Diffie-Hellman Key Exchange

Introduction to Basic Cryptography

Dr. Ryan Riley

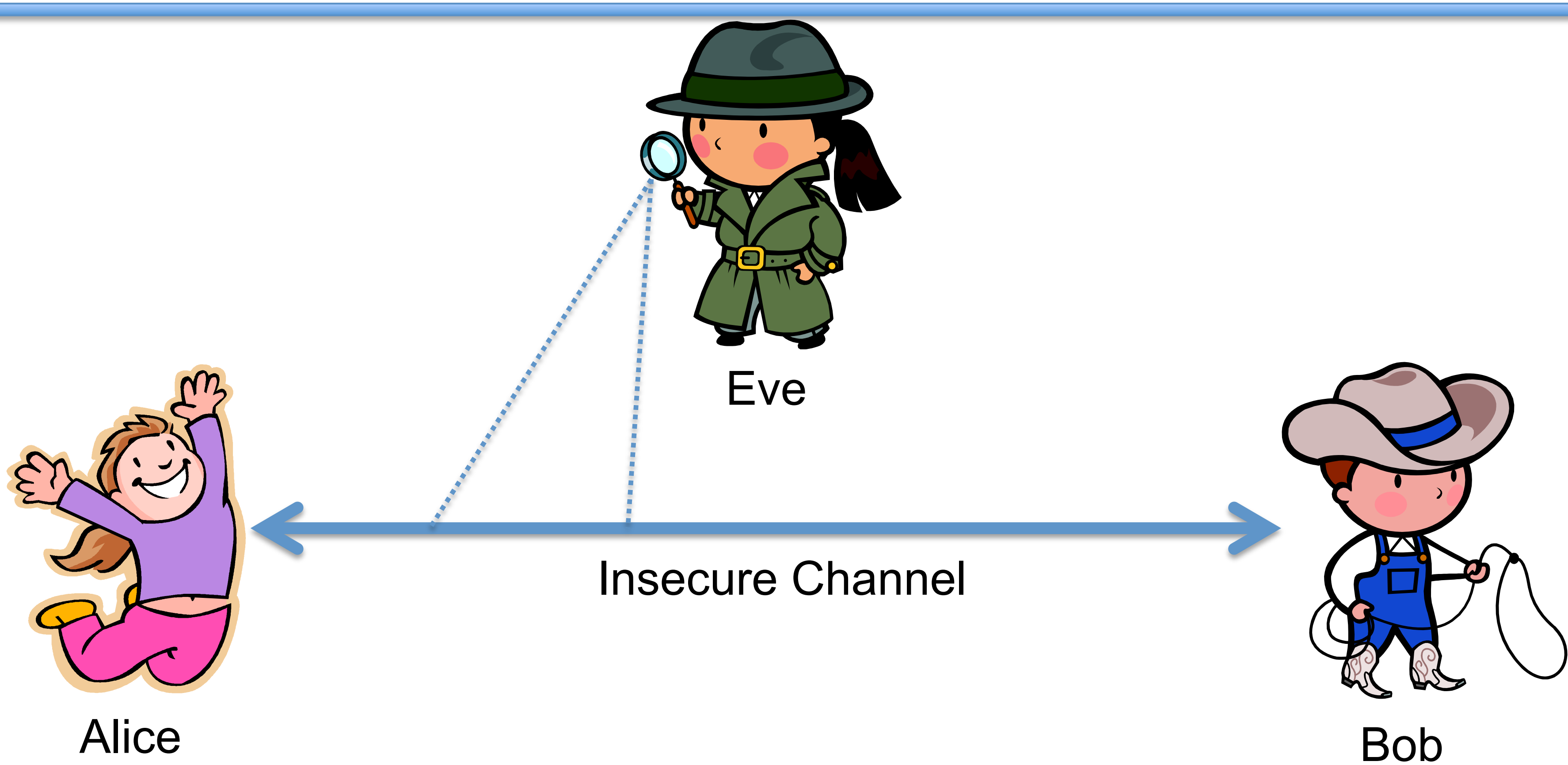
جامعة قطر
QATAR UNIVERSITY

Symmetric Key Crypto Problem

- Symmetric key crypto lets two parties share secret messages *as long as they already have a shared key*
- How do you share secret messages with someone when you don't already have a shared key?
  – Such as shared messages between computers on the internet

QATAR UNIVERSITY

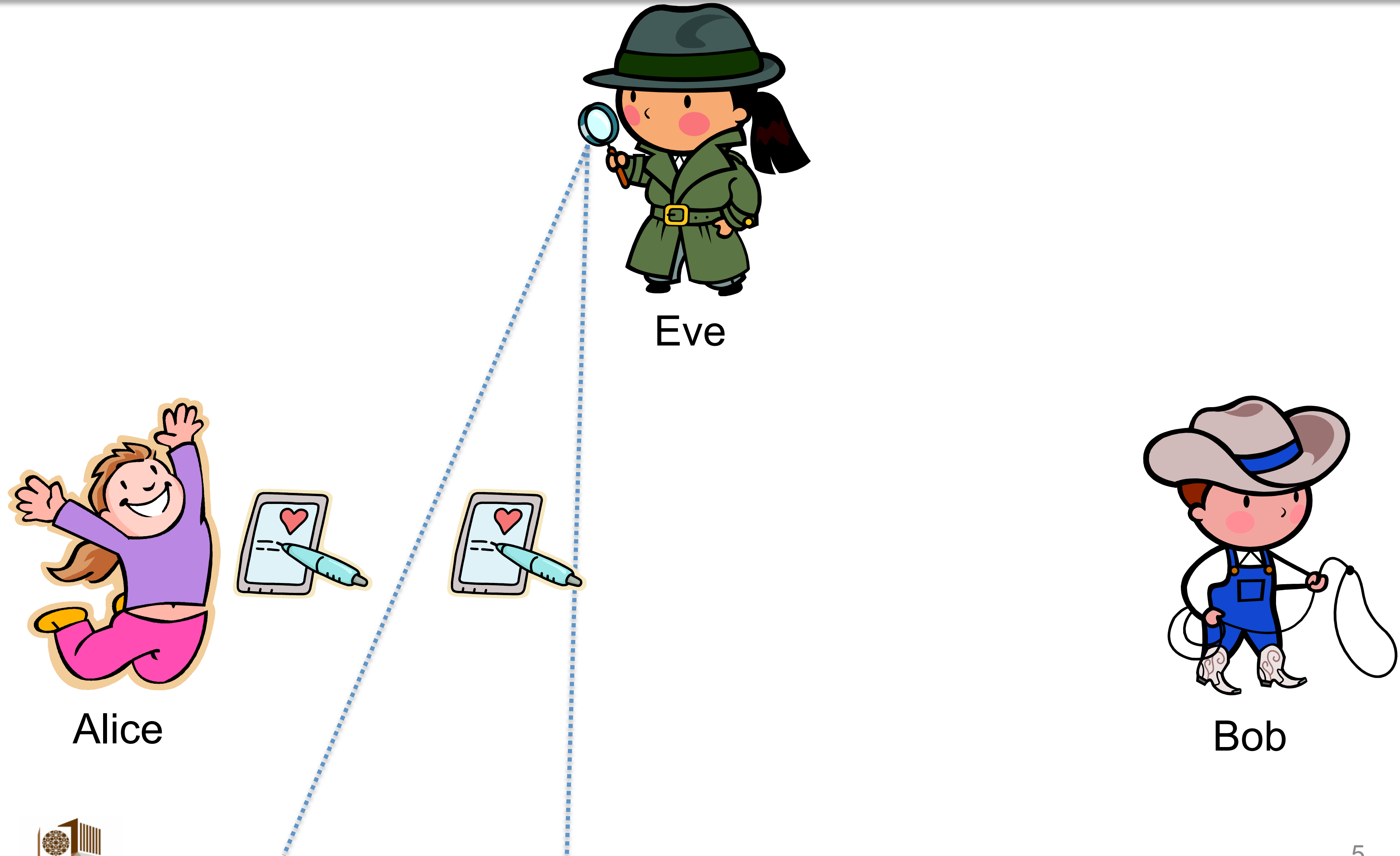
Problem: Eve



Eve the Eavesdropper

- Eve is an attacker who can see Alice and Bob's messages
- Eve can't modify them
- Eve is a *passive attacker*
- Real-world examples
  - Internet provider
  - Government
  - Anyone nearby if your wifi is unencrypted
  - Someone else on the same network
  - Lots of potential people…

Behold the Power of Eve



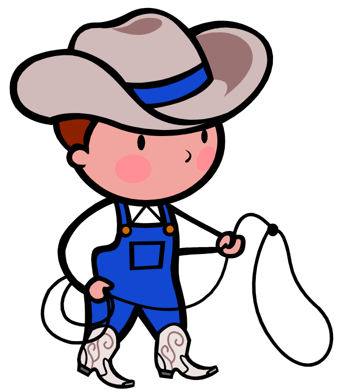
Trouble for Alice and Bob

- Obviously, Alice and Bob need to use encryption
- How do they choose a key?

جامعة قطر
QATAR UNIVERSITY

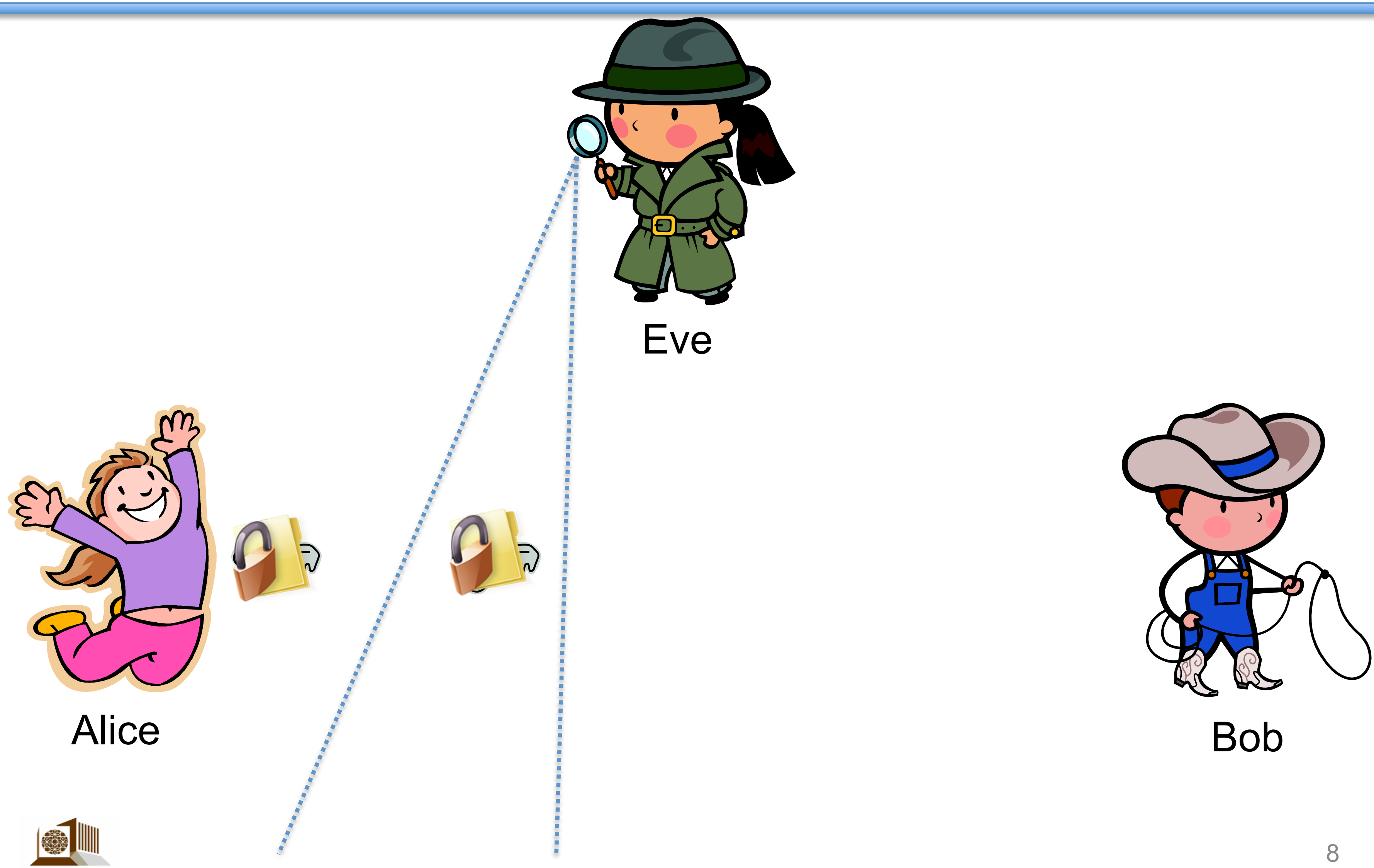
Idea!


Alice



Bob

:(


Eve
Alice
Bob

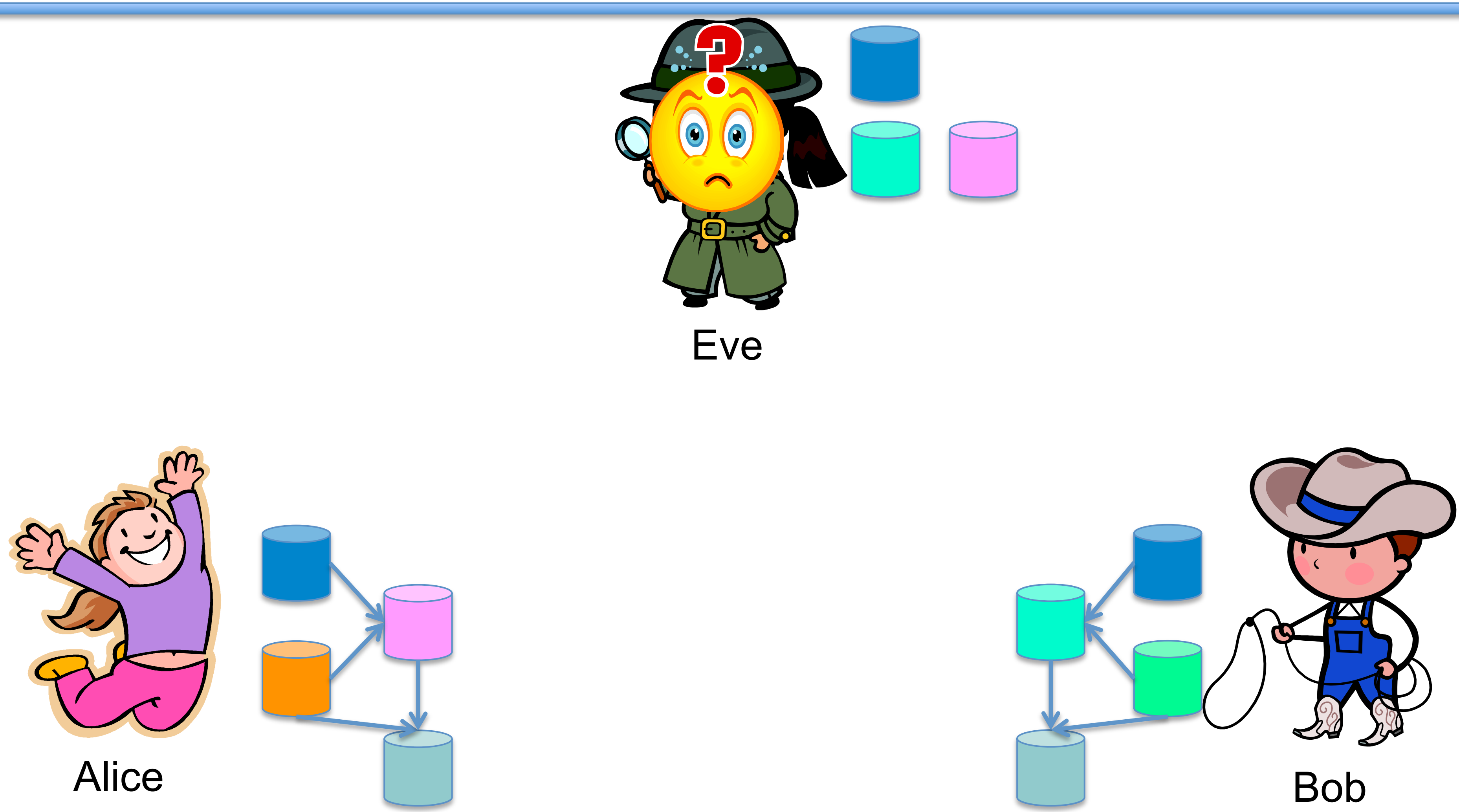
Ok, so…

- We can't pick a key and send it
- We could pick a key together offline
  - Not feasible in the general case
  - You want to use encrypted communication with a lot of different services on the internet…

Diffie-Hellman Key Exchange

- Invented by Whitfield Diffie and Martin Hellman in 1976
  - Independently invented at GCHQ a few years earlier, but never released
- Allows Alice and Bob to exchange a key without Eve learning it

DH in Colors



DH in Colors

- Eve can't determine the secret color because she doesn't have the right colors to mix together
- This works based on two assumptions:
  - Paint is easy to mix
  - Paint is hard to unmix
- This is just an analogy, the actual algorithm uses mathematics

DH in Math

- The mathematics of real DH is based on modulo exponentiation
- Makes use of prime numbers and primitive roots
- The basic math is not that hard

DH in Math Example

1. Alice and Bob agree on a prime number p and a base value g. Here, $p=23$ and $g=5$
2. Alice chooses a secret number, **a**, and sends Bob $A=g^a \bmod p$. Here, **a=6**
   - $A=5^6 \bmod 23$
   - $A = \mathbf{15625} \bmod 23$
   - $A = 8$

Example from http://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange

DH in Math Example

3. Bob chooses a secret number, **b**, and sends Alice $B=g^b \bmod p$. Here, **b=15**
   - $B=5^{15} \bmod 23$
   - B = **30,517,578,125** mod 23
   - B = 19

Example from http://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange

جامعة قطر
QATAR UNIVERSITY

DH in Math Example

4. Alice computes $s = B^a \bmod p$
   - $s = 19^6 \bmod 23$
   - $s = \mathbf{47{,}045{,}881} \bmod 23$
   - $s = \mathbf{2}$
5. Bob computes $s = A^b \bmod p$
   - $s = 8^{15} \bmod 23$
   - $s = \mathbf{35{,}184{,}372{,}088{,}832} \bmod 23$
   - $s = \mathbf{2}$
6. Alice and Bob now share a secret, s=2, that can't be derived from the public information

Example from http://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange

DH in Practice

- a, b, and p would need to be MUCH larger in practice
  - 100s of digits long
- This works because Eve can't use A and B to figure out the secret numbers a and b chosen by Alice and Bob
  - Called the discrete logarithm problem
- DH doesn't prove *who* you share the key with, just that the key isn't known by anyone else

Summing Up

- Symmetric Key crypto has a major problem: How do two people who don't know each other share a key?
- A Diffie-Hellman key exchange lets them compute a shared key even in the presence of an eavesdropper, Eve.
- Note: If Eve was *active*, instead of *passive*, this wouldn't work…