CS 70 Discrete Mathematics and Probability Theory
Spring 2026 Sinclair, Song

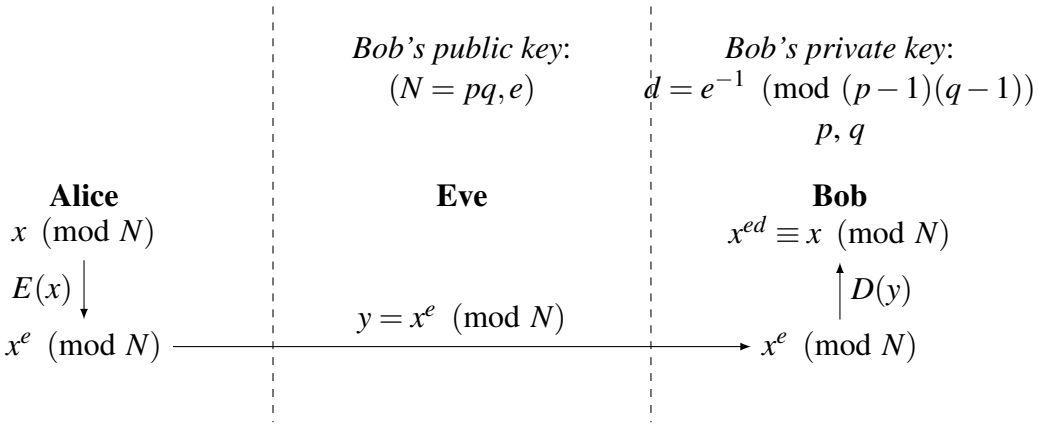
DIS 4A

RSA Intro

Note 7

Fermat's Little Theorem: For all primes p, $a^{p-1} \equiv 1 \pmod{p}$ if $a \neq 0$. An equivalent version of the statement (still assuming p is prime) is $a^p \equiv a \pmod{p}$ for all a.

RSA Scheme: A cryptographic scheme that allows communication over insecure channels via public-key encryption. Alice encrypts her message x with Bob's public key, ensuring that only Bob (with his private key) can decrypt it, which prevents Eve from eavesdropping.



1 FLT and RSA

Note 7

(a) Evaluate $3123^{30} \pmod{31}$.

(b) Suppose we would like to evaluate $141^{161} \pmod{187}$.

(i) First, evaluate $141^{161} \pmod{11}$ and $141^{161} \pmod{17}$ without simplifying the base (i.e. only simplify the exponent). Use the results of those computations to evaluate $141^{161} \pmod{187}$. (*Hint: You may find the following lemma helpful:* if $x \equiv a \pmod{p}$ and $x \equiv a \pmod{q}$ for coprime p and q, then $x \equiv a \pmod{pq}$. *Try to prove this lemma!*)

(ii) Alternatively we can evaluate $141^{161} \pmod{187}$ by thinking of the computation as an instance of the RSA equation $x^{ed} \equiv x \pmod{pq}$. What are p, q, e, and d? What is the final result of the computation? (*Hint: We know that* $187 = 11 \times 17$ *and* $161 = 23 \times 7$.)

Solution:

(a) Since 31 is prime, we know that $a^{30} \equiv 1 \pmod{31}$ for any nonzero a, by FLT. In particular, we have

$$3123^{30} \equiv 23^{30} \equiv 1 \pmod{31}.$$

(b) (i)

$$141^{161} = 141 \cdot (141^{16})^{10} \equiv 141 \cdot 1 \equiv 141 \pmod{11},$$
$$141^{161} = 141 \cdot (141^{10})^{16} \equiv 141 \cdot 1 \equiv 141 \pmod{17}.$$

By CRT, we know that if $x \equiv 141 \pmod{11}$ and $x \equiv 141 \pmod{17}$, then there is a unique $x \pmod{187}$ that satisfies these two equations. We note that $x \equiv 141 \pmod{187}$ does indeed satisfy these equations, and thus we conclude that: $141^{161} \equiv 141 \pmod{187}$. You can also apply the lemma: plugging in $a = 141$, $p = 11$, and $q = 17$ gives the desired result.

Proof of Lemma: Assume $x \equiv a \pmod{p}$ and $x \equiv a \pmod{q}$ for coprime p and q. Consider $x - a$. We see that $x - a \equiv 0 \pmod{p}$ and $x - a \equiv 0 \pmod{q}$. Now, by the CRT formula, we have $x - a \equiv 0 \cdot qq_1 + 0 \cdot pp_1 \equiv 0 \pmod{pq}$, and thus $x \equiv a \pmod{pq}$.

(ii) This is an instantiation of the RSA scheme, with $p = 11$, $q = 17$, $e = 7$, and $d = 23$. (p and q could be swapped here, and similarly with e and d.)

In particular, Alice is attempting to send the message $x = 141$, and the encryption is $x^e \pmod{pq}$, or in this case $141^7 \pmod{187}$.

When Bob decrypts the message, he computes $x^{ed} \pmod{pq}$, or in this case $141^{7\times 23} = 141^{161} \pmod{187}$.

Since we know that this scheme will always recover the original message, the resulting quantity must be $141 \pmod{187}$.

2 RSA Warm-Up

Note 7

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

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

(b) What is the private key?

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

(d) Ignoring the previous part, suppose Bob receives a different encrypted message $y = 19$ from Alice. What equation would he use to decrypt the message? What is the decrypted message?

Solution:

(a) $N = p \cdot q = 85$ 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.

(b) 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 $a = 1$, $b = -21$.

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

(d) We have $D(y) = y^{43} \pmod{85}$, where $D(y)$ is the decryption function, the inverse of $E(x)$.

$$x \equiv 19^{43} \pmod{85}$$

From CRT we know that for coprime numbers p and q if

$$x \equiv a \pmod{p}$$
$$x \equiv b \pmod{q}$$

then

$$x = aqq_1 + bpp_1 \pmod{pq}$$

where $p_1 = p^{-1} \pmod{q}$ and $q_1 = q^{-1} \pmod{p}$.

In our case we have $p = 5$ and $q = 17$. So

$$x \equiv 19^{43} \equiv (-1)^{43} \equiv -1 \equiv 4 \pmod{5}$$

and

$$x \equiv 19^{43} \pmod{17}$$
$$x \equiv (2)^{43} \pmod{17}$$
$$x \equiv (2^4)^{10} \cdot 2^3 \pmod{17}$$
$$x \equiv (-1)^{10} \cdot 8 \pmod{17}$$
$$x \equiv 8 \pmod{17}$$

Hence

$$x = a = 4 \pmod{5} \qquad x = b = 8 \pmod{17}$$

and

$$p_1 = p^{-1} \pmod{17} = 5^{-1} \pmod{17} = 7$$
$$q_1 = q^{-1} \pmod{5} = 17^{-1} \pmod{5} = 3$$

So we have

$$x \equiv aqq_1 + bpp_1 \pmod{pq}$$
$$x \equiv 4 \cdot 17 \cdot 3 + 8 \cdot 5 \cdot 7 \pmod{85}$$
$$x \equiv 4 \cdot 17 \cdot 3 + 280 \pmod{85}$$
$$x \equiv 17 \cdot (12) + 280 \pmod{85}$$
$$x \equiv 17 \cdot (10 + 2) + 280 \pmod{85}$$
$$x \equiv 34 + 25 \pmod{85}$$
$$x \equiv 59 \pmod{85}$$

so $D(y) = 59$.

3 RSA Gone Wrong?

Note 7

Alice wants to send a message to Bob using RSA. Unfortunately for them, there is an eavesdropper Eve, and Eve has evolved. **cue dramatic music**

(a) Suppose that Eve has a magical eye that can see the prime factors of any number, no matter how large or small. Can Eve obtain Alice's original message? If so, how?

(b) Suppose that Eve acquires the modular n^{th}-root-inator, which allows her to find the n^{th} root of any number in modular arithmetic. Precisely, when given n and $a^n \pmod{p}$, Eve can use the modular n^{th}-root-inator to obtain a. Can Eve obtain Alice's original message? If so, how?

Alice and Bob decide to modify their RSA scheme, but they forgot to consider whether their scheme remains both correct and secure!

(c) Suppose Alice and Bob continue to use large primes p, q, but they choose to use $e = 2$. Is their scheme correct (they can encrypt and decrypt to recover the original message)? If so, is it secure (Eve cannot obtain the original message)?

(d) Suppose Alice wants to send a Bob her 3-digit code on the back of her credit card, with the standard RSA scheme. (All codes on the back of credit cards are 3 digits.) Is their scheme correct? If so, is it secure?

Solution:

(a) Yes. Eve can take N from the public key and obtain its prime factors p, q. With this information, she can compute $d = e^{-1} \pmod{(p-1)(q-1)}$, since they now know all the quantities on the RHS. Accordingly, Eve can simply raise the encrypted message to the power of d to obtain the original message.

For RSA to be secure, we assume that it is very hard to find the prime factorization of very large numbers, especially when they are *semiprimes* (i.e. they have exactly two prime factors). This part shows what can go wrong when this assumption no longer holds, as Eve now knows the private key.

(b) Yes. With the modular n^{th}-root-inator, Eve can compute the original message x when given $y = x^e \pmod{N}$, since N and e are part of the public key.

For RSA to be secure, we also assume that finding the modular n^{th} root is very hard. This part shows what can go wrong when this assumption no longer holds, as Eve can easily find the original message.

(c) No, their scheme is not correct because they won't have a private key for decryption. To find the private key d from the public key (N, e), we need $\gcd(e, (p-1)(q-1)) = 1$. However, $(p-1)(q-1)$ is necessarily even since p, q are distinct odd primes, so if $e = 2$, $\gcd(e, (p-1)(q-1)) = 2$, and a private key does not exist. (Note that this shows that e should more generally never be even.)

(d) Yes, the standard RSA scheme is correct. However, it is no longer secure because there are

only 1000 possible 3-digit codes. Eve can try encrypting all 1000 values with Bob's public key and find out which one matches the one Alice sent.

4 RSA with Multiple Keys

Note 7

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.

Further, in all of the subparts, you may assume that Eve knows the details of the modified RSA schemes (i.e. Eve knows the format of the N_i's, but not the specific values used to compute the N_i's).

(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 ($e = 3$), 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 $x^3 < N_1N_2N_3$, so she can directly take the cube root of the result from CRT. Uh oh!