601.445/645
Practical Cryptographic Systems

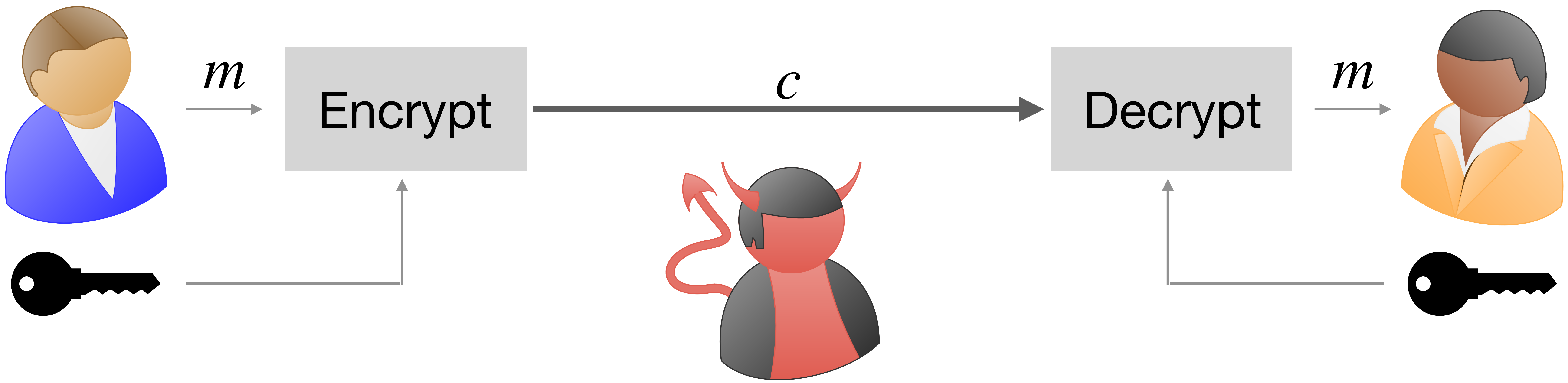
Asymmetric Cryptography II

Instructor: Matthew Green

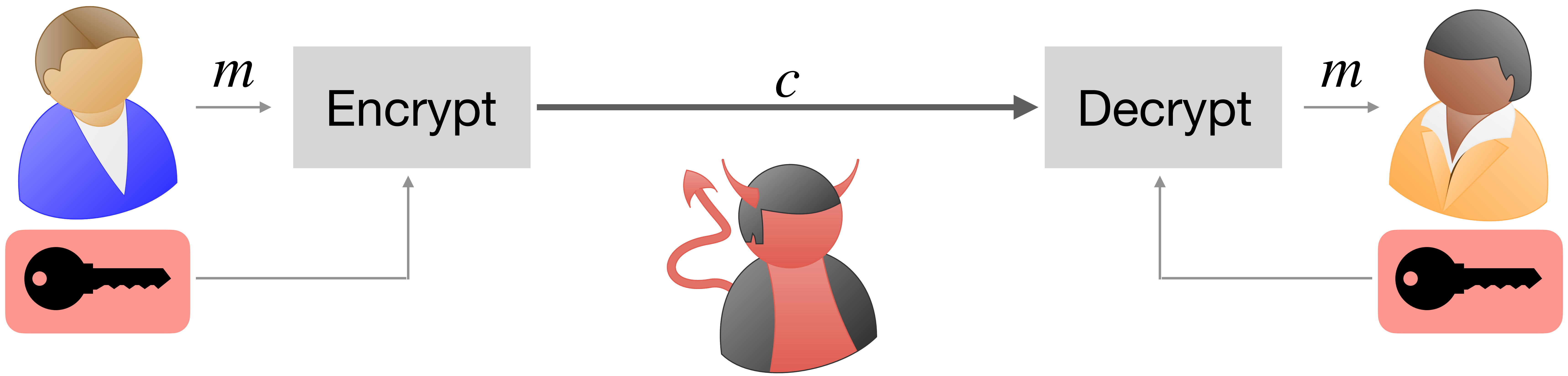
Housekeeping

- 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

Review

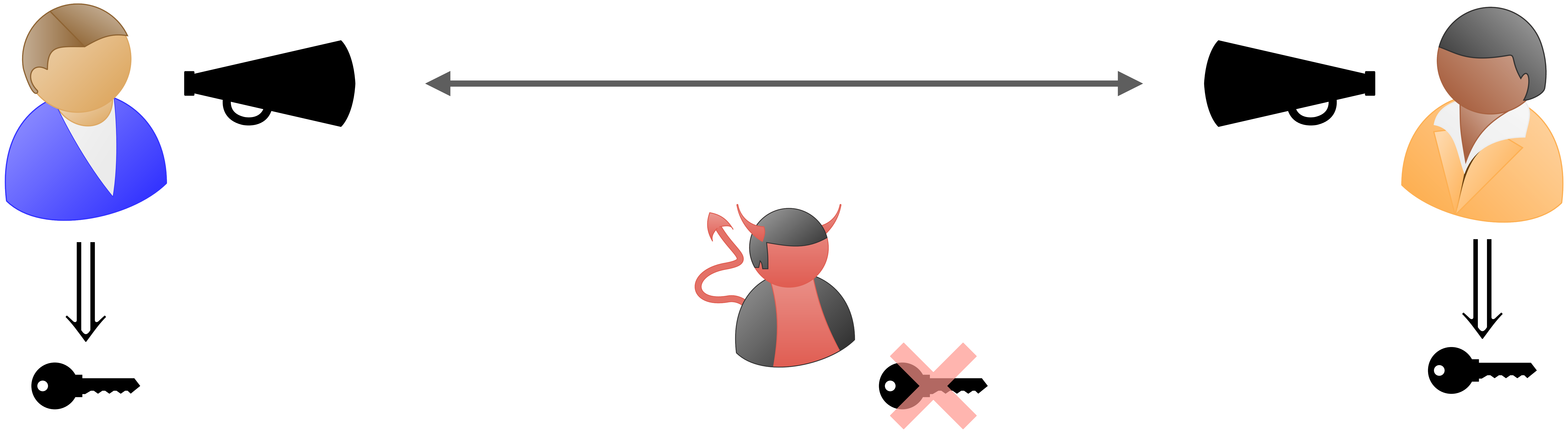


Review



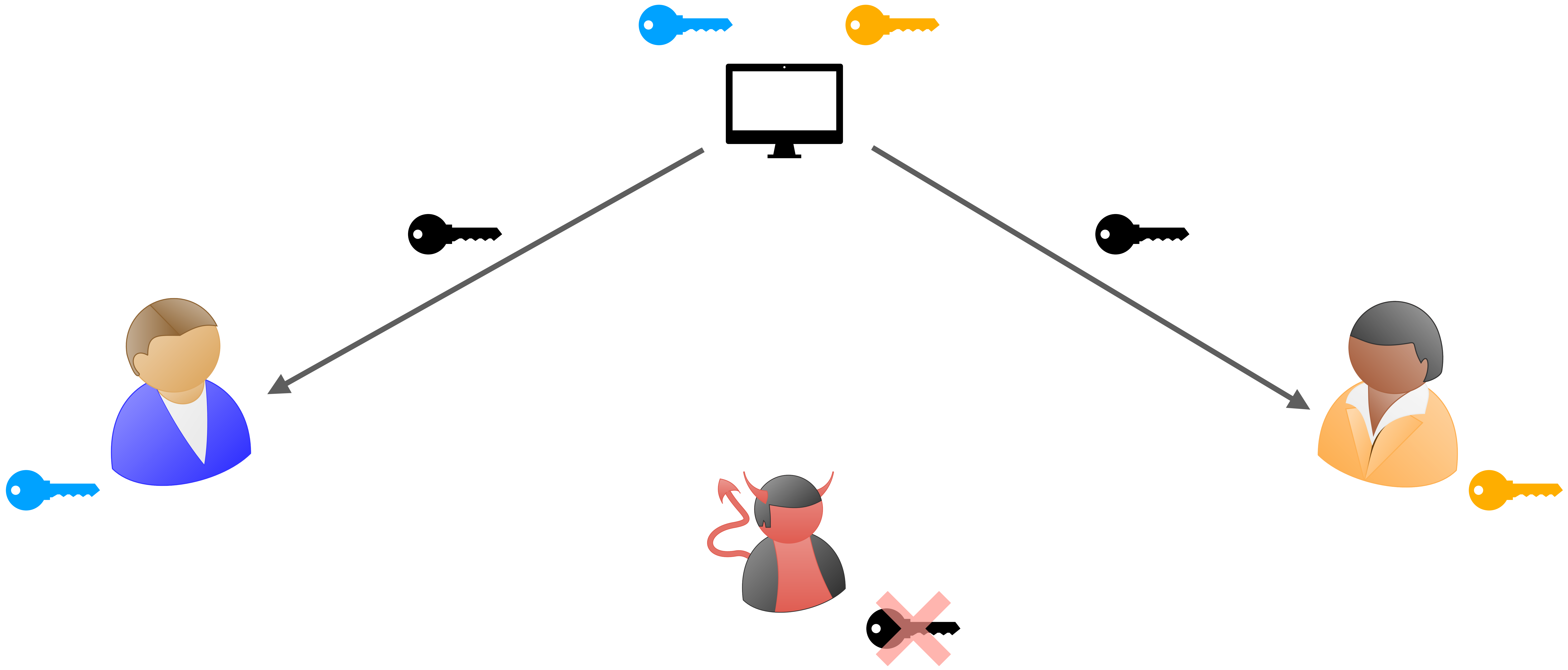
How do parties agree on a common key?

Key Exchange



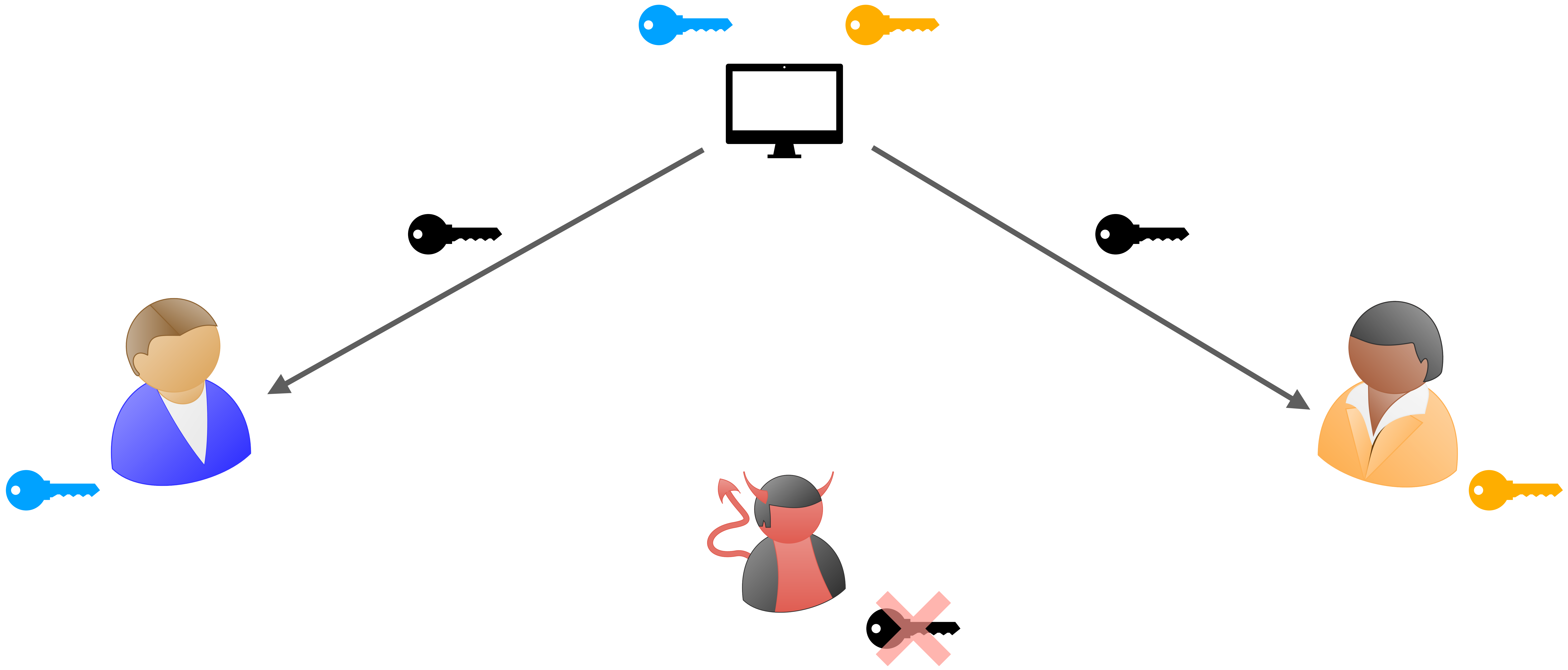
Key Exchange

Kerberos



Key Exchange

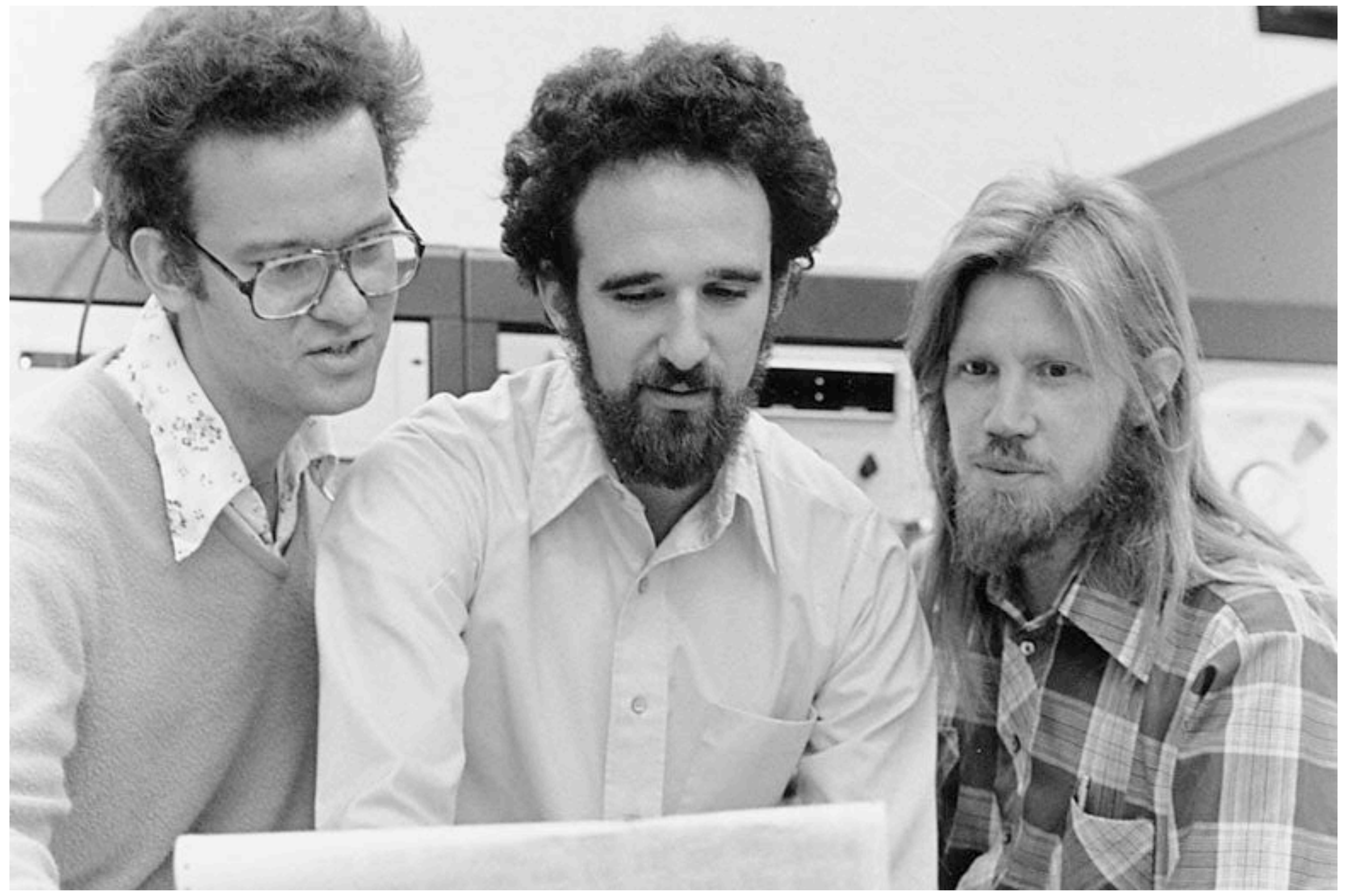
Kerberos

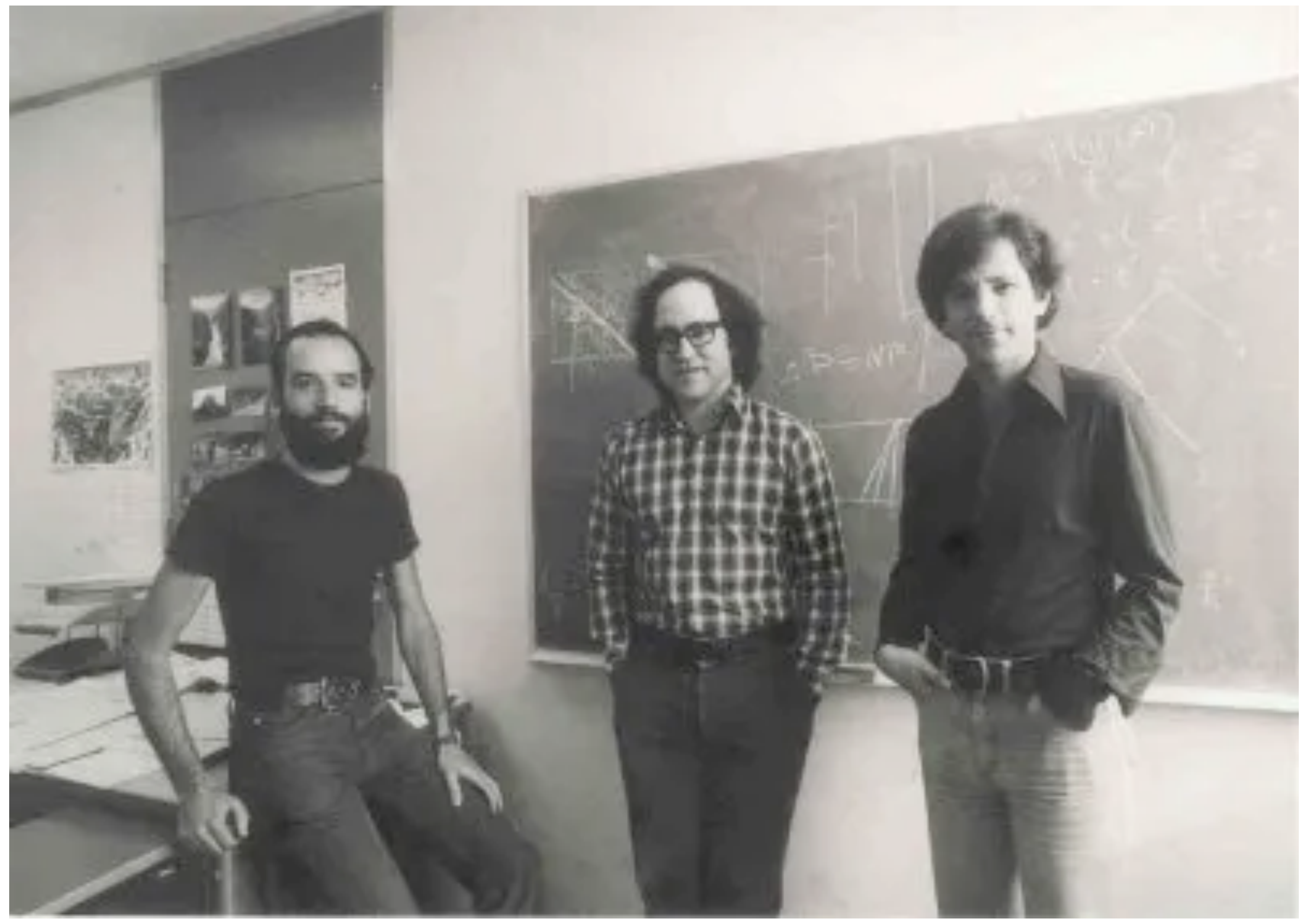


Drawbacks?

Asymmetric Cryptography

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



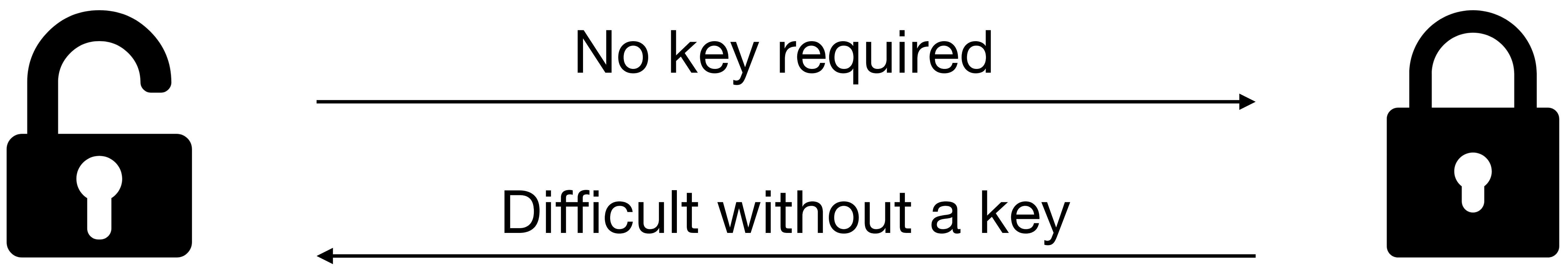


Diffie-Hellman Key Exchange

Agreeing on a common secret over an untrusted/public channel

Key Idea: Exploiting asymmetry

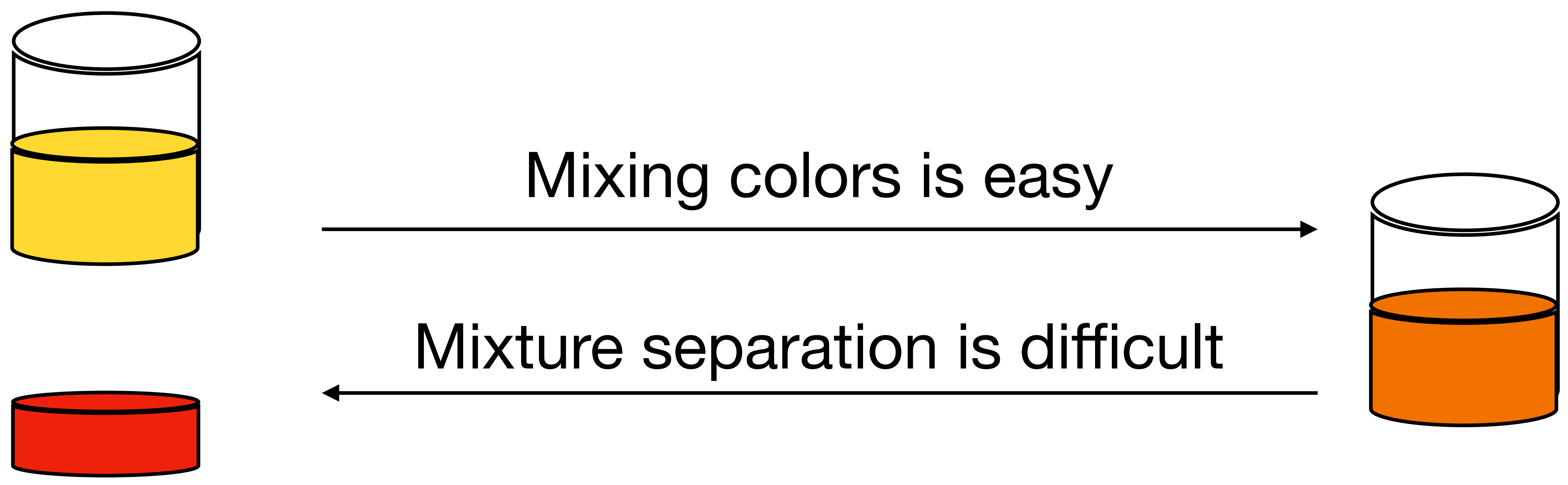
Often present in the real world!



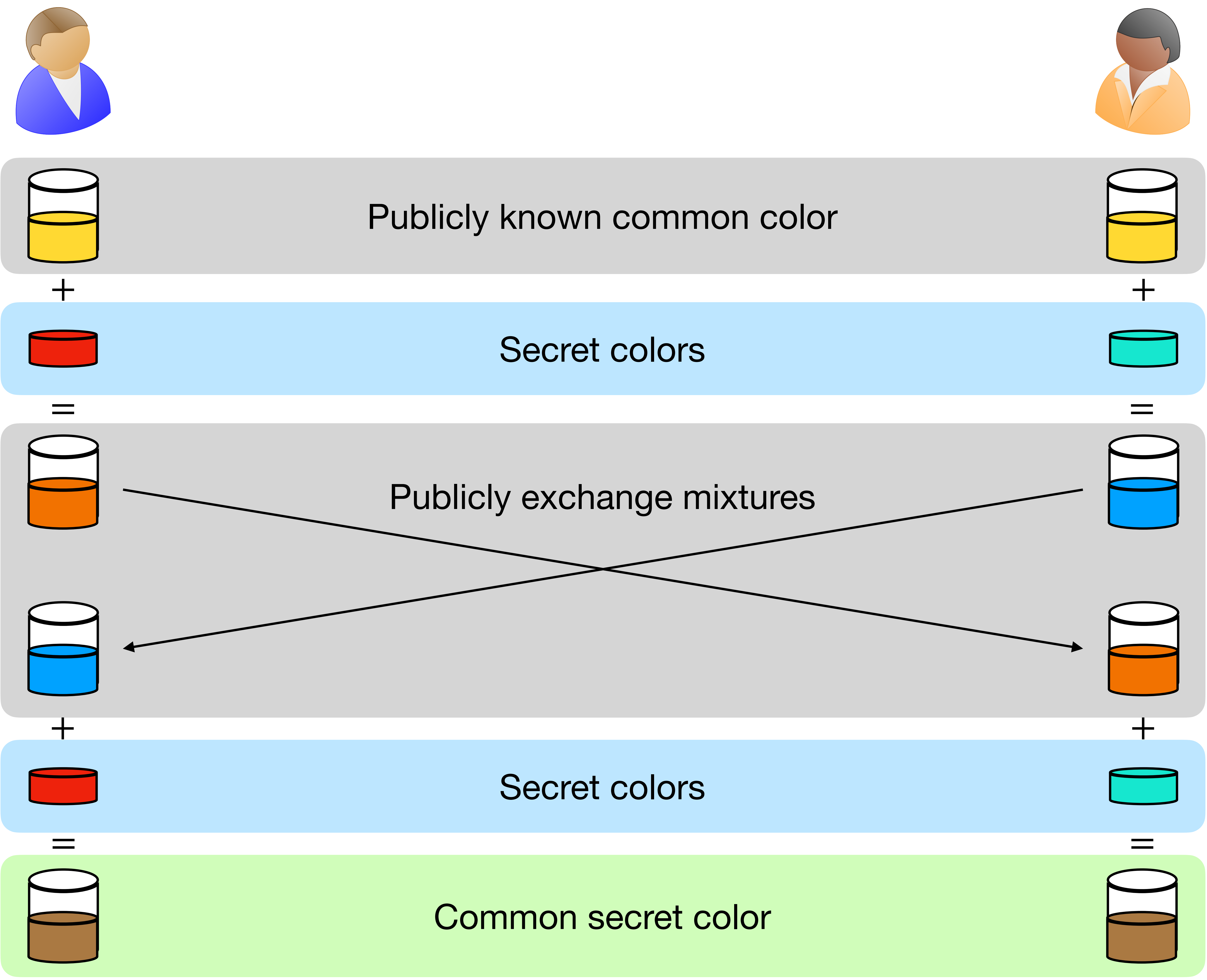
Diffie-Hellman Key Exchange

Agreeing on a common secret over an untrusted/public channel

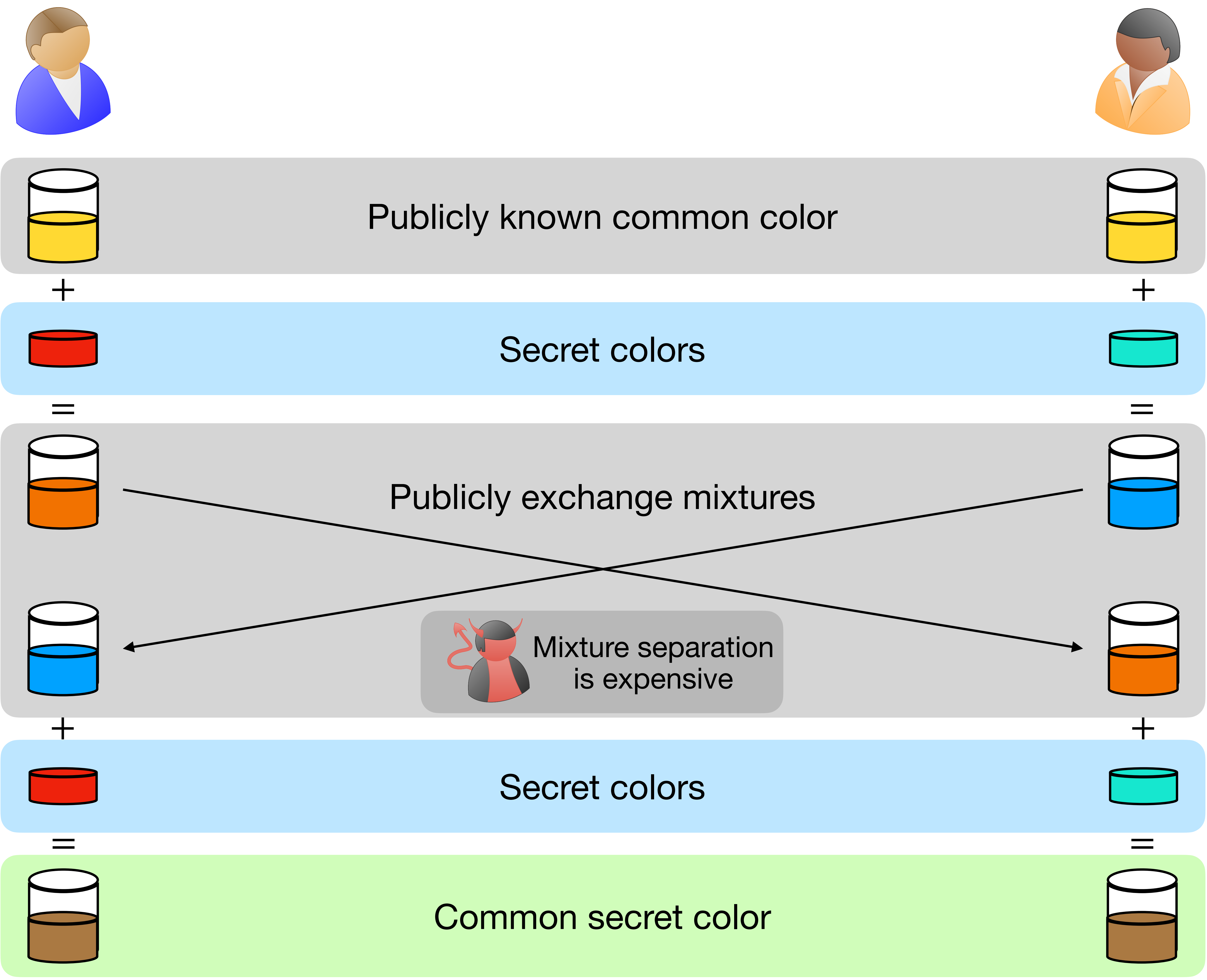
Key Idea: Exploiting asymmetry



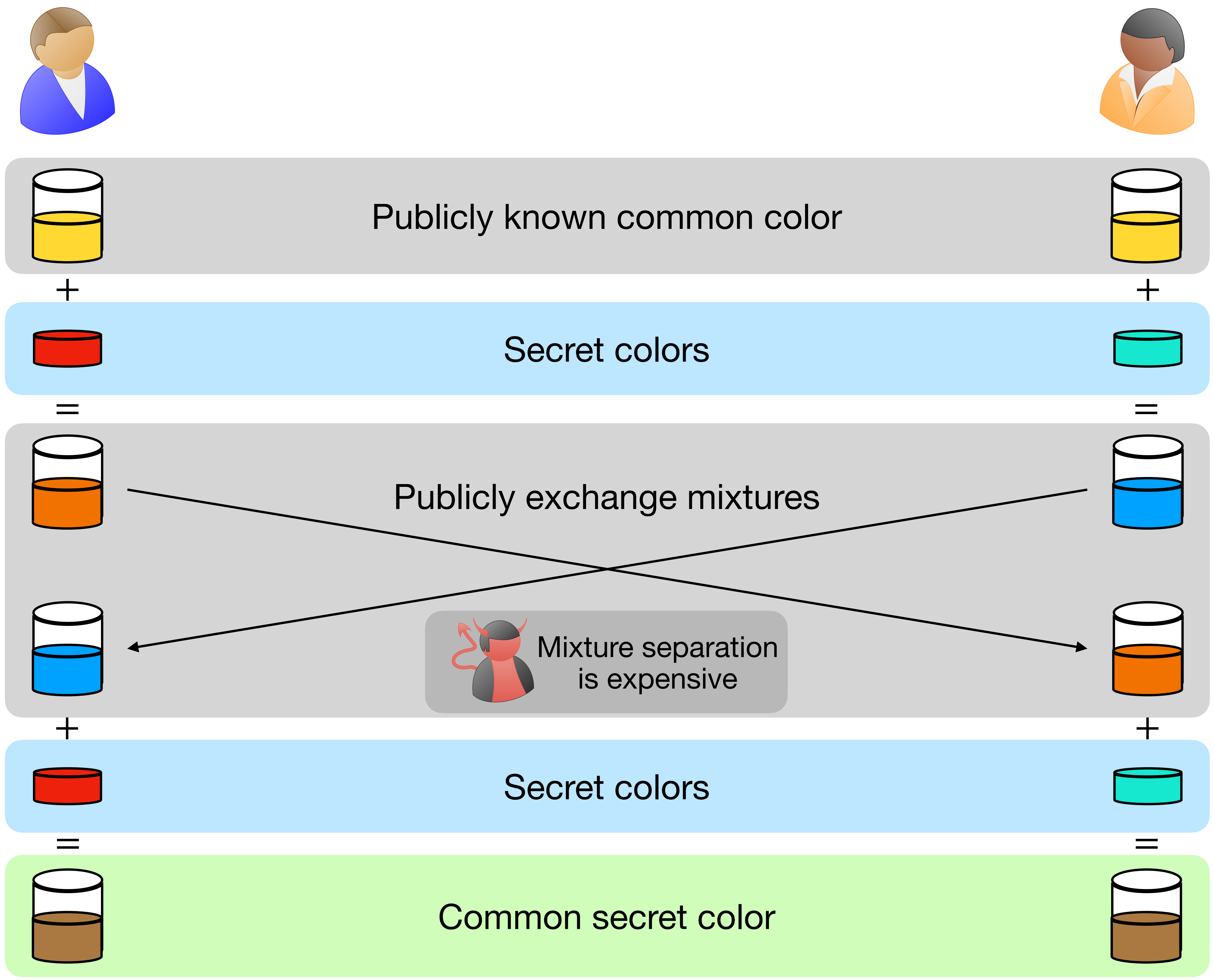
Diffie-Hellman Key Exchange



Diffie-Hellman Key Exchange



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 $N > 1$

$[a \bmod N] \equiv$ remainder when a 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 $a \equiv b \bmod N$ and $c \equiv d \bmod N$
  - $a + c \equiv b + d \bmod N$
  - $a - c \equiv b - d \bmod N$
  - $a \cdot c \equiv b \cdot d \bmod N$

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

- What about division?

Modular Arithmetic

Division

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

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

  - It may not even be well defined:

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

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

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

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 $\{0,\ldots,N-1\}$.
  - We denote this multiplicative inverse by b^{-1}

Modular Arithmetic

Multiplicative Inverse

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

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

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

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

- 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

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