# 601.445/645
# Practical Cryptographic Systems

## Asymmetric Cryptography II

**Instructor: Matthew Green**

# Housekeeping

- A2 released
  - Due 23rd February, 11:59pm
  - Start early!
- Quiz moved to 19th February
  - Will follow-up on any (minor) changes to the material
  - Primarily based on Boneh/Shoup readings

# News?

OPINION COMMENTARY Follow

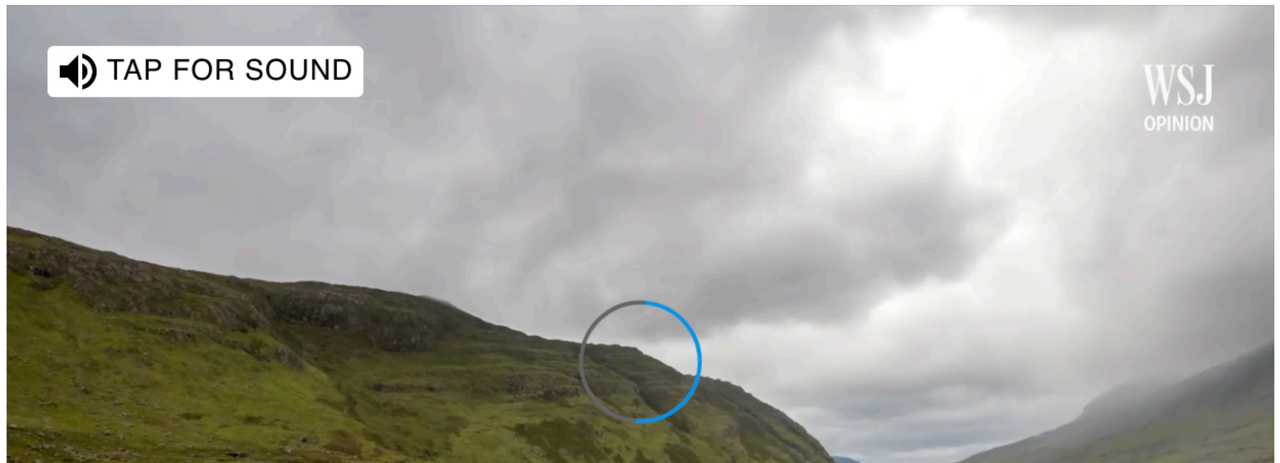
## *U.K. Kicks Apple's Door Open for China*

Beijing would quickly exploit the British order to allow access to encrypted data.

By Matthew Green and Alex Stamos

Feb. 10, 2025 5:07 pm ET

Share Resize 137 Listen (3 min)



# News?

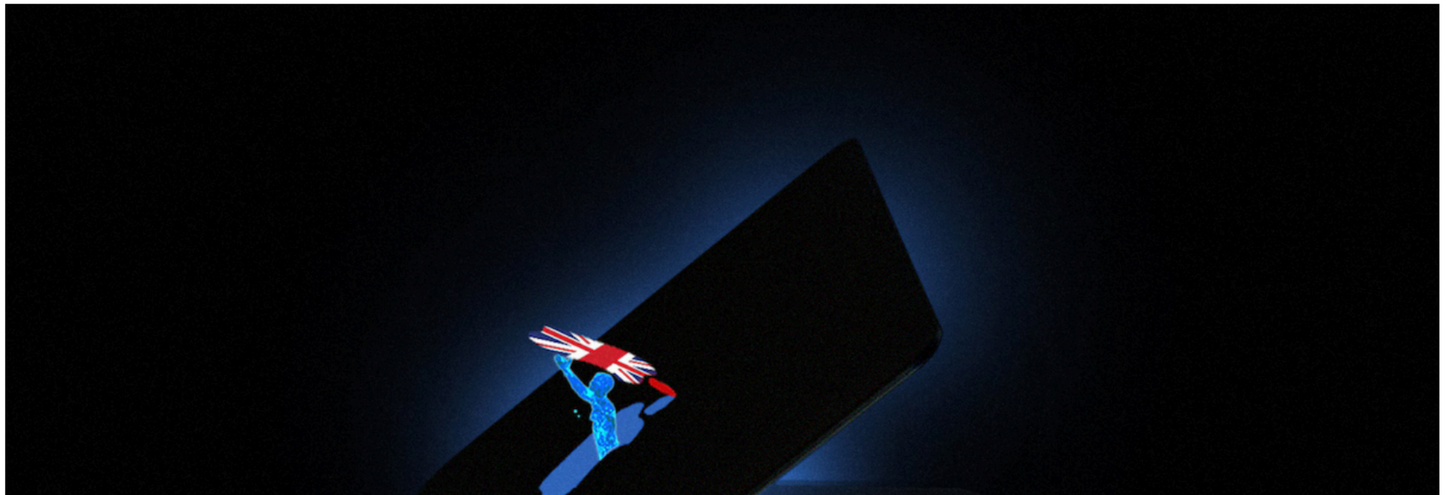
EXCLUSIVE

# U.K. orders Apple to let it spy on users' encrypted accounts

Secret order requires blanket access to protected cloud backups around the world, which if implemented would undermine Apple's privacy pledge to its users.

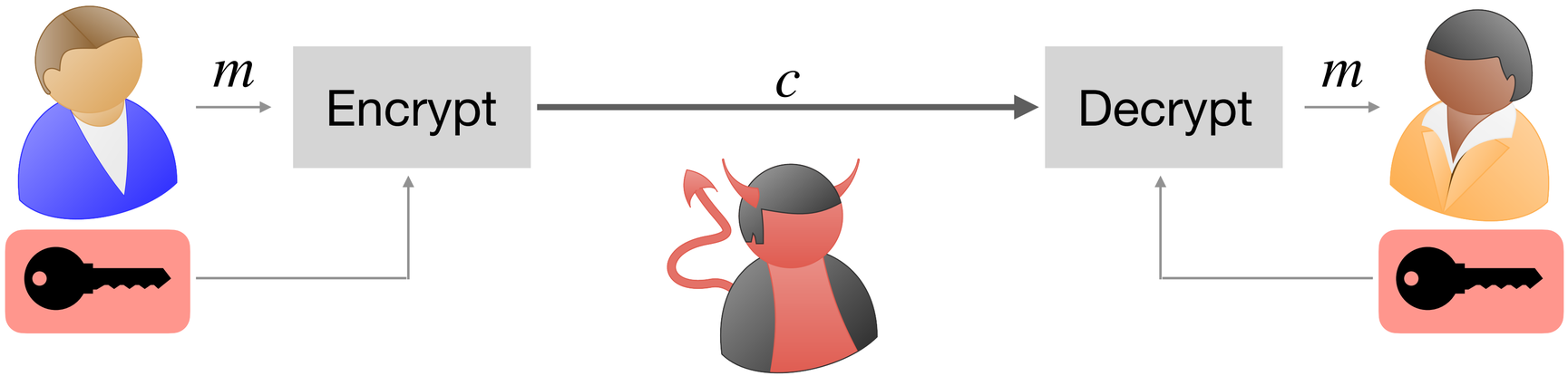
Updated February 7, 2025

8 min 1336



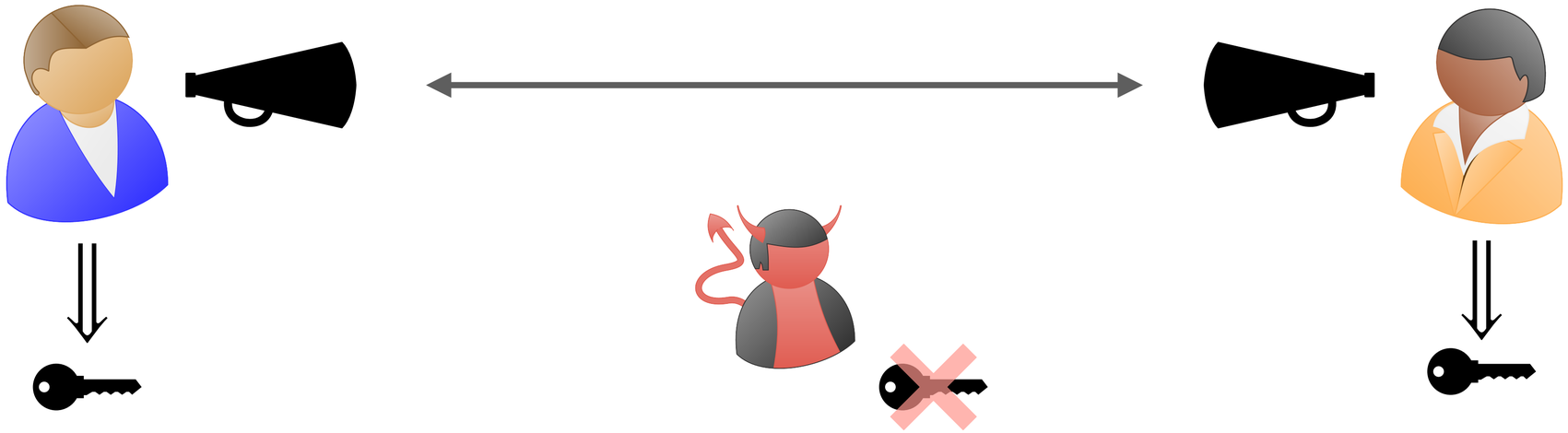
Most Read Techn

# Review



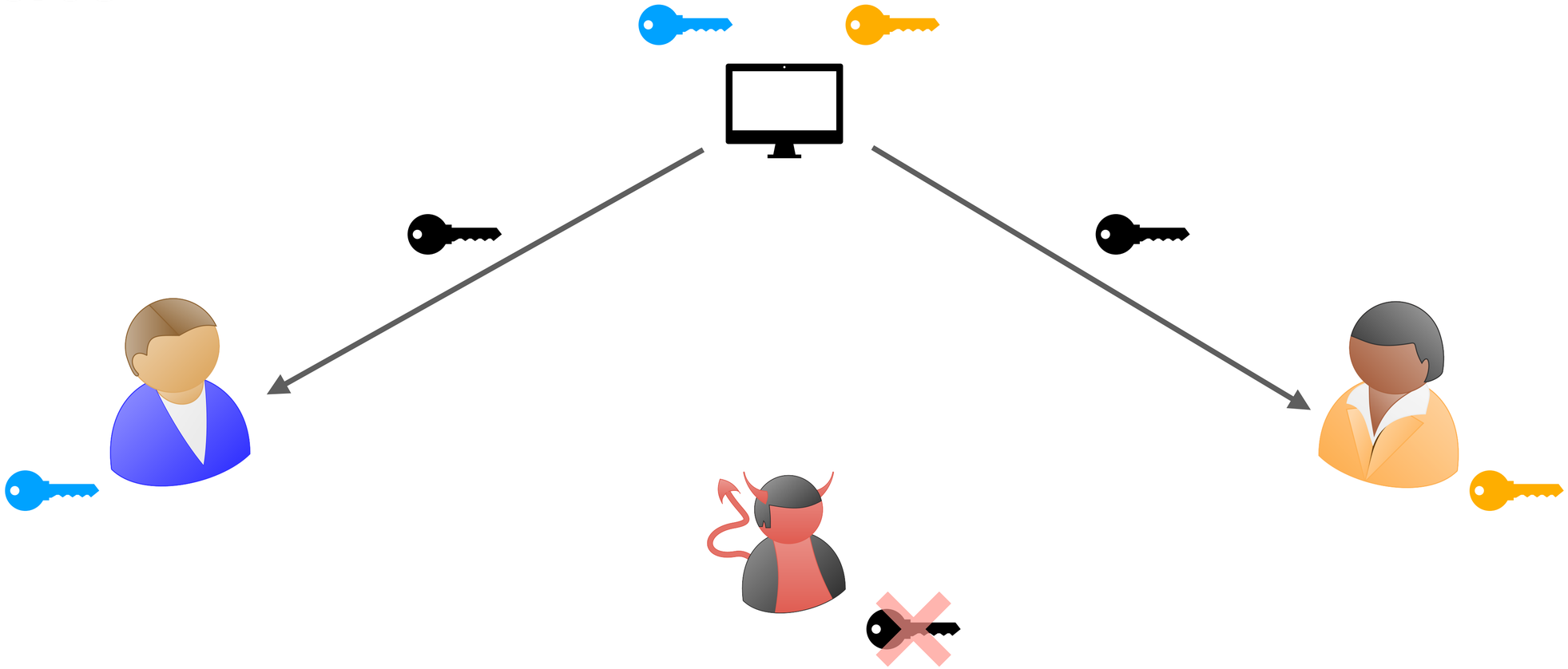

How do parties agree on a common key?

# Key Exchange



# Key Exchange

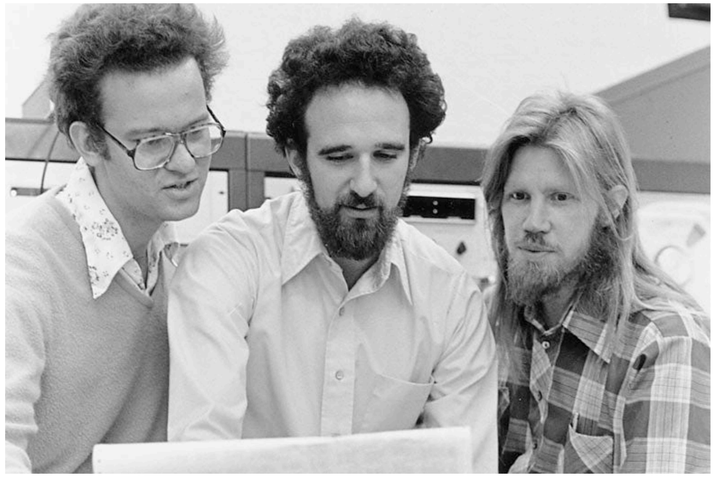
## Kerberos

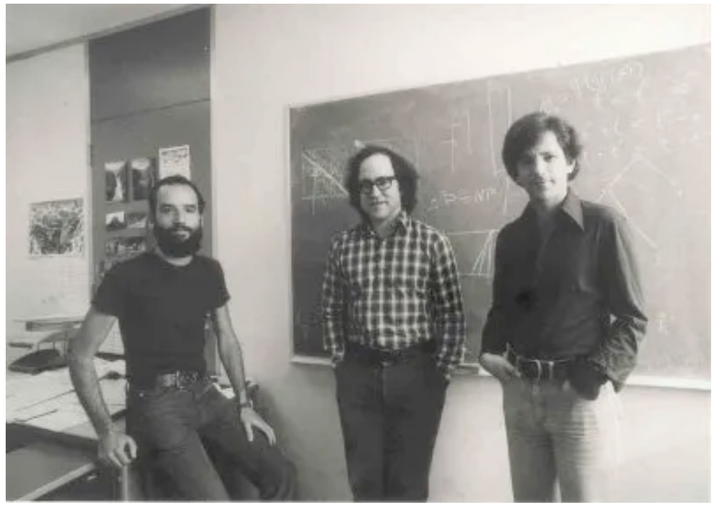


Drawbacks?

# Asymmetric Cryptography

- Aka “public-key” crypto
  - Gives us a way to encrypt material without pre-existing shared secrets



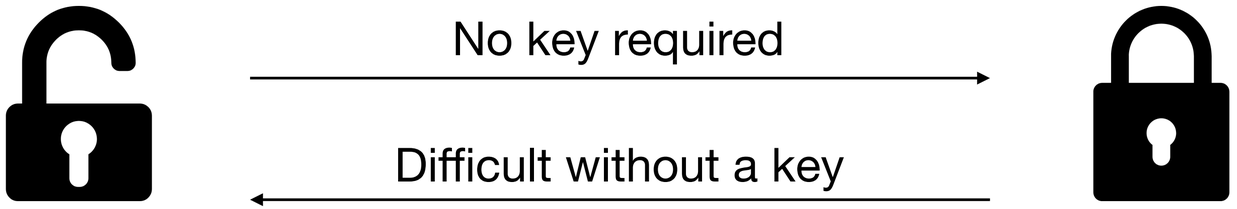


# Diffie-Hellman Key Exchange

Agreeing on a common secret over an untrusted/public channel

Key Idea: Exploiting asymmetry

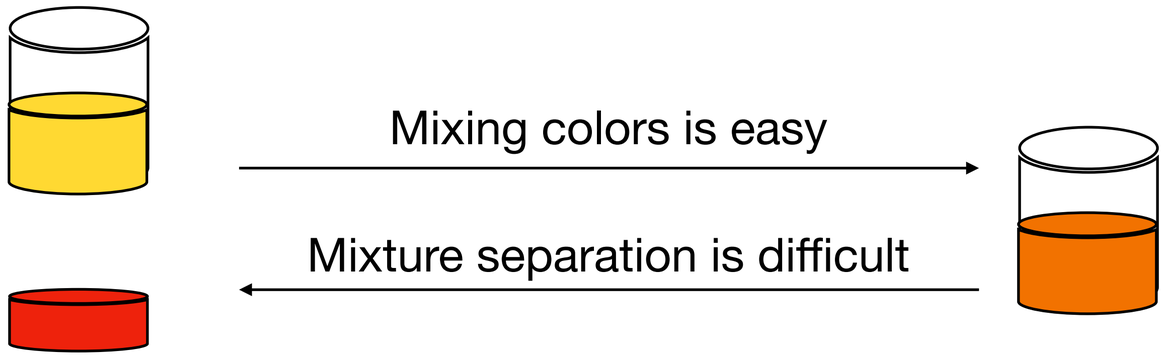
Often present in the real world!



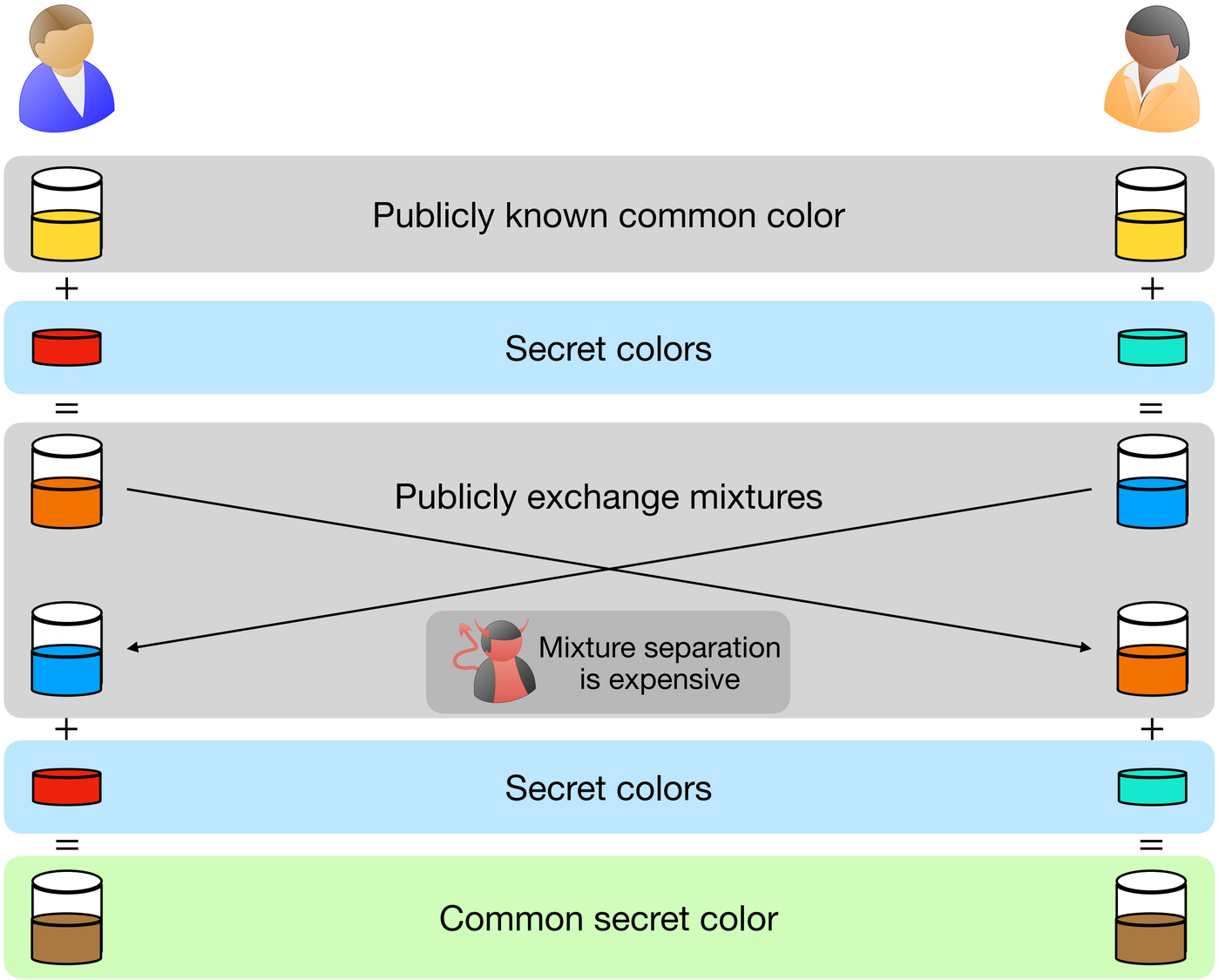
# Diffie-Hellman Key Exchange

Agreeing on a common secret over an untrusted/public channel

Key Idea: Exploiting asymmetry



# Diffie-Hellman Key Exchange




Mathematical equivalent of the mixture separation?

# Modular Arithmetic

- $\mathbb{Z}$ : The set of integers
- Let $a, N \in \mathbb{Z}$ with $N > 1$

$$[a \bmod N] \equiv \text{remainder when } a \text{ is divided by } N$$

where remainder is in $\{0, \ldots, N-1\}$

- For any $a, b, N \in \mathbb{Z}$ with $N > 1$

If $[a \bmod N] = [b \bmod N]$ then we say "$a$ is congruent to $b$ modulo $N$" and denote it by

$$a \equiv b \bmod N$$

# Modular Arithmetic

- Let $a \equiv c \mod N$ and $b \equiv d \mod N$
  - $a + c \equiv b + d \mod N$
  - $a - c \equiv b - d \mod N$
  - $a \cdot c \equiv b \cdot d \mod N$

$\Longrightarrow$ Reduce by the modulus and then perform the arithmetic operation

- What about division?

# Modular Arithmetic

## Division

- Division in modular arithmetic
  - If $a \equiv c \mod N$ and $b \equiv d \mod N$ then

$$[a/b \mod N] \text{ need not equal } [c/d \mod N]$$

  - It may not even be well defined:

$$12 \equiv 4 \mod 4 \text{ and } 5 \equiv 1 \mod 4$$

$$\text{But } 12/5 \not\equiv 4/1 \mod 4$$

$\implies$ $ab \equiv cb \mod N$ does NOT imply $a \equiv c \mod N$

Example: $a = 5, c = 9, b = 2, N = 8.$

# Modular Arithmetic

## Multiplicative Inverse

- **Multiplicative Inverse:** Given $b \in \mathbb{Z}$, if there exists $d \in \mathbb{Z}$ such that

$$bd \equiv 1 \bmod N$$

  then $d$ is called the multiplicative inverse of $b$ modulo $N$.

- If $b \in \mathbb{Z}$ has a multiplicative inverse modulo $N$ then it has a **unique** inverse in the range $\{0,...,N-1\}$.
  - We denote this multiplicative inverse by $b^{-1}$

# Modular Arithmetic

## Multiplicative Inverse

- If $ab \equiv cb \mod N$ and $b$ has a multiplicative inverse $b^{-1}$, then

$$ab \cdot b^{-1} \equiv cb \cdot b^{-1} \mod N \quad \Longrightarrow \quad a \equiv c \mod N.$$

- Which integers $b$ are invertible modulo $N$?

# Modular Arithmetic

## Multiplicative Inverse

| Mod 7 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| 1 | 1 | 2 | 3 | 4 | 5 | 6 |
| 2 | 2 | 4 | 6 | 1 | 3 | 5 |
| 3 | 3 | 6 | 2 | 5 | 1 | 4 |
| 4 | 4 | 1 | 5 | 2 | 6 | 3 |
| 5 | 5 | 3 | 1 | 6 | 4 | 2 |
| 6 | 6 | 5 | 4 | 3 | 2 | 1 |

| Mod 9 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 2 | 2 | 4 | 6 | 8 | 1 | 3 | 5 | 7 |
| 3 | 3 | 6 | 0 | 3 | 6 | 0 | 3 | 6 |
| 4 | 4 | 8 | 3 | 7 | 2 | 6 | 1 | 5 |
| 5 | 5 | 1 | 6 | 2 | 7 | 3 | 8 | 4 |
| 6 | 6 | 3 | 0 | 6 | 3 | 0 | 6 | 3 |
| 7 | 7 | 5 | 3 | 1 | 8 | 6 | 4 | 2 |
| 8 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |

# Modular Arithmetic

## Multiplicative Inverse

| Mod 7 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| 1 | 1 | 2 | 3 | 4 | 5 | 6 |
| 2 | 2 | 4 | 6 | 1 | 3 | 5 |
| 3 | 3 | 6 | 2 | 5 | 1 | 4 |
| 4 | 4 | 1 | 5 | 2 | 6 | 3 |
| 5 | 5 | 3 | 1 | 6 | 4 | 2 |
| 6 | 6 | 5 | 4 | 3 | 2 | 1 |

| Mod 9 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 2 | 2 | 4 | 6 | 8 | 1 | 3 | 5 | 7 |
| 3 | 3 | 6 | 0 | 3 | 6 | 0 | 3 | 6 |
| 4 | 4 | 8 | 3 | 7 | 2 | 6 | 1 | 5 |
| 5 | 5 | 1 | 6 | 2 | 7 | 3 | 8 | 4 |
| 6 | 6 | 3 | 0 | 6 | 3 | 0 | 6 | 3 |
| 7 | 7 | 5 | 3 | 1 | 8 | 6 | 4 | 2 |
| 8 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |

# Modular Arithmetic

## Multiplicative Inverse

- If $ab \equiv cb \mod N$ and $b$ has a multiplicative inverse $b^{-1}$, then

$$ab \cdot b^{-1} \equiv cb \cdot b^{-1} \mod N \quad \Longrightarrow \quad a \equiv c \mod N.$$

- Which integers $b$ are invertible modulo $N$?

$b$ has a multiplicative inverse modulo $N$ if and only if

$b$ is co-prime to $N$ i.e., $\gcd(b, N) = 1$.

If $N$ is a prime number then each element in $\{1, \ldots, N-1\}$ has a multiplicative inverse.

# Group

- An (abelian) group is a set $\mathbb{G}$ with an operation $\cdot : \mathbb{G} \times \mathbb{G} \to \mathbb{G}$ such that
  - **Associativity:** $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, for all $a, b, c \in \mathbb{G}$.
  - **Commutativity:** $a \cdot b = b \cdot a$**,** for all $a, b, c \in \mathbb{G}$.
  - **Identity element:** There exists $e \in \mathbb{G}$ such that for all $a \in \mathbb{G}$, $e \cdot a = a$.
  - **Inverse element:** For all $a \in \mathbb{G}$, there exists $b \in \mathbb{G}$ such that $a \cdot b = e$.
- Examples: $(\{0\}, +)$, $(\{1\}, \cdot)$, $(\mathbb{Z}_N, +)$, $(\mathbb{Z}_N^*, \cdot)$
- In particular, $\mathbb{Z}_p^* = \{1, \ldots, p-1\}$

# Cyclic Group

- An (abelian) group is a set $\mathbb{G}$ with an operation $\cdot : \mathbb{G} \times \mathbb{G} \to \mathbb{G}$ such that
  - **Associativity:** $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, for all $a, b, c \in \mathbb{G}$.
  - **Commutativity:** $a \cdot b = b \cdot a$**,** for all $a, b, c \in \mathbb{G}$.
  - **Identity element:** There exists $e \in \mathbb{G}$ such that for all $a \in \mathbb{G}$, $e \cdot a = a$.
  - **Inverse element:** For all $a \in \mathbb{G}$, there exists $b \in \mathbb{G}$ such that $a \cdot b = e$.
  - **Generator:** There exists at least one generator $g \in \mathbb{G}$ such that

$$g_1, g^2, g^3, \ldots \text{ produces every element in the group.}$$

# Discrete Logarithm problem

- **Discrete logarithm problem**

  Given: $x \in_R 0, \ldots, p-2$

  $$\langle g \rangle = \mathbb{G} \qquad order(g) = p - 1$$

  $$h = g^x$$

  Find: $x$

  This problem is hard if for all p.p.t. adversaries, all attackers find x with "small" probability

See Boneh-Shoup, Appendix A

# Discrete Logarithm problem

This means that “reversing” exponentiation is assumed to have super-polynomial running time.

How about the exponentiation itself?

- **Discrete logarithm problem**

  Given: $x \in_R 0, \ldots, p-2$

  $$\langle g \rangle = \mathbb{G} \qquad order(g) = p - 1$$

  $$h = g^x$$

  Find: $x$

  This problem is hard if for all p.p.t. adversaries, all attackers find x with “small” probability

See Boneh-Shoup, Appendix A

# Discrete Logarithm problem

This means that “reversing” exponentiation is assumed to have super-polynomial running time.

How about the exponentiation itself?

- **Discrete logarithm problem**

  Given: $x \in_R 0, \ldots, p-2$

  $\langle g \rangle = \mathbb{G}$ $order(g) = p$

  $h = g^x$

  Find: $x$

Note that for this to hold, the size of *p* must be pretty large!

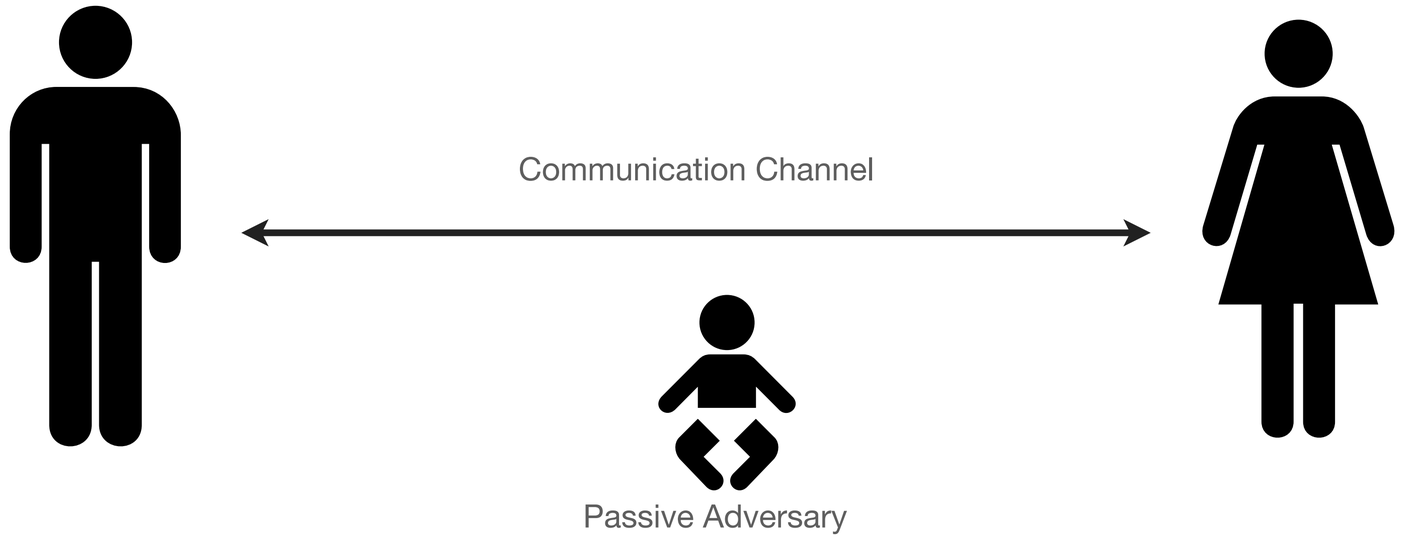
In practice, we typically assume *p* is at least 1024 bits. And 3072 bits is the minimum in modern protocols!

This problem is hard if for all p.p.t. adversaries, all attackers find x with “small” probability

See Boneh-Shoup, Appendix A

# Key Agreement

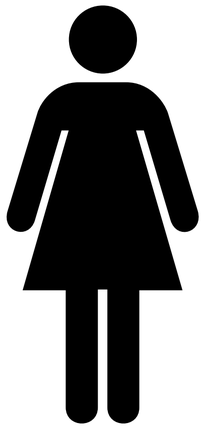
- Establish a shared key in the presence of a passive adversary

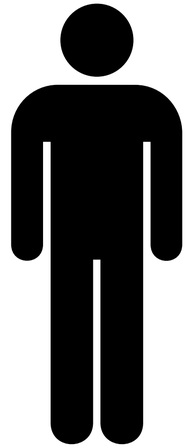


# D-H Protocol

$$p, \langle g \rangle = \mathbb{Z}_p^*$$

$$a \in \mathbb{Z}_{\phi(p)}$$

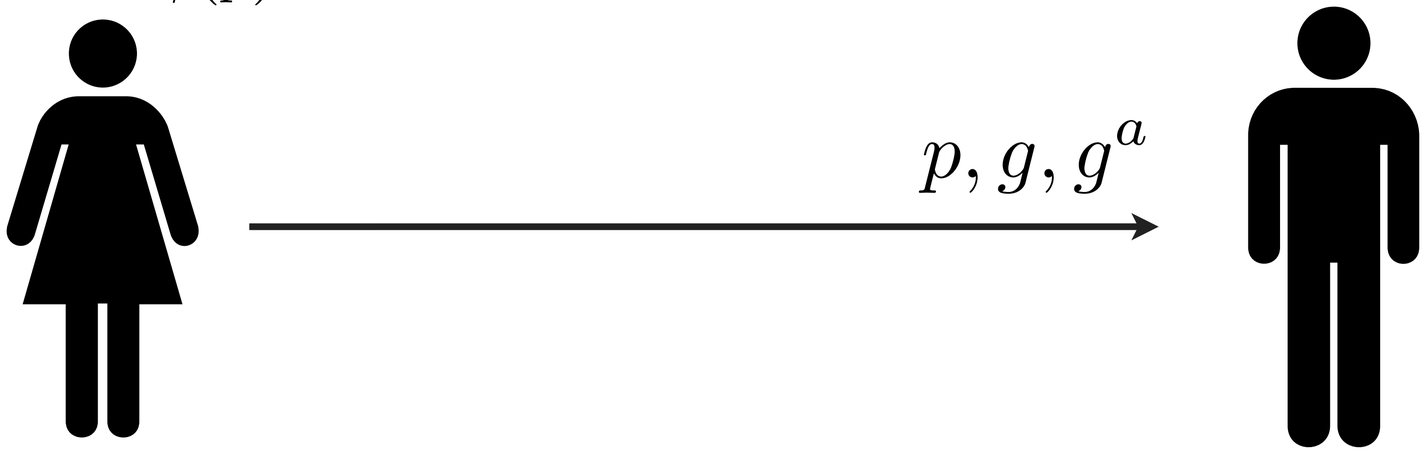




# D-H Protocol

$$p, \langle g \rangle = \mathbb{Z}_p^*$$

$$a \in \mathbb{Z}_{\phi(p)}$$

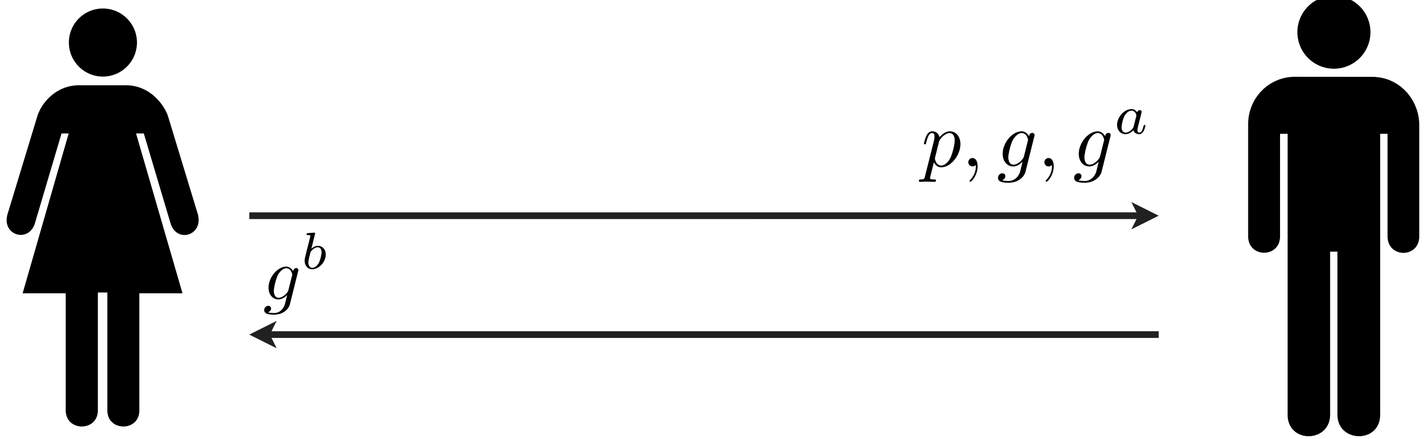


# D-H Protocol

$p, \langle g \rangle = \mathbb{Z}_p^*$

$a \in \mathbb{Z}_{\phi(p)}$

$b \in \mathbb{Z}_{\phi(p)}$

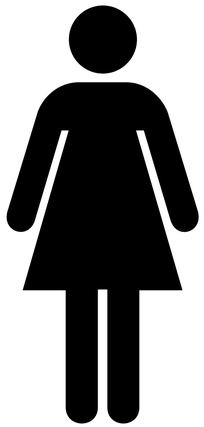


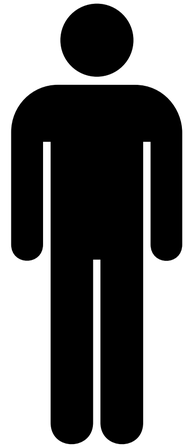
# D-H Protocol

$p, \langle g \rangle = \mathbb{Z}_p^*$

$a \in \mathbb{Z}_{\phi(p)}$

$b \in \mathbb{Z}_{\phi(p)}$





$p, g, g^a$

$g^b$

$g^{ba}$

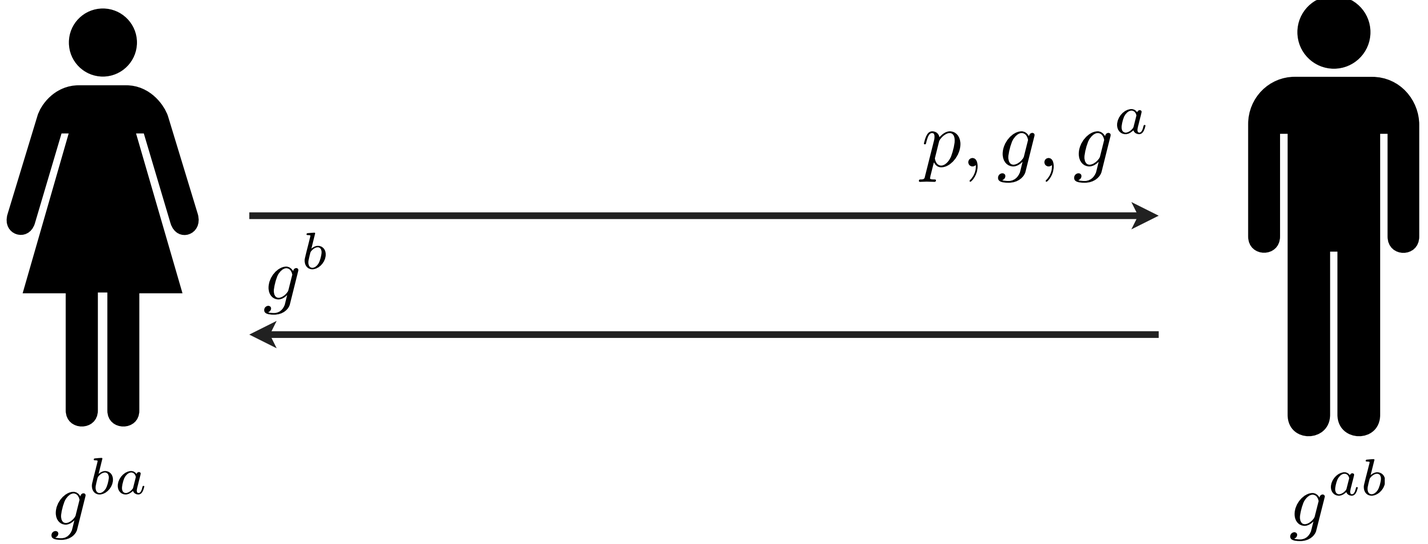
$g^{ab}$

# D-H Protocol

$p, \langle g \rangle = \mathbb{Z}_p^*$

$a \in \mathbb{Z}_{\phi(p)}$

$b \in \mathbb{Z}_{\phi(p)}$




Usually we “hash” the shared secret value to make a secret encryption key, and then encrypt using a fast symmetric encryption scheme!

# Hard problems (2)

- **Diffie-Hellman problem**

  Given: $a, b \in_R 0, \ldots, p-2$

  $$\langle g \rangle = \mathbb{G} \qquad order(g) = p - 1$$

  $$(g, g^a, g^b)$$

  Find: $g^{ab}$

  This problem is hard if for all p.p.t. adversaries, all attackers output a solution with “small” probability

See Boneh-Shoup, Appendix A

# Hard problems (2)

- **Diffie-Hellman problem**

  Given: $a, b \in_R 0, \ldots, p-2$

  $$\langle g \rangle = \mathbb{G} \qquad order(g) = p - 1$$

  $$(g, g^a, g^b)$$

  Find: $g^{ab}$

  This problem is hard if for all p.p.t. adversaries, all attackers output a solution with “small” probability.

Notice this is just the Diffie-Hellman scheme re-written as a mathematical assumption!

See Boneh-Shoup, Appendix A

# Hard problems (2)

- **Diffie-Hellman problem**

  Given: $a, b \in_R 0, \ldots, p-2$

  $\langle g \rangle = \mathbb{G} \qquad order(g) = p - 1$

  $(g, g^a, g^b)$

  Find: $g^{ab}$

Notice this is just the Diffie-Hellman scheme re-written as a mathematical assumption!

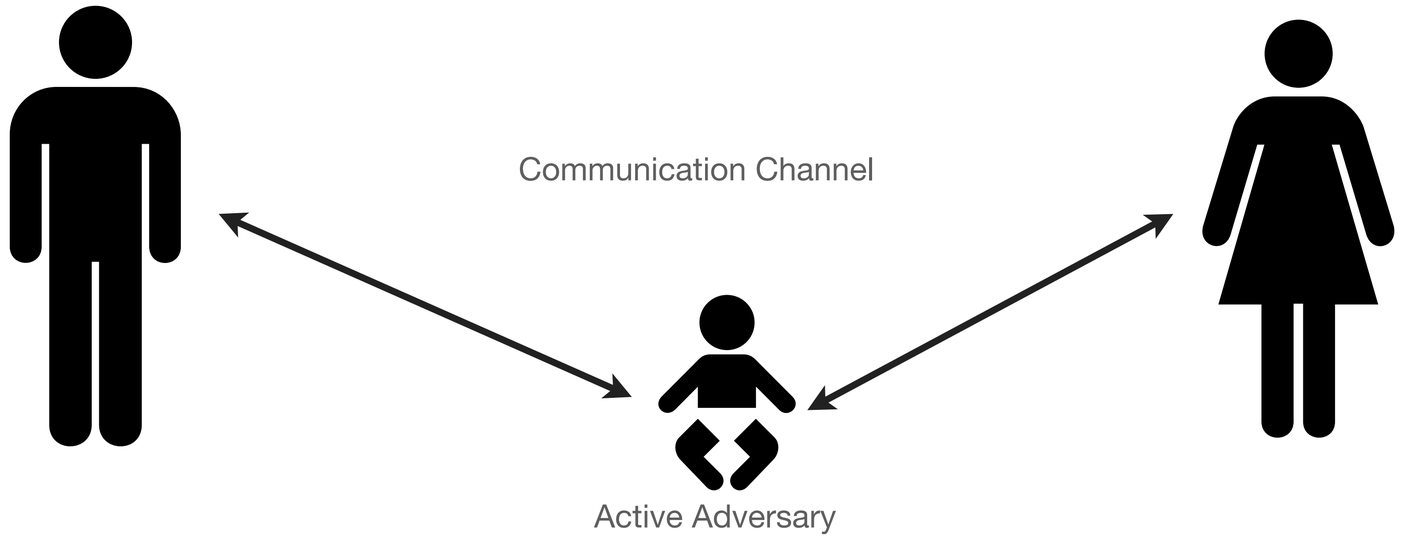
Note that for this to hold, the size of *p* must be pretty large!

In practice, we typically assume *p* is at least 1024 bits. And 3072 bits is the minimum in modern protocols!

This problem is hard if for all p.p.t. adversaries, all attackers output a solution with “small” probability.

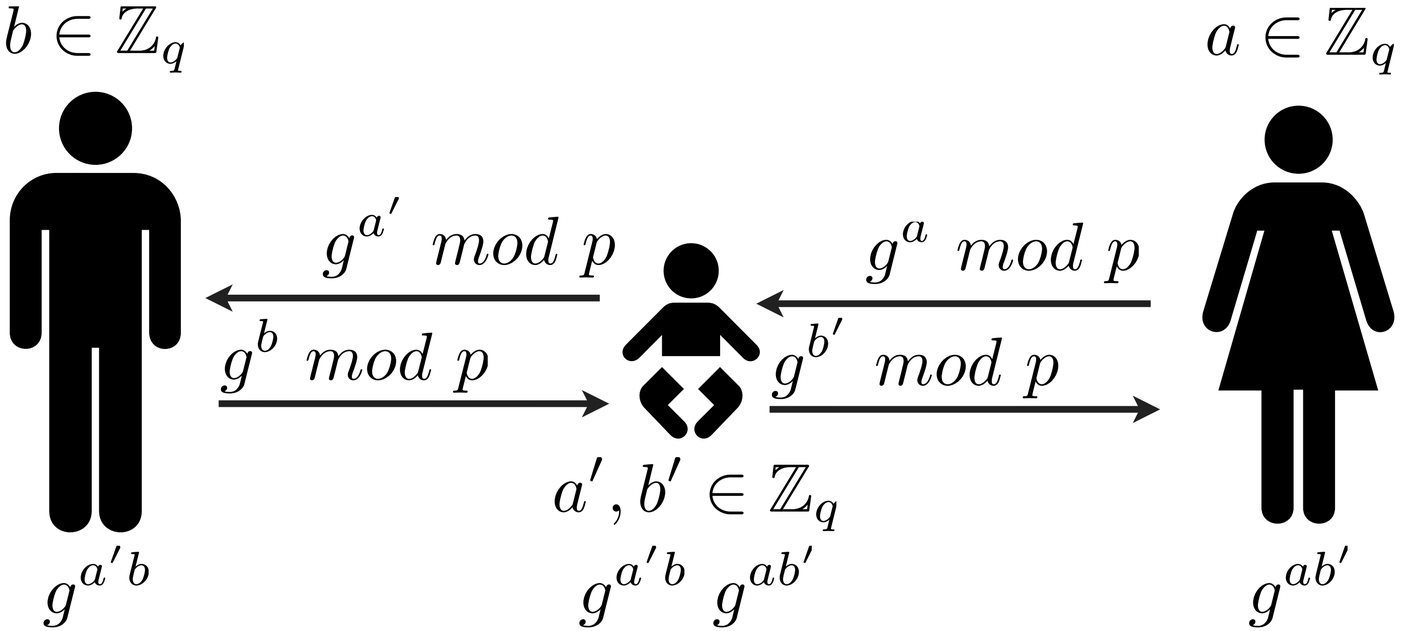
See Boneh-Shoup, Appendix A

# What if we have an active adversary?



# Man in the Middle

- Assume an active adversary:



# Man in the Middle

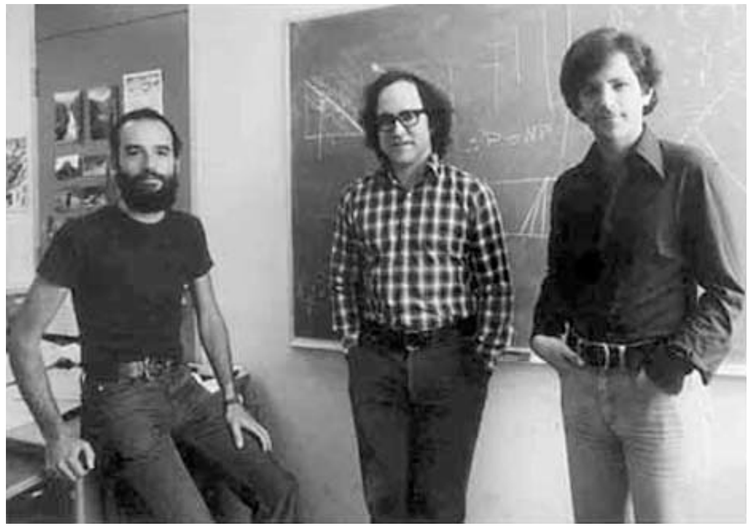
- Caused by lack of authentication
  - D-H lets us establish a shared key with anyone...
    but that's the problem…
  - We don't know if the person we're talking to is the right person
- Solution?

# Preventing MITM

- Verify key via separate channel
- Password-based authentication
- Authentication via PKI

# Public Key Encryption

- What if our recipient is offline?
  - Key agreement protocols are interactive
  - e.g., want to send an email



# Public Key Encryption