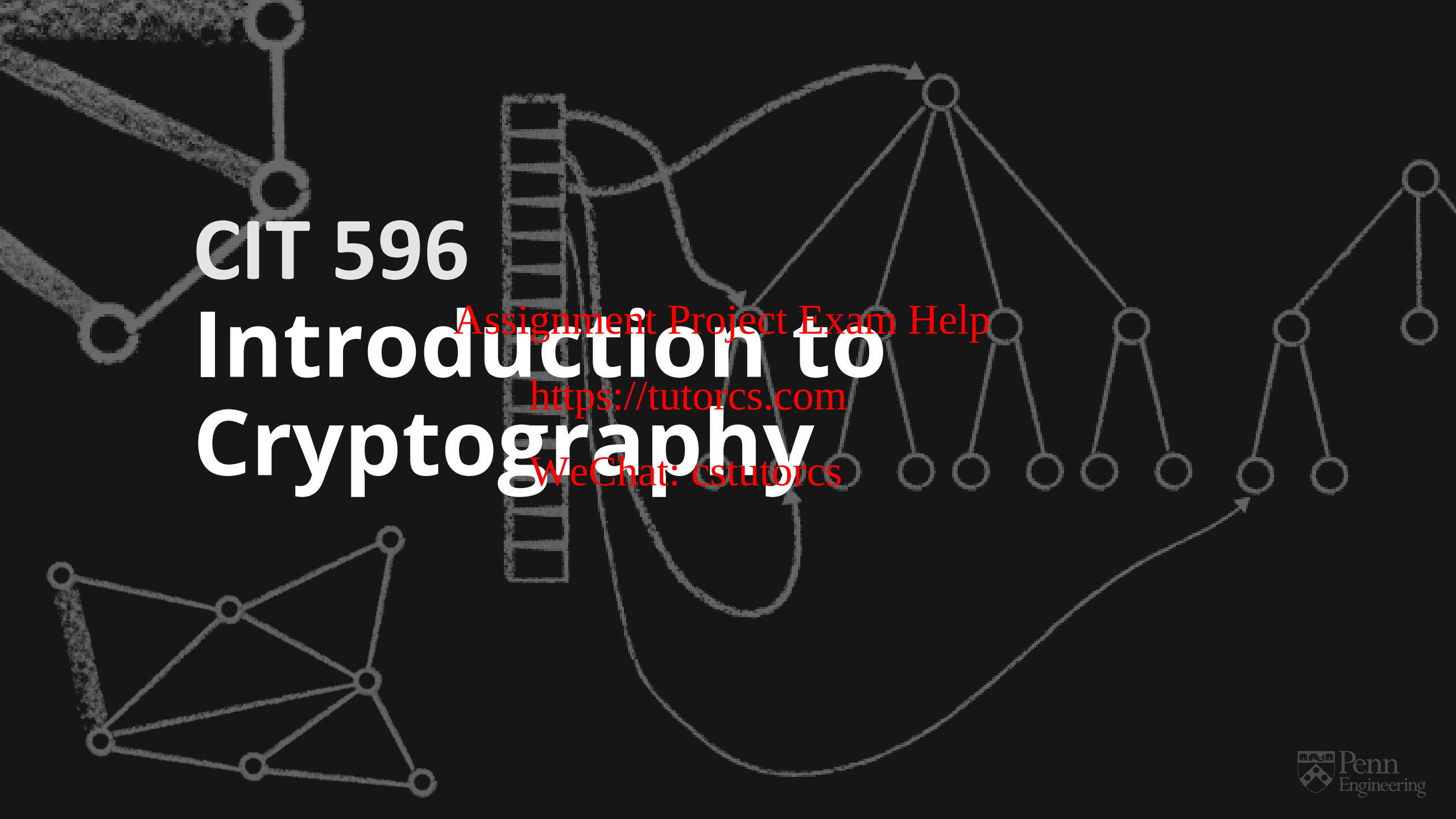
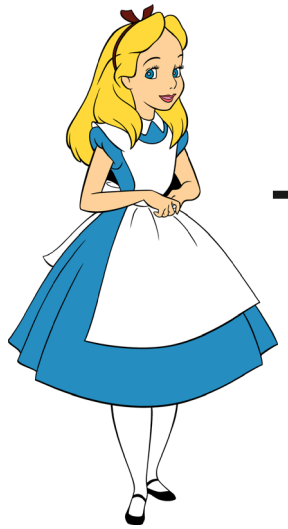


CIT 596
Introduction to Cryptography

Penn Engineering

INTRO TO CRYPTOGRAPHY

- Traditional goal of cryptography: Secure communication via insecure channels.



Alice

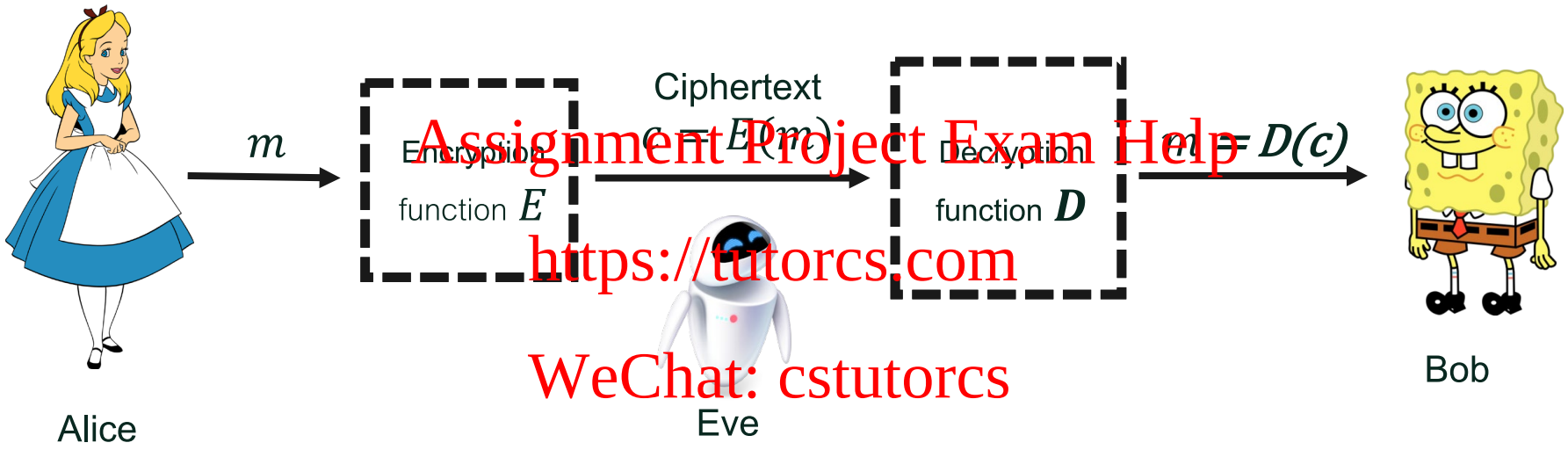
m: message Alice wants to send

Eve

listening to the channel

Bob

SOLUTION



Properties we need:

- Alice can compute E efficiently
- Eve doesn't learn m from c efficiently
- Bob can compute D efficiently

PRIVATE-KEY CRYPTOGRAPHY

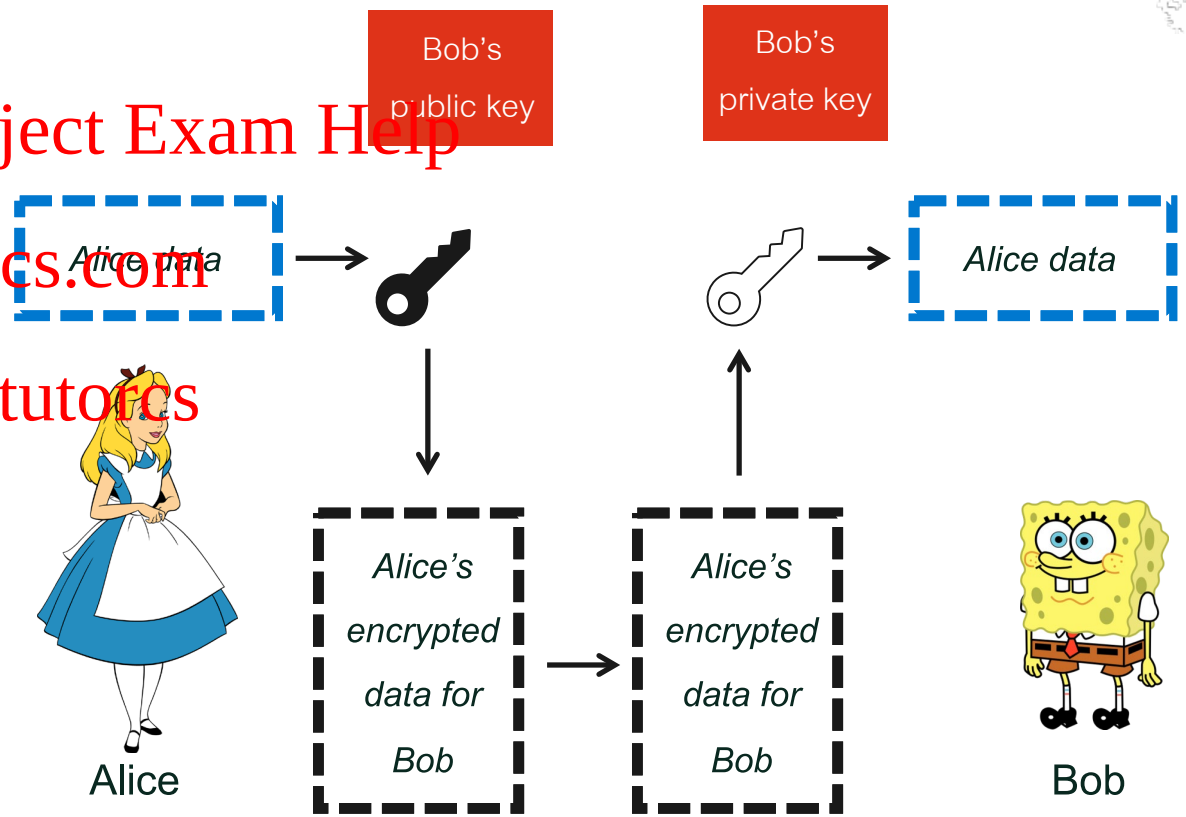
- Solution before 1980:
  - Message m viewed as a binary string
  - Alice and Bob share a secret key K (as long as m)
  - To encrypt, Alice sends bitwise XOR of strings
  - Example:

$$\begin{aligned} m &= 11010101 \\ K &= 101100101 \\ c &= 110110000 \end{aligned}$$

  - To decrypt, Bob computes bitwise XOR of K and c (You should check that this gets you back m.)
  - Problems:
    - Key distribution: need keys as long as messages
    - Keys get used up after a transmission, need different keys for every pair of communicators

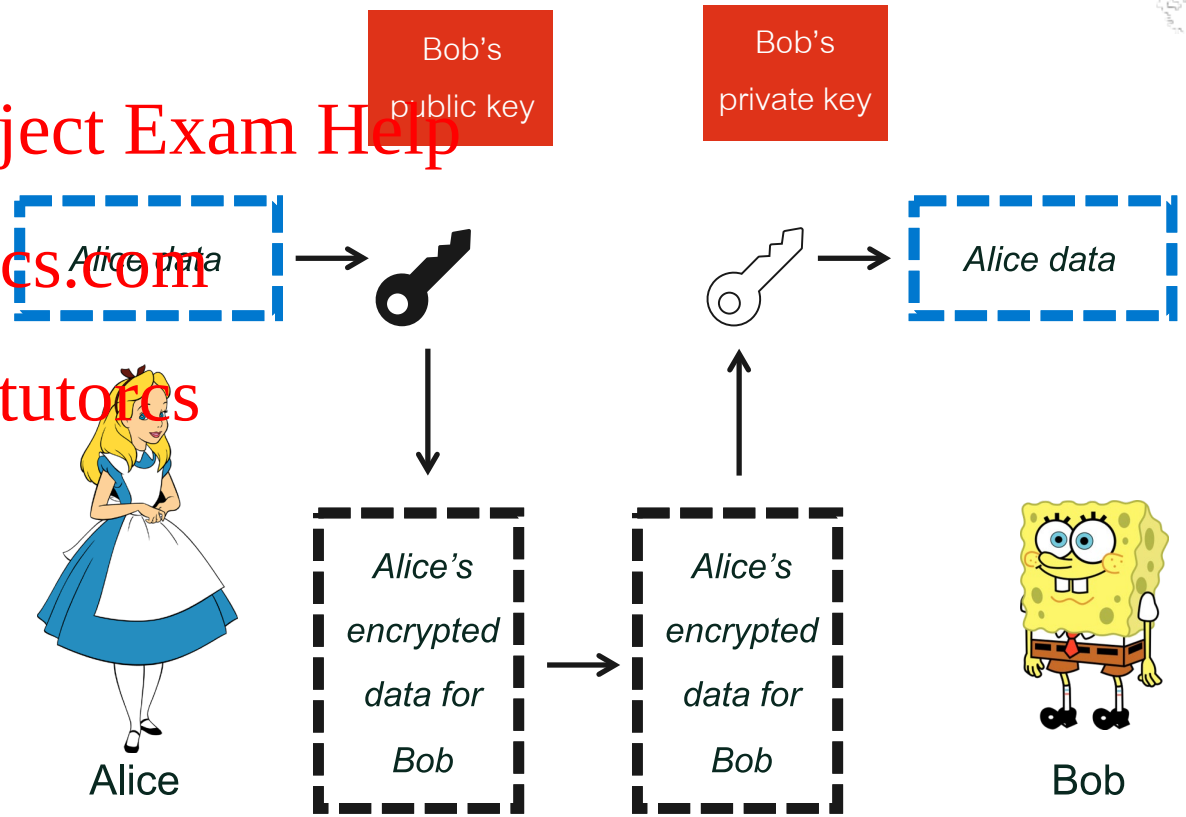
PUBLIC-KEY CRYPTOGRAPHY

- Bob publishes his public key!
- Alice encrypts message using this key.
- Eve cannot decrypt efficiently.
- But Bob knows a private and secret key and can!
- Mathematically: Bob has a public key P_B and a secret key S_B
  - Bob publishes P_B
  - Alice encrypts m as $c = E(m, P_B)$
  - Bob decrypts as $m = D(c, S_B)$
- Requires that Eve cannot decrypt c



PUBLIC-KEY CRYPTOGRAPHY (CONTINUED)

- Pairs of functions (E, D) that work in the above way are called one-way trapdoor functions:
  - One-way: easy to compute E and hard to invert
  - Trapdoor: knowing a secret makes it easy to invert



PUBLIC-KEY CRYPTOGRAPHY - BENEFITS

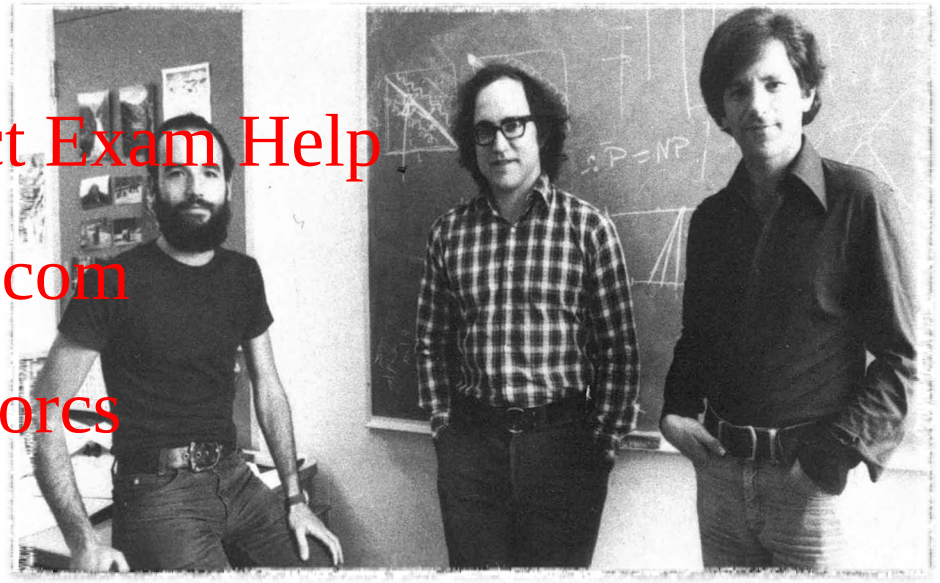
- Like using a phone book to send someone a secret message!
- Essential for eCommerce and modern communication, where we want to communicate securely with strangers.
- Opens up possibilities for other secure operations like:
  - Signatures on documents
  - Several parties jointly computing a function without learning each other's inputs

RSA CRYPTOSYSTEM

- Bob picks two primes p and q. $N = pq$
- Bob picks an encryption exponent e and publishes (e, N) as his public key.
- Quantity $(p-1)(q-1)$ is important and denoted $\varphi(N)$. It is called the "Euler Totient Function."
- Bob chooses e such that $\gcd(e, \varphi(N)) = 1$
- Using extended $\gcd$, Bob finds decryption exponent d such that

$$de = 1 \bmod \varphi(N)$$

- (d, p, q) is Bob's private key



Shamir, Rivest, and *Adleman*