CS 70 Discrete Mathematics and Probability Theory
Fall 2018 Alistair Sinclair and Yun Song **DIS 4B**

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?

Solution:

(a) Both p and q must be of the form $3k+2$. $p = 3k+1$ is a problem since then $p-1$ has a factor of 3 in it. $p = 3k$ is a problem because then p is not prime.

(b) $N = p \cdot q = 85$ and $e = 3$ are displayed publicly. Note that in practice, p and q should be much larger 512-bit numbers. We are only choosing small numbers here to allow manual computation.

(c) We must have $ed = 3d \equiv 1 \pmod{64}$, so $d = 43$. Reminder: we would do this by using extended gcd with $x = 64$ and $y = 3$. We get $\gcd(x,y) = 1 = ax + by$, and $a = 1$, $b = -21$.

(d) We have $E(x) = x^3 \pmod{85}$. $10^3 \equiv 65 \pmod{85}$, so $E(x) = 65$.

(e) We have $D(y) = y^{43} \pmod{85}$. $24^{43} \equiv 14 \pmod{85}$, so $D(y) = 14$.

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 $(e, N_1), \ldots, (e, N_k)$ 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 $(7,35)$ and $(7,77)$ 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.

(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 $(3,5\times 23)$, $(3,11\times 17)$, and $(3,29\times 41)$ along with their transmissions. Argue why Eve cannot break the encryption in the same way as above.

Solution:

(a) Yes. Note that $\gcd(77,35)=7$. She can figure out the GCD of the two numbers using the GCD algorithm, and then divide 35 by 7, getting 5. Then she knows that the p and q corresponding to the first transmission are 7 and 5, and can break the encryption.

(b) Since none of the N's have common factors, she cannot find a GCD to divide out of any of the Ns. Hence the approach above does not work.

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) Describe how Alice and Bob might modify the RSA procedure to stop Eve from using this exploit. *(Hint: Try using a one-time pad somewhere in your procedure)*

Solution:

(a) Since there are only two messages Alice might have encrypted, Eve can just try both. Specifically, since Eve also knows Bob's public key, she can use it to encrypt both the message "Yes" and the message "No". Whichever encryption matches the encrypted message Alice sent must be the plaintext message Alice wanted to get to Bob.

(b) We would ideally like to just 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.

This is where we leverage the original RSA procedure. We can have Alice pick a pad randomly, then encrypt the pad (rather than her message!) using Bob's public key and send it to Bob. Since Alice could have chosen any appropriate-length bit string for the pad, Eve can't use the trick from the previous part to find out the pad. This means that Alice and Bob can now use the one-time pad procedure to send Alice's actual message without worrying about Eve exploiting the fact that there are only two possible messages.