CS 442
Introduction to Cryptography

Lecture 20: Key Exchange

Instructor: Aarushi Goel

Spring 2026

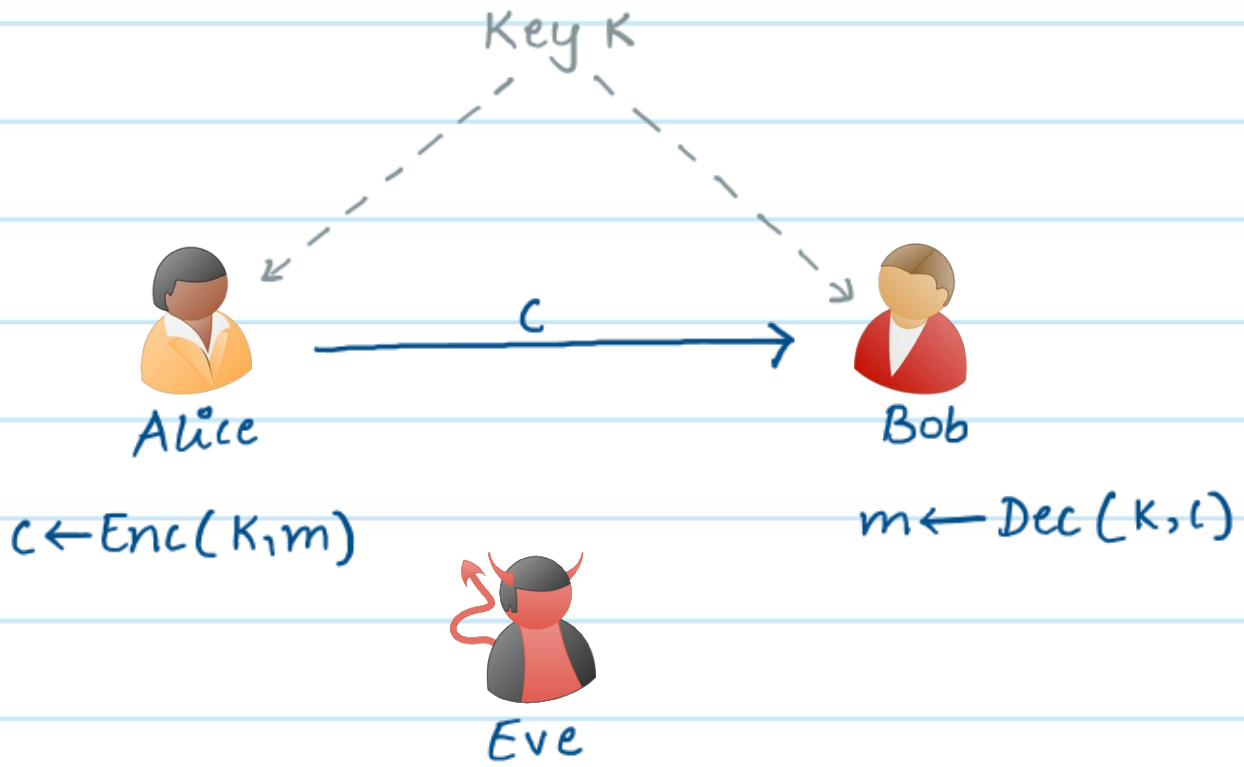
Agenda

* Key-exchange problem
* Diffie-Hellman Key-exchange protocol

* HW4 will be released today.

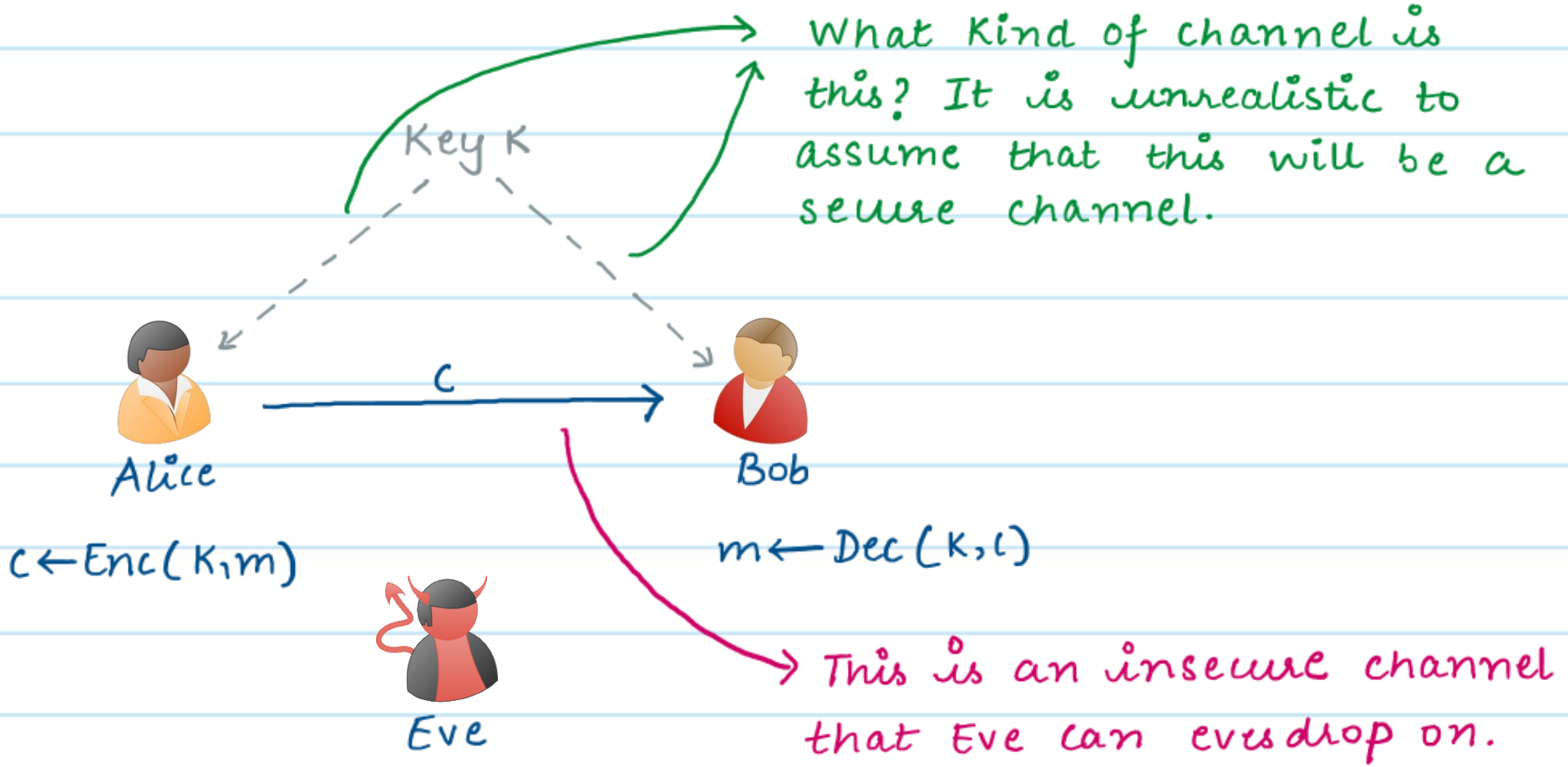
Encryption

* So far, when discussing encryption schemes, we assumed that Alice and Bob have a pre-shared *secret* key.



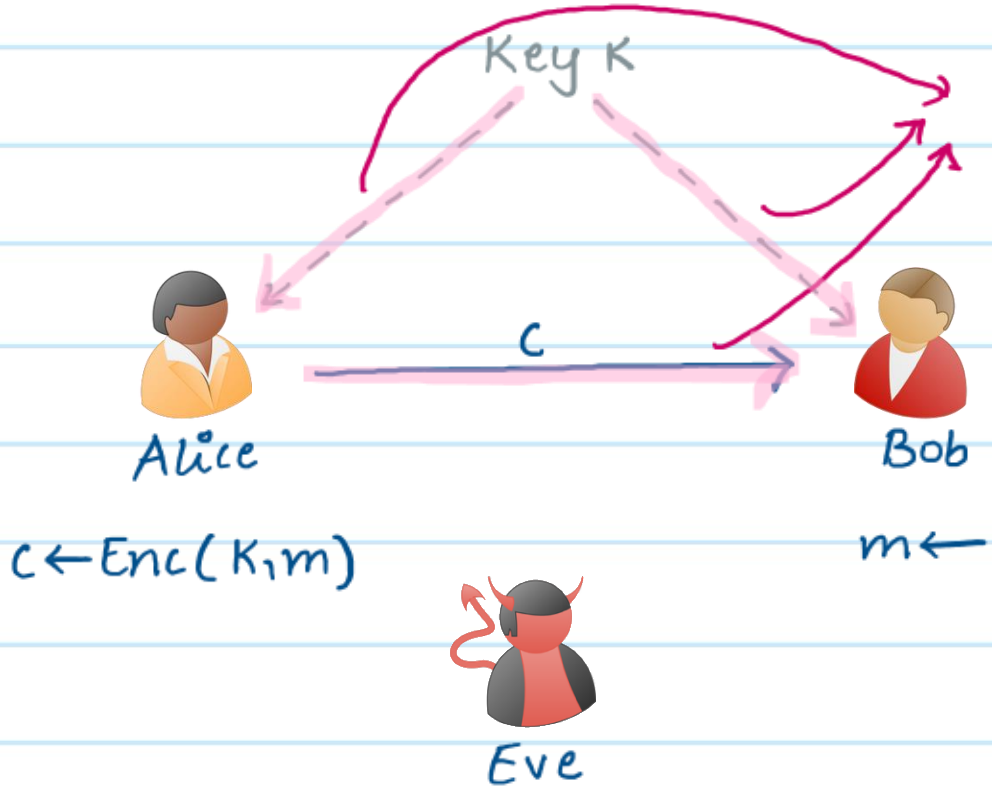
Key - Exchange Problem

* How do Alice and Bob share this key?



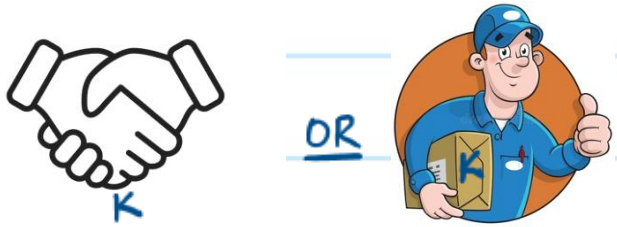
Key - Exchange Problem

* It is more realistic to believe that all of these are insecure communication channels.
* How do Alice and Bob share this key over an insecure communication channel?



Key-Exchange Problem : Attempt 1

Trusted Courier or face-to-face meeting.



Alice

$c \leftarrow Enc(K, m)$

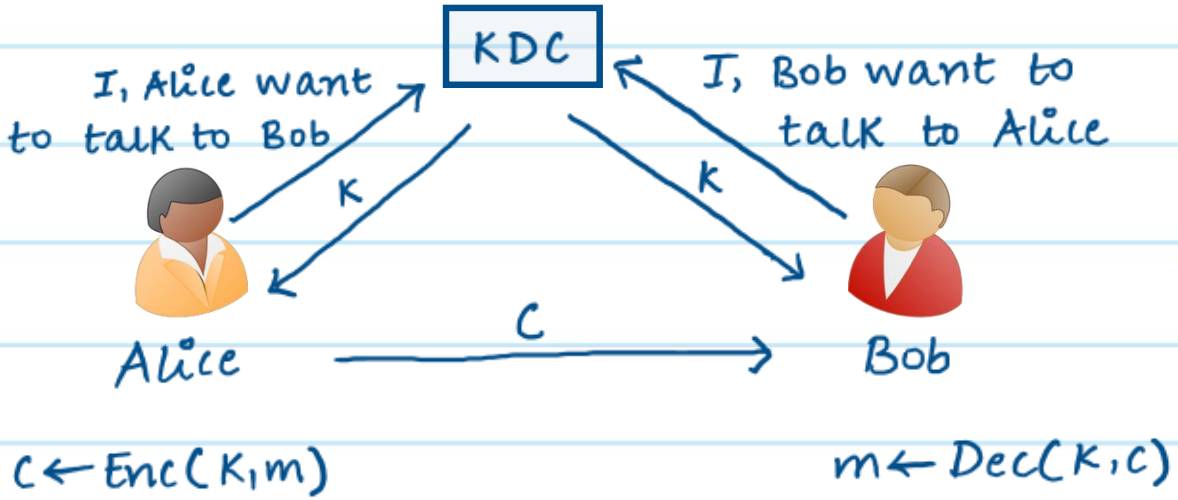
Bob

$m \leftarrow Dec(K, c)$

PROBLEM. Not practical for large-scale applications!

Key-Exchange Problem : Attempt 2

Key-distribution centers: have a trusted center with whom Alice and Bob are *registered* and they can request the trusted center for the shared Key.



PROBLEM: Requires trusting these centers, creates a single-point of failure, doesn't scale.

Key-Exchange Protocol

* A way to establish a secret key via insecure communication channel.
* A protocol is an *interactive algorithm*.

Alice

Bob

A_1 →

← B_1

Sample randomness r_A

Sample randomness r_B

A_2 →

← B_2

⋮

A_l →

← B_l

At the end, based on these messages, outputs K_A.

At the end, based on these messages, Bob outputs K_B.

Key-Exchange Protocol

* A way to establish a secret key via insecure communication channel.
* A protocol is an *interactive algorithm*.

Alice

Bob

These messages are called the transcript.

A_1

B_1

A_2

B_2

A_l

B_l

Eve can eavesdrop on all these channels.

Sample randomness r_A

Sample randomness r_B

At the end, based on these messages, outputs K_A.

At the end, based on these messages, Bob outputs K_B.

Key-Exchange Protocol

randomized

Definition: A two-party key-exchange protocol π is a probabilistic interactive algorithm between two parties Alice and Bob, where transcript represents all the messages exchanged between Alice and Bob during the protocol. At the end, Alice locally computes $K_A \in \{0,1\}^n$, and Bob locally computes $K_B \in \{0,1\}^n$.

* **Correctness:** $\forall n \in \mathbb{N}$, $Pr[K_A = K_B] = 1$
* **Security:** For all PPT adversaries Eve, there exists a negligible function $\nu(.)$, such that, for $r \xleftarrow{\$} \{0,1\}^n$,

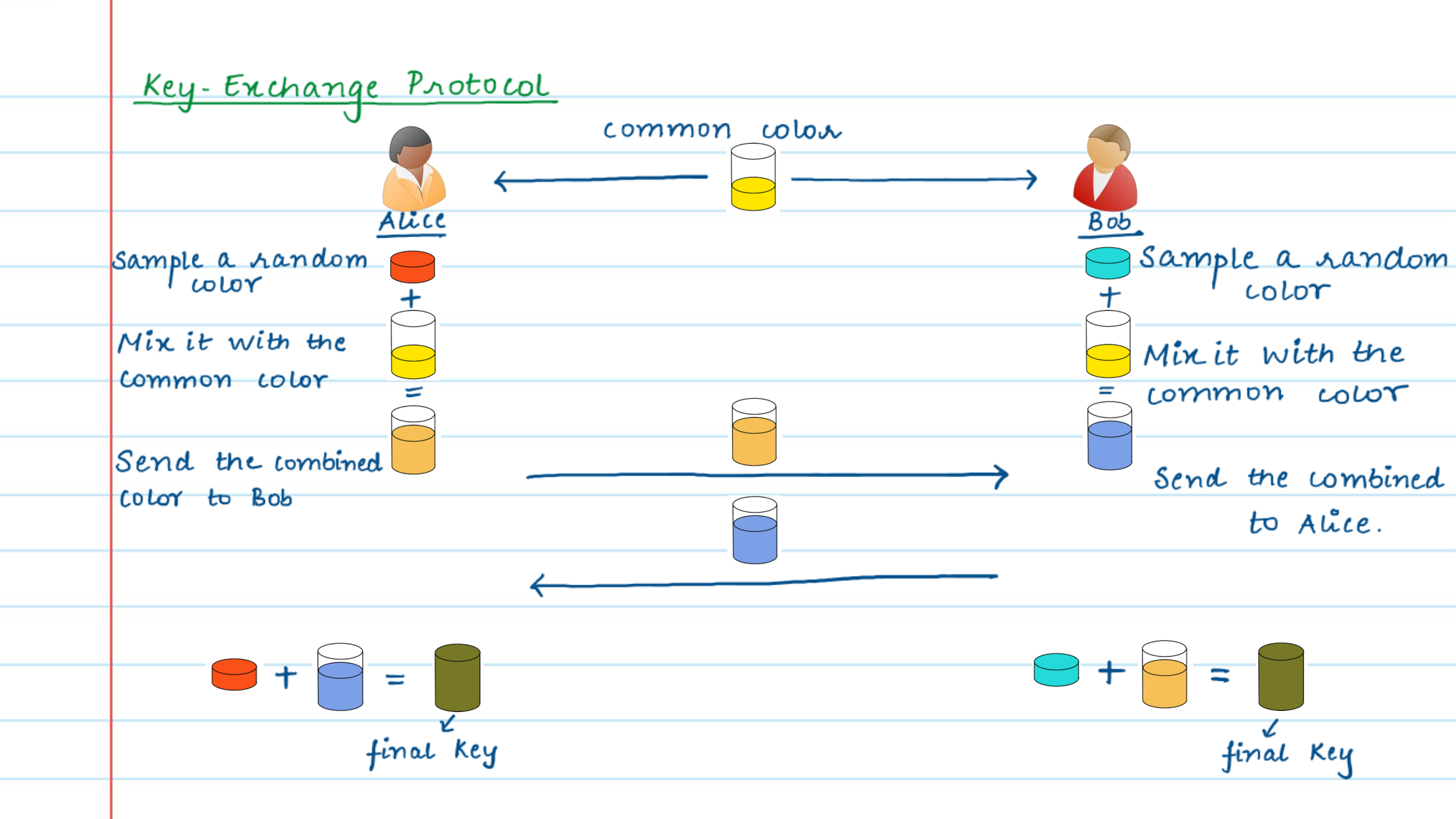
$$Pr[Eve(transcript, K_A) = 1] - Pr[Eve(transcript, r) = 1] \leq \nu(n).$$

In other words.

$$\{(transcript, K_A)\} \approx_c \{(transcript, r)\}$$

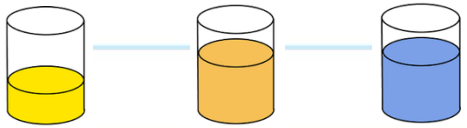
computationally indistinguishable.

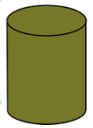
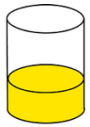
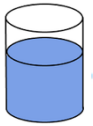
Key-Exchange Protocol



Correctness: Both Alice and Bob mix the same set of colors and hence end up with the same final key.

Security: What does Eve see in this protocol?



* In order to learn the final key  , Eve needs to know which color was mixed with  to get  or  .
* However, this color separation is hard.
* Hence, Eve cannot learn the key with very high probability.

Basic Group Theory

Recall the definition of groups.

Definition: A group, represented by $(G, \circ)$, is defined by a set G and a binary operator $\circ$ that satisfies the following properties:

* **Closure**: $\forall\ a, b \in G$, we have $a \circ b \in G$
* **Associativity**: $\forall\ a, b, c \in G$, we have $(a \circ b) \circ c = a \circ (b \circ c)$
* **Identity**: $\exists$ an element $e \in G$, such that $\forall\ a \in G$, we have $a \circ e = a$
* **Inverse**: $\forall$ elements $a \in G$, $\exists$ an element $(-a) \in G$, such that $a \circ (-a) = e$

Basic Group Theory

* Group exponentiation: For a group $(G, \cdot)$. and group elements $g, h \in G$

$$g^m = \overbrace{g \cdot g \cdots g}^{m}, \quad g^0 = e, \quad g^{-m} = (g^{-1})^m$$

$$g^{m_1} \cdot g^{m_2} = g^{m_1 + m_2}, \quad (g^{m_1})^{m_2} = g^{m_1 \cdot m_2}, \quad g^m \cdot h^m = (g \cdot h)^m$$

* For a finite group, we use $|G|$ to denote its order (# of elements)
* Let G be a group of order q.
* G is a cyclic group if $\exists g \in G$, s.t. $\{g^0, g^1, \cdots, g^{q-1}\} = G$.
  g is called the generator of G.

Diffie - Hellman Assumptions

Let's sample a cyclic group $(G, \cdot)$ of order q with generator g.

* Decisional Diffie-Hellman (DDH) Assumption: Sample $x, y, z \xleftarrow{\$} \mathbb{Z}_q$, compute $h_1 = g^x$, $h_2 = g^y$. Given (G, q, g, h_1, h_2), it is computationally hard to distinguish between g^{xy} and g^z.

In other words,

$$(G, g, q, h_1, h_2, g^{xy}) \approx_c (G, g, q, h_1, h_2, g^z)$$

$\approx_c$: computationally indistinguishable.

Diffie - Hellman Assumptions

* This problem is assumed to be computationally hard.
* In other words, *we don't know* of any PPT algorithms to solve it.

  Note that this does not mean that PPT algorithms for solving it cannot exist. It simply means that no one has been able to find one yet. This is why it is only assumed to be hard
* Modern cryptographic primitives are based on the hardness assumptions of such problems. That is, if a PPT Eve can solve these problems, then they can break security of the cryptographic primitive.

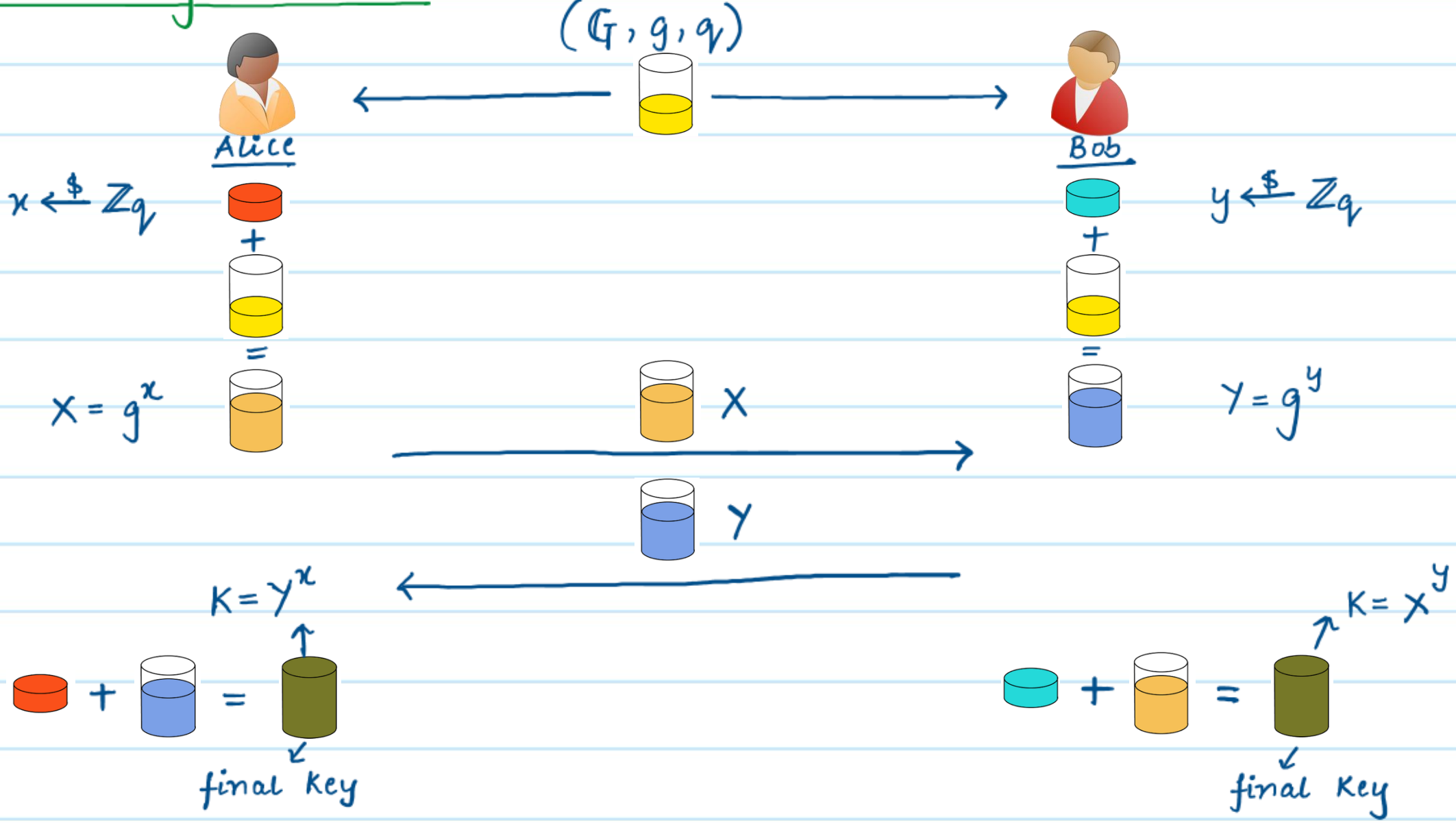
Diffie-Hellman Key-Exchange Protocol

Whitfield Diffie

Martin Hellman

* A key exchange protocol from 1976.
* Security of this protocol is based on the decisional Diffie-Hellman assumption
* A concrete (mathematical) way to implement the coloring based protocol.

Diffie-Hellman Key-Exchange Protocol



Diffie-Hellman Key-Exchange Protocol

Alice

Bob

$(\mathbb{G}, g, q)$

$x \xleftarrow{\$} \mathbb{Z}_q$

$y \xleftarrow{\$} \mathbb{Z}_q$

$X = g^x$

X

$Y = g^y$

Y

$K = Y^x$

$K = X^y$

Correctness.

$$Y^x = (g^y)^x = g^{xy}$$

$$X^y = (g^x)^y = g^{xy}$$

Both Alice and Bob compute the same key.

Security: What does Eve get to see in this protocol?

$$\text{transcript} = (\mathbb{G}, g, q, X, Y)$$

* For security, we need to show that:

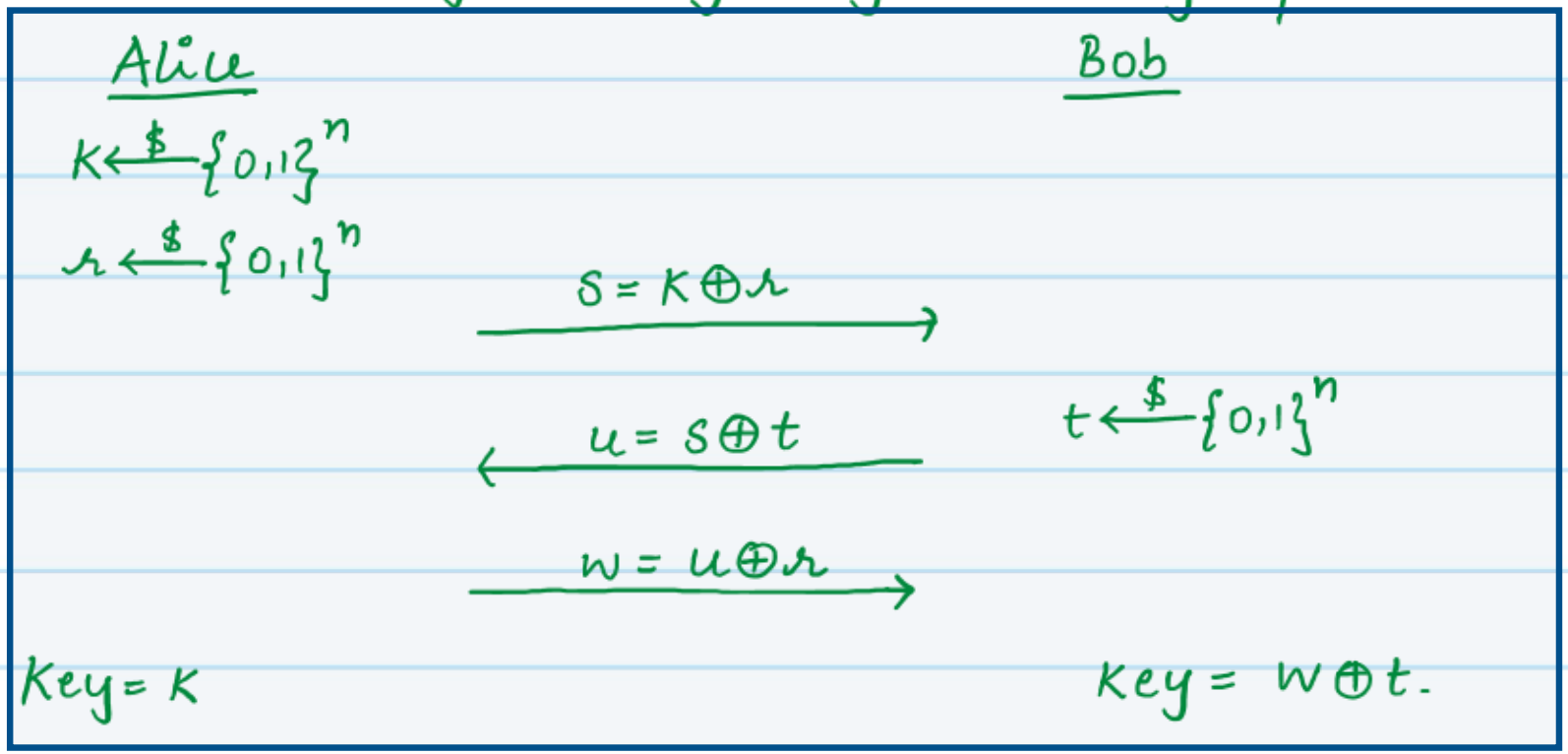
$$\{(\text{transcript}, \text{key})\} \approx_c \{(\text{transcript}, r)\}, \quad r \in \mathbb{G}$$

$$(\mathbb{G}, g, q, X, Y, K) \qquad (\mathbb{G}, g, q, X, Y, r)$$

* According to the decisional Diffie-Hellman assumption, it is hard to distinguish between these two distributions.
* Security of this key-exchange protocol follows from the decisional Diffie-Hellman assumption

Another Protocol

Ques Consider the following key-exchange protocol:



Is this a secure key-exchange protocol?

No! Eve can easily compute $K = w \oplus u \oplus s$. Since Eve can learn the key, this is not a secure protocol for key-exchange.