Diffie-Hellman Key Exchange Color Mixing Example

Dr. Nausheen Shoaib

The Problem of Key Exchange

- One of the main problems of symmetric key encryption is it requires a secure & reliable channel for the shared key exchange.

- The Diffie-Hellman Key Exchange protocol offers a way in which a public channel can be used to create a confidential shared key.

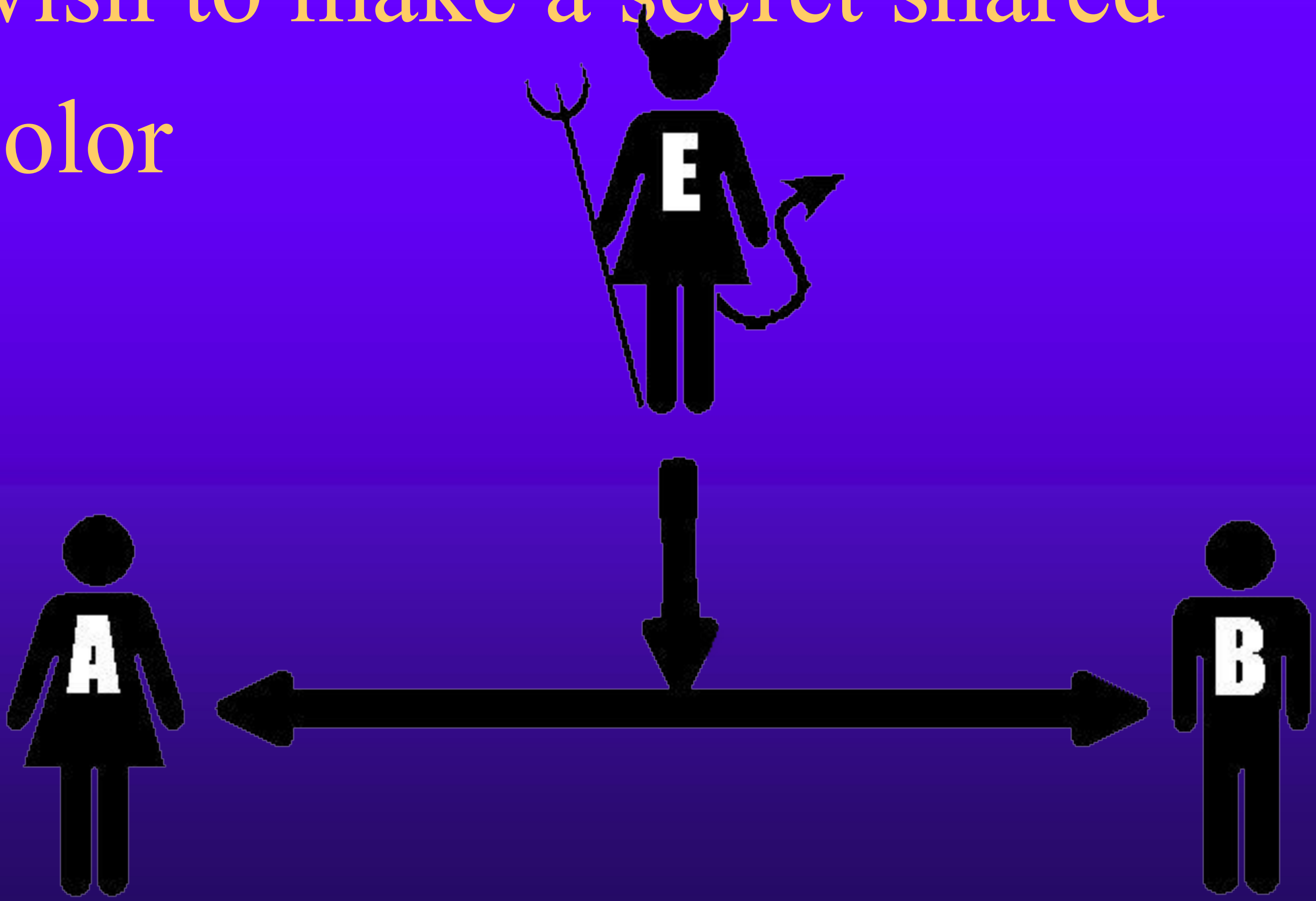
Modular what?

- In practice the shared encryption key relies on such complex concepts as *Modular Exponentiation*, *Primitive Roots* and *Discrete Logarithm Problems*.
- Let’s see though is we can explain the Diffie-Hellman algorithm with no complex mathematics.

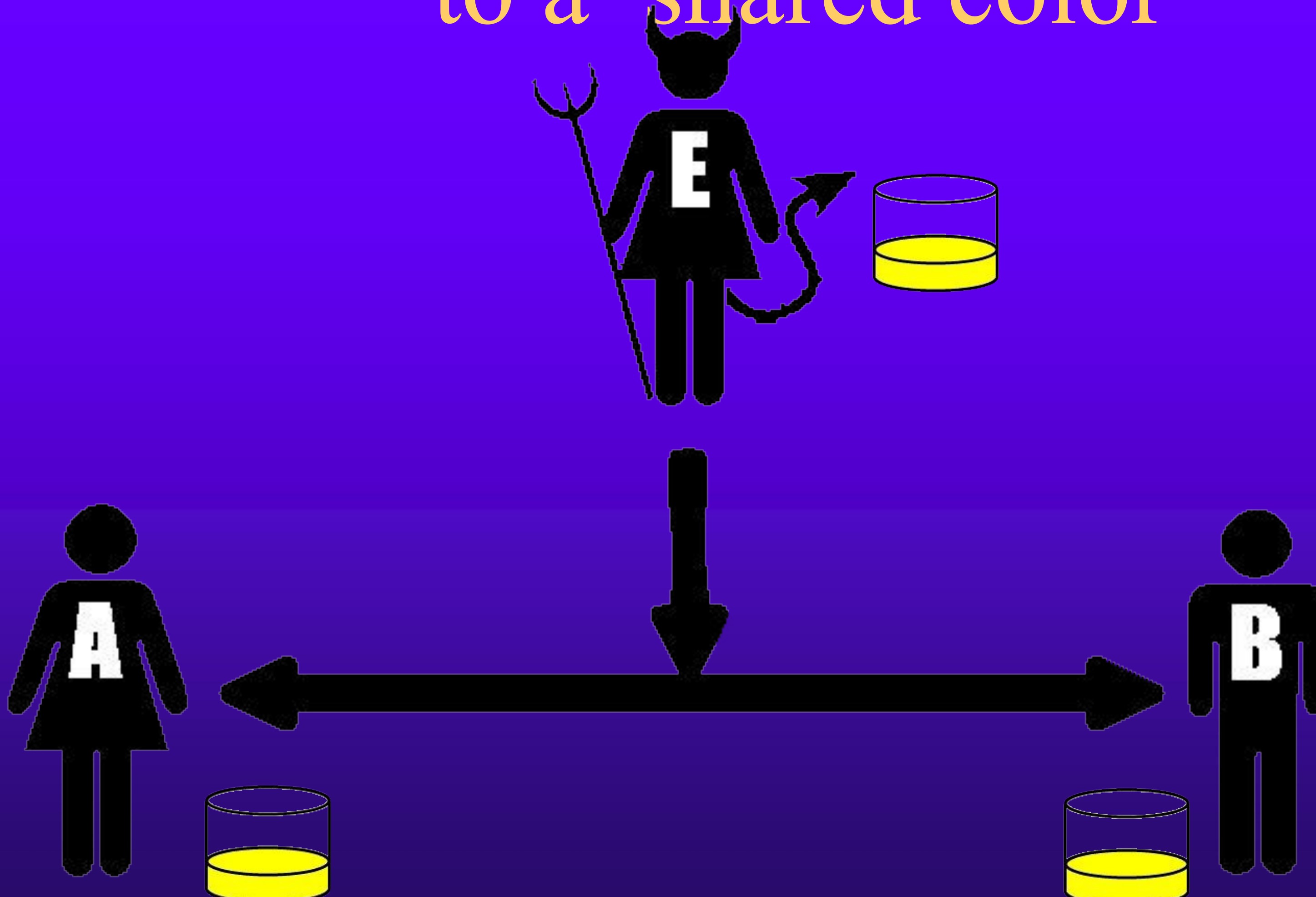
A Difficult One-Way Problem

- The first thing we require is a simple real-world operation that is easy to ***Do*** but hard to ***Undo***.
  - You can ring a bell but not unring one.
  - Toothpaste is easy to squeeze out of a tube but famously hard to put back in.
- In our example we will use *Mixing Colors*.

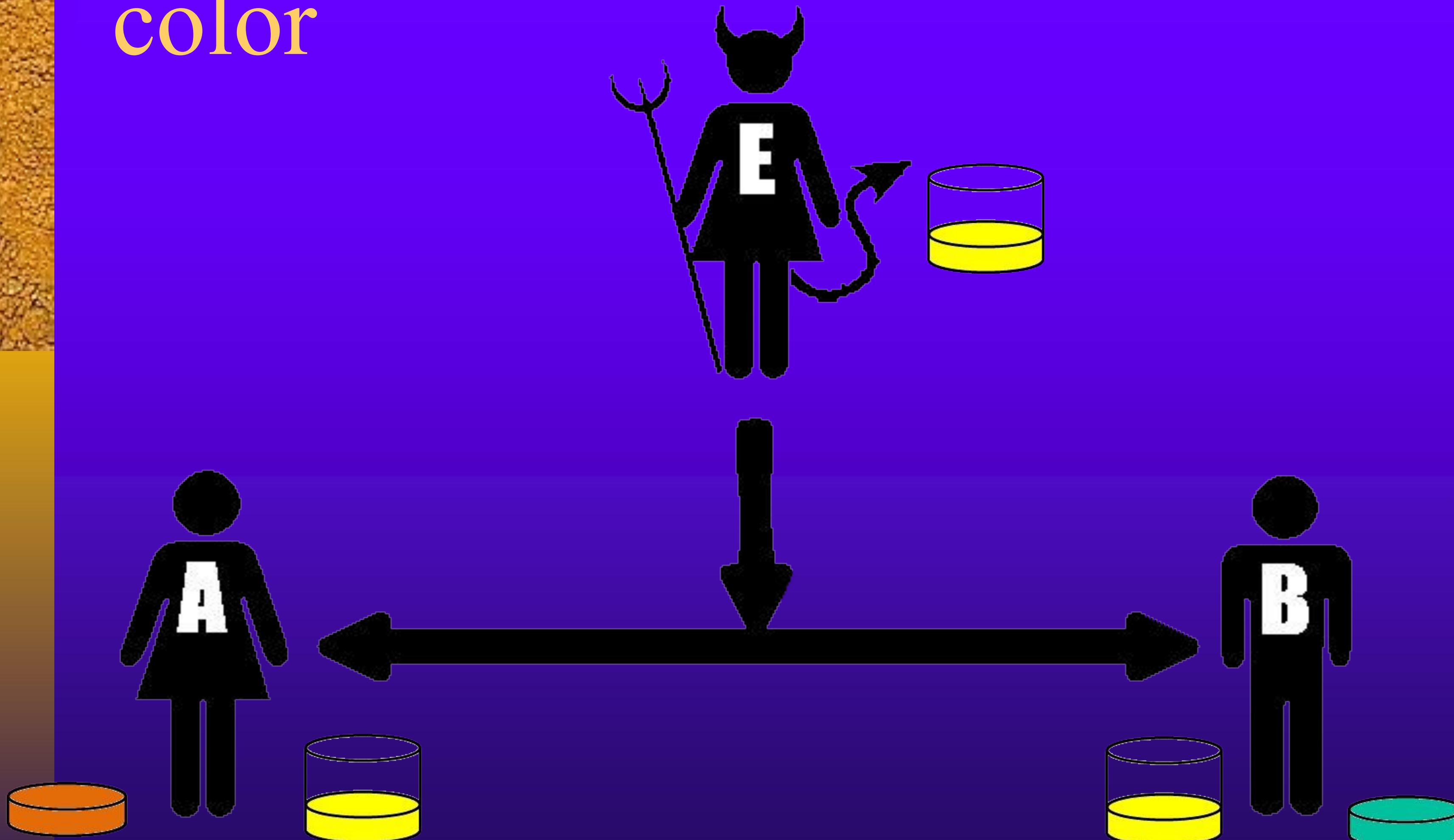
Alice & Bob with Eve listening wish to make a secret shared color



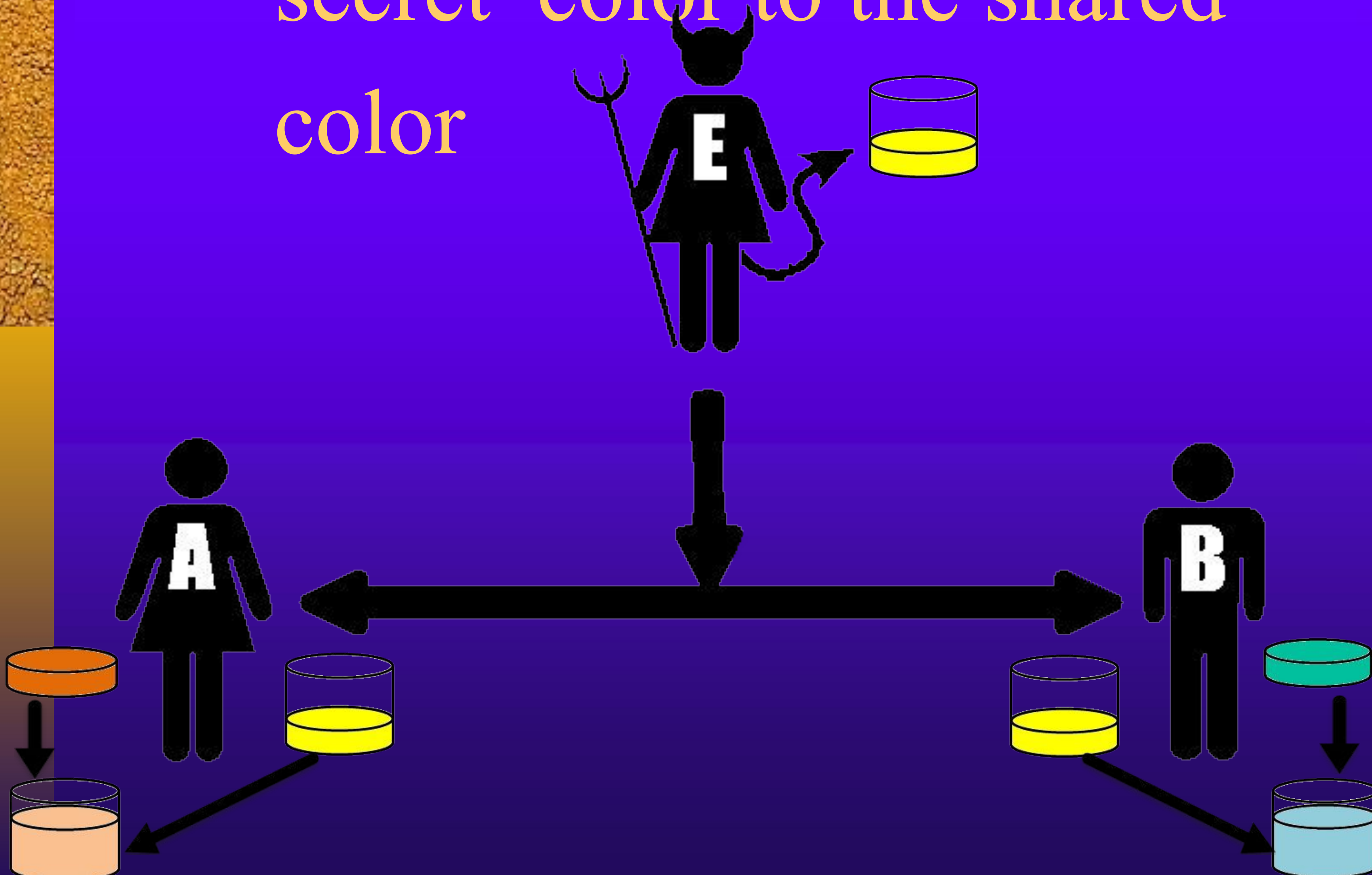
Step 1 - Both publicly agree to a shared color



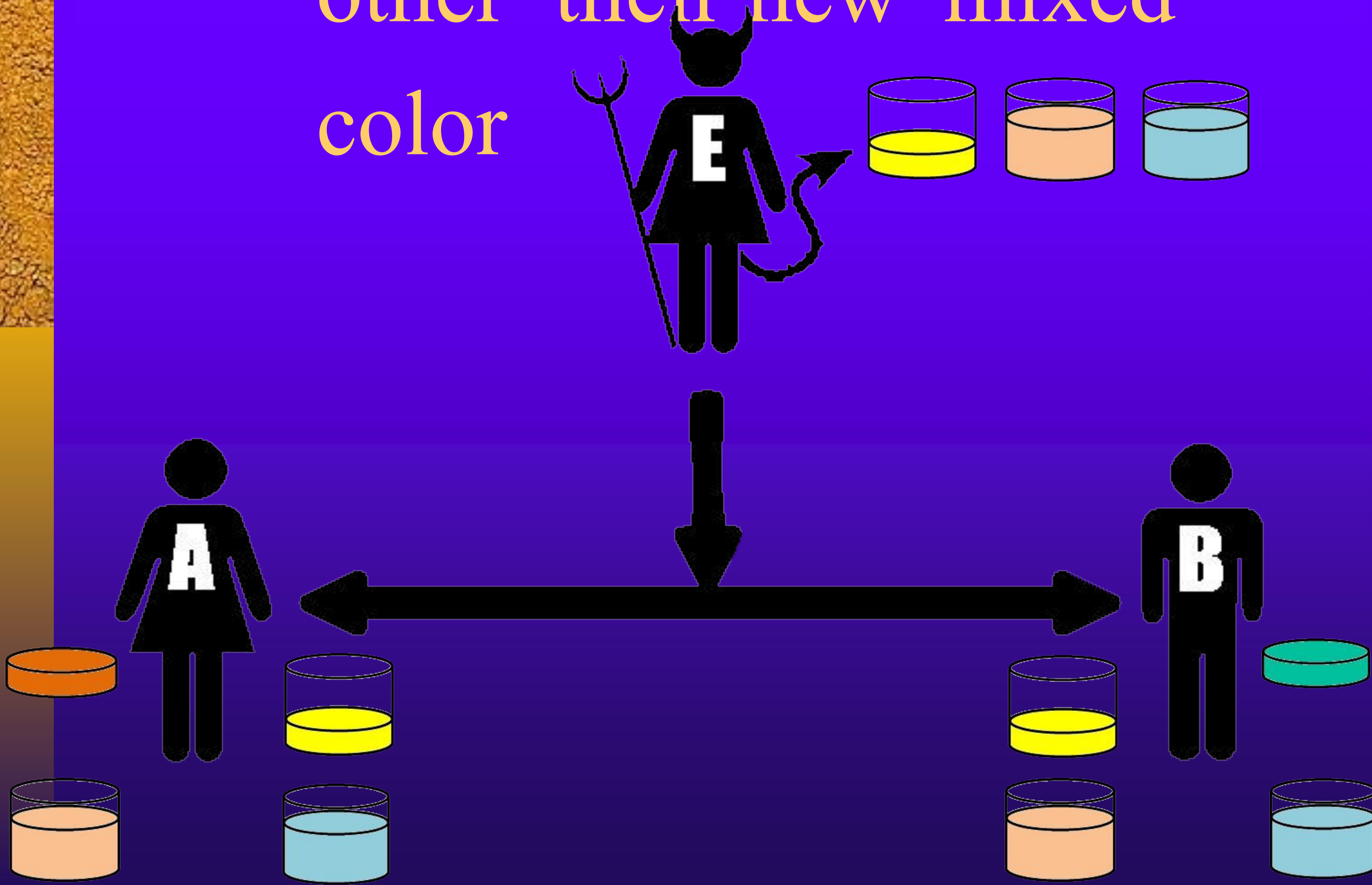
Step 2 - Each picks a secret color



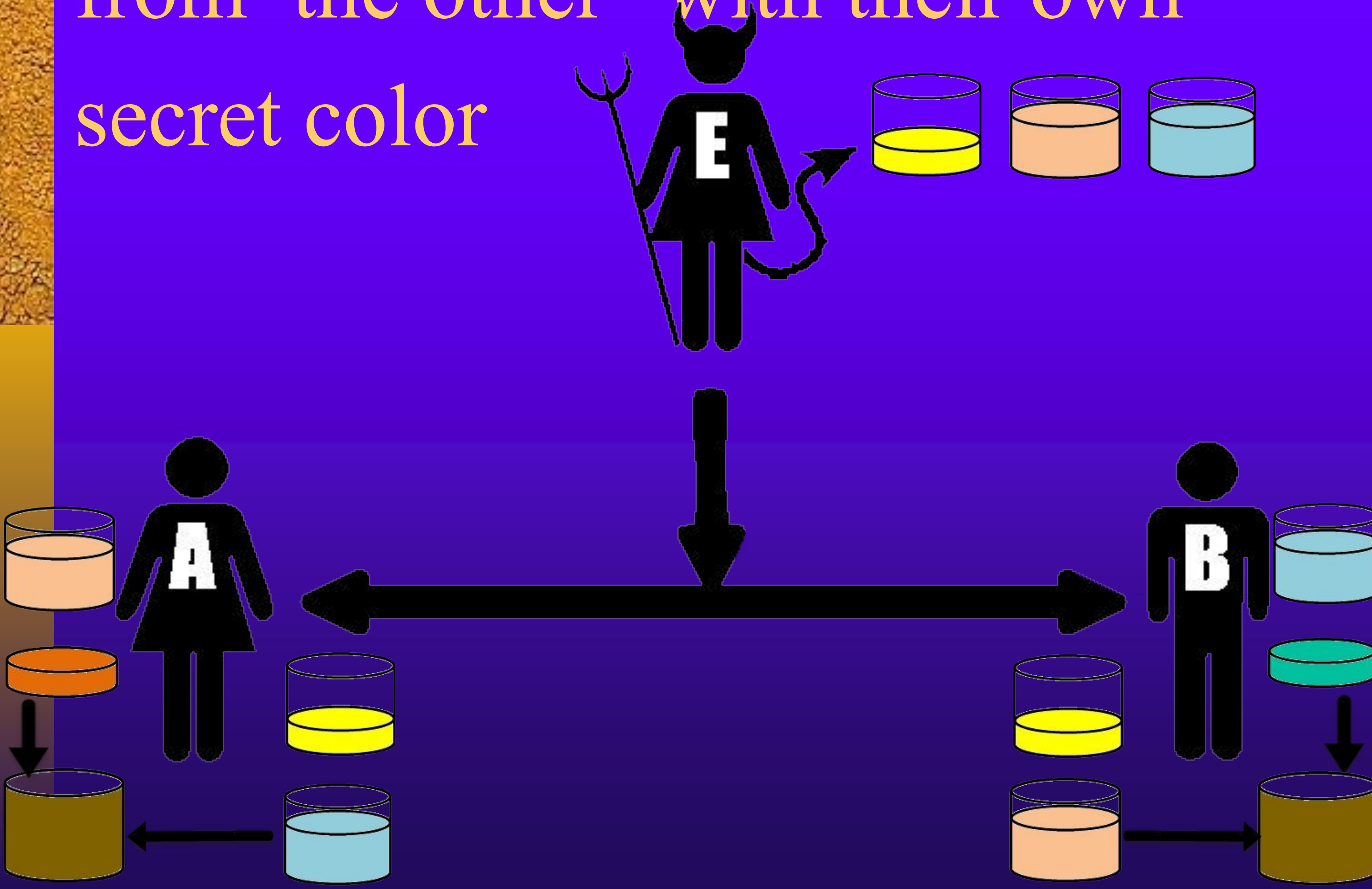
Step 3 - Each adds their secret color to the shared color



Step 4 - Each sends the other their new mixed color



Each combines the shared color from the other with their own secret color



Alice & Bob have agreed to a shared color unknown to Eve

- How is it that Alice & Bob's final mixtures are identical?

- Alice mixed
  - [(Yellow + Teal) from Bob] + Orange

- Bob mixed
  - [(Yellow + Orange) from Alice] + Teal

Alice & Bob have agreed to a shared color unknown to Eve

- How is it that Alice & Bob's final mixture is secret?
- Eve never has knowledge of the secret colors of either Alice or Bob
- Unmixing a color into its component colors is a hard problem

Alice & Bob have agreed to a shared color unknown to Eve

- How is it that Alice & Bob's final mixture is secret?
- Eve never has knowledge of the secret colors of either Alice or Bob
- Unmixing a color into its component colors is a hard problem

Diffie-Hellman Key Exchange Adding Mathematics

Rick Stroud

21 September 2015

CSCE 522

Let's get back to math

- We will rely on the formula below being an easy problem one direction and hard in reverse.
- $s = g^n \bmod p$
  - Easy: given g, n, & p, solve for s
  - Hard: given s, g, & p, solve for n
- And the property of
  - $g^{a*b} \bmod p = g^{b*a} \bmod p$

Step 1 –Publicly shared information

- Alice & Bob publicly agree to a large prime number called the modulus, or p.
- Alice & Bob publicly agree to a number called the generator, or g, which has a primitive root relationship with p.
- In our example we'll assume
  - $p = 17$
  - $g = 3$
- Eve is aware of the values of p or g.

Step 2 – Select a secret key

- Alice selects a secret key, which we will call *a*.
- Bob selects a secret key, which we will call *b*.
- For our example assume:
  - $a = 54$
  - $b = 24$
- Eve is unaware of the values of *a* or *b*.

Step 3 – Combine secret keys with public information

- Alice combines her secret key of *a* with the public information to compute *A*.
  - $A = g^a \bmod p$
  - $A = 3^{54} \bmod 17$
  - $A = 15$

Step 3 – Combine secret key with public information

- Bob combines his secret key of *b* with the public information to compute *B*.
  - $B = g^b \bmod p$
  - $B = 3^{54} \bmod 17$
  - $B = 16$

Step 4 – Share combined values

- Alice shares her combined value, *A*, with Bob. Bob shares his combined value, *B*, with Alice.
- Sent to Bob
  - $A = 15$
- Sent to Alice
  - $B = 16$
- Eve is privy to this exchange and knows the values of *A* and *B*

Step 5 – Compute Shared Key

- Alice computes the shared key.
  - $s = (B \bmod p)^a \bmod p$
  - $s = g^{b*a} \bmod p$
  - $s = 3^{54*24} \bmod 17$
  - $s = 1$
- Bob computes the shared key.
  - $s = (A \bmod p)^a \bmod p$
  - $s = g^{a*b} \bmod p$
  - $s = 3^{24*54} \bmod 17$
  - $s = 1$

Alice & Bob have a shared encryption key, unknown to Eve

- Alice & Bob have created a shared secret key, s, unknown to Eve
- In our example s=1
- The shared secret key can now be used to encrypt & decrypt messages by both parties.
- See the Youtube video on this example at:

  https://www.youtube.com/watch?v=3QnD2c4Xovk