Intro to Discrete Mathematics

9/29/25

finite / discrete objects vs inf/cont. objects

i.e. counting problems, trees/graphs, permutations, partitions

I. elementary number theory and cryptography

II. Graph theory

III. Graph algorithms

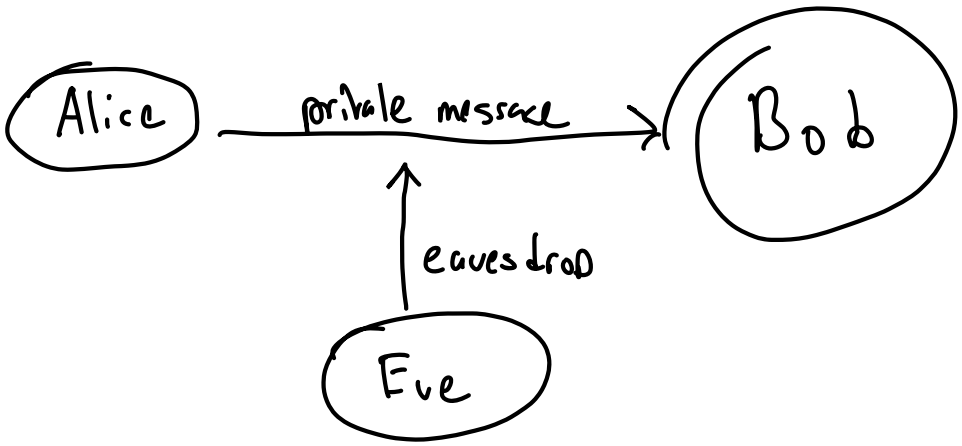
IV. Counting

V. Generating functions

VI. Recurrence relations

I. Elementary number theory and cryptography

1. Motivations



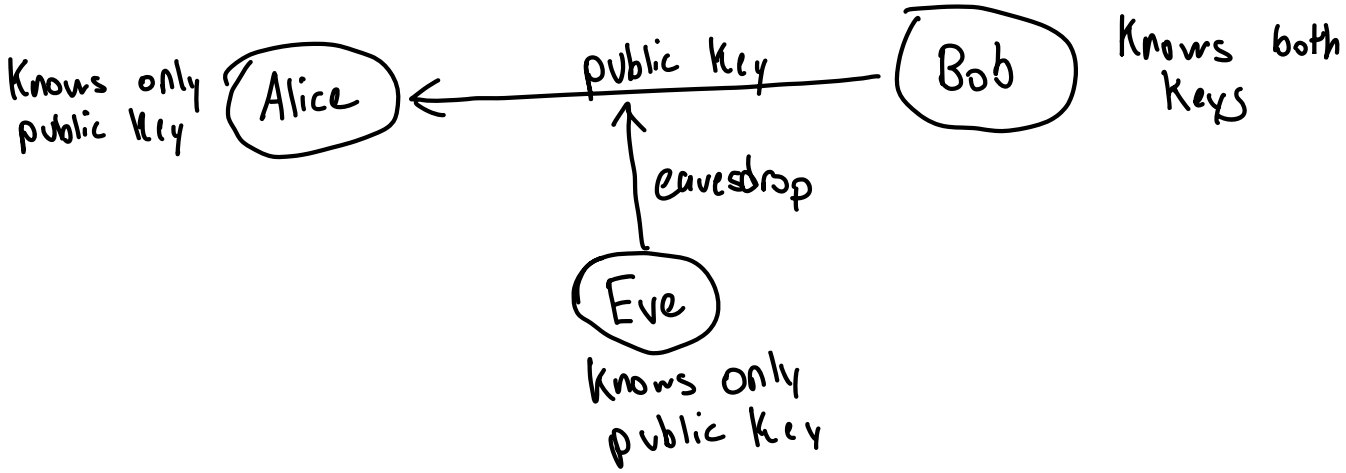
Classical cryptography: Alice and Bob agree on procedure beforehand.

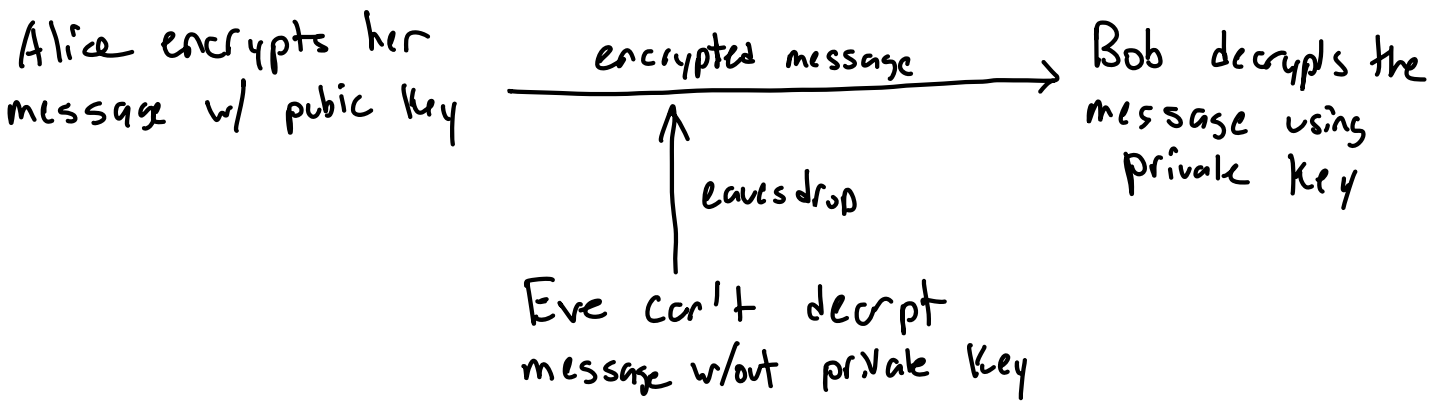
Examples: Substitution cipher
- Ceaser cipher
- Atbash cipher

- More generally: arbitrary assignments
  ciphertext attack: frequency analysis (for longer messages)

Issue: Rules exchanged in advance.
Solution: pubic key encryption

Bob generates public + private key.





We need a mathematical process that is easy to perform but difficult to reverse.

- RSA encryption based on prime factorization
  - ↳ Easy to multiply two large prime numbers, hard to factorize the product.
- Diffie-Hellman key exchange protocol
  - ↳ Given base b and prime p, easy to compute $c := b^e \bmod p$ given any e, but hard to find e given c, p.
- Elliptic curve cryptography. → Widely used, somewhat quantum secure
  - ↳ Given a point P on an elliptic curve, easy to compute $Q := kP$ for any k, but hard to find k given P, Q.

Elementary Number Theory

Fundamental theorem of arithmetic: Every nonzero natural number is a product of primes, in a unique way up to reordering.

Proof: By induction for existence.
Uniqueness needs a bit more work: requires theory for gcd.

7