CS 70 Discrete Mathematics and Probability Theory
Spring 2019 Satish Rao and Babak Ayazifar

DIS 4A

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 $E(x) = x^3 \pmod{85}$, where $E(x)$ is the encryption function. $10^3 \equiv 65 \pmod{85}$, so $E(x) = 65$.

(e) We have $D(y) = y^{43} \pmod{85}$, where $D(y)$ is the decryption function, the inverse of $E(x)$. $24^{43} \equiv 14 \pmod{85}$, 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 $(N_1, e), \ldots, (N_k, e)$ where no two N_i's are the same. Assume that the message is x such that $0 \leq x < N_i$ for every i.

(a) Suppose Eve sees the public keys $(p_1q_1, 7)$ and $(p_1q_2, 7)$ 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 $(p_1q_1, 3)$, $(p_2q_2, 3)$, and $(p_3q_3, 3)$ 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?

Solution:

(a) Normally, the difficulty of cracking RSA hinges upon the believed difficulty of factoring large numbers. If Eve were given just p_1q_1, she would (probably) not be able to figure out the factors.

However, Eve has access to two public keys, so yes, she will be able to figure it out. Note that $\gcd(p_1q_1, p_1q_2) = p_1$. Taking GCDs is actually an efficient operation thanks to the Euclidean Algorithm. Therefore, she can figure out the value of p_1, and from there figure out the value of q_1 and q_2 since she has p_1q_1 and p_1q_2.

(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.

(c) Eve observes $x^3 \pmod{N_1}$, $x^3 \pmod{N_2}$, $x^3 \pmod{N_3}$. Since all N_1, N_2, N_3 are pairwise relatively prime, Eve can use the Chinese Remainder Theorem to figure out $x^3 \pmod{N_1N_2N_3}$. However, once she gets that, she knows x, since $x < N_1$, $x < N_2$, and $x < N_3$, which implies $x^3 < N_1N_2N_3$. Uh oh!

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?

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) Let's call Alice's randomly generated pad x, and call the message she wants to send y. Eve gets to see $x^e \pmod N$ as well as $p := x \oplus y$. Since Eve knows that $y \in \{0,1\}$, then she knows that the pad is either $p \oplus 0$ or $p \oplus 1$. Here, we're leveraging the idea that $x \oplus y \oplus y = x$. She raises both of those to the e-th power modulo N, thus decrypting the message.