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

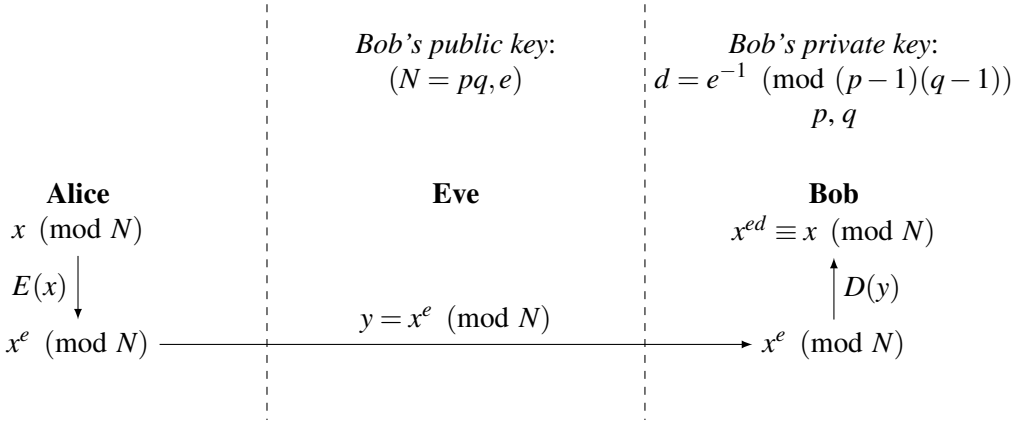
DIS 4A

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* $161 = 23 \times 7$.)

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?

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?

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?