the same. Assume that the message is $x$ such that $0 \le x < N_i$ for every $i$.

(a) Suppose Eve sees the public keys $(p_1 q_1, 7)$ and $(p_1 q_2, 7)$ as well as the corresponding transmissions. Can Eve use this knowledge to break the encryption? If so, how? Assume that Eve

cannot compute prime factors efficiently. Think of $p_1, q_1, q_2$ as massive 1024-bit numbers. Assume $p_1, q_1, q_2$ are all distinct and are valid primes for RSA to be carried out.

(b) The secret society has wised up to Eve and changed their choices of $N$, in addition to changing their word $x$. Now, Eve sees keys $(p_1 q_1, 3)$, $(p_2 q_2, 3)$, and $(p_3 q_3, 3)$ along with their transmissions. Argue why Eve cannot break the encryption in the same way as above. Assume $p_1, p_2, p_3, q_1, q_2, q_3$ are all distinct and are valid primes for RSA to be carried out.

(c) Let's say the secret $x$ was not changed, so they used the same public keys as before, but did not transmit different messages. How can Eve figure out $x$?

# 3 RSA with Limited Messages

Suppose that Alice only has two possible messages she might send Bob: either "Yes" or "No".

(a) If Alice and Bob use the standard RSA procedure, describe how Eve could find out which message Alice sent.

(b) Instead, we would like to use the one-time pad procedure discussed in lecture. Even with only two possible messages, Eve gets absolutely no information about the original message if all she sees is the message xor-ed with an unknown pad. However, in order to make this work, we need a way for both Alice and Bob to know the pad without letting Eve find out.

They decide to leverage the original RSA procedure. Alice picks a pad randomly, then encrypts the pad (rather than her message!) using Bob's public key and sends it to Bob. Alice then sends over the message encrypted with the one-time-pad.

Somehow, Eve still figured out the message. How?