Key Distribution Using Diffie-Hellman

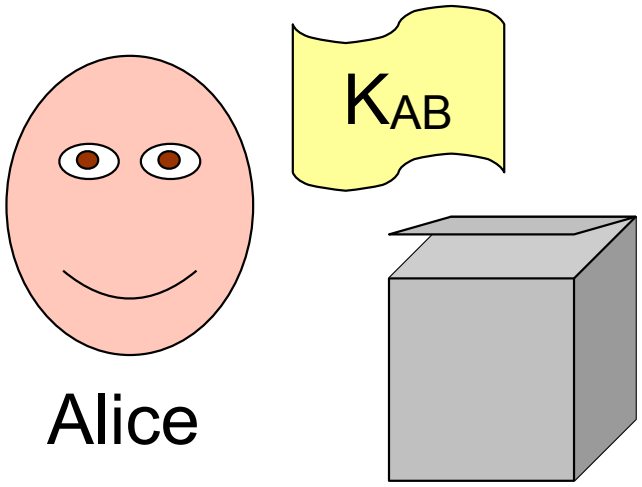
Yan Huang

Credit: David Evans (UVA)

Key Distribution

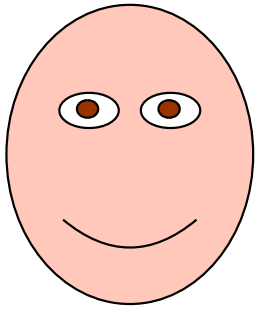
- All the cryptosystems we have seen depend on two parties having a shared secret
- Distributing secret keys is hard and expensive
  - $O(n^2)$ keys needed for n communicating parties
- Can two people communicate securely without having to meet first and establish a key?

Padlocked Boxes



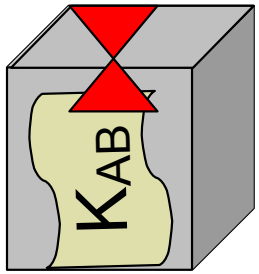
Padlocked Boxes

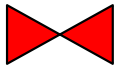
$E_A(M)$



Alice

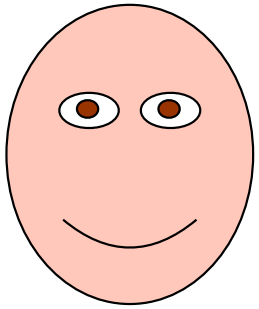
Alice's Padlock



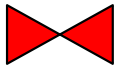


Alice's Padlock Key

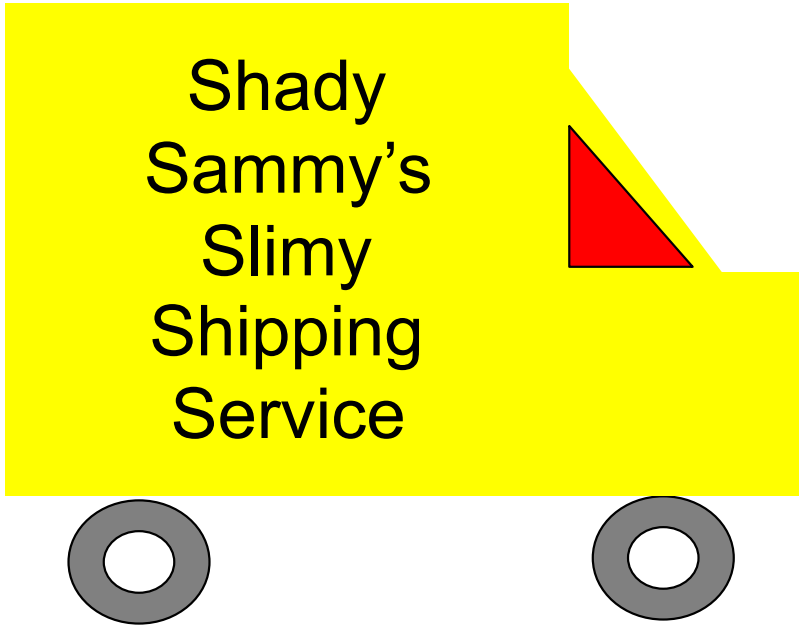
Padlocked Boxes



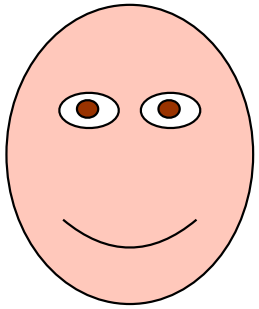
Alice



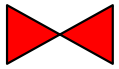
Alice's Padlock Key



Padlocked Boxes



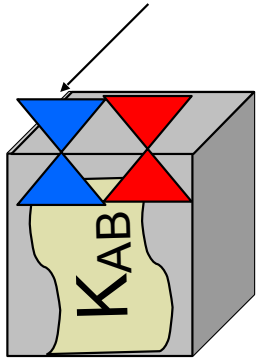
Alice

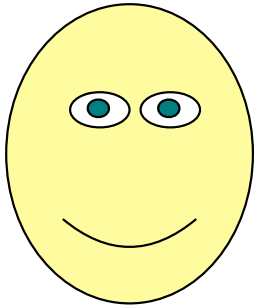


Alice's Padlock Key

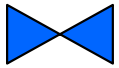
$E_B(E_A(M))$

Bob's Padlock





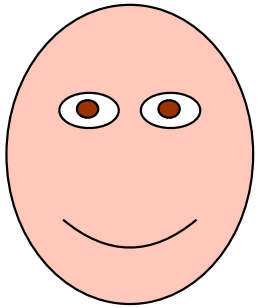
Bob



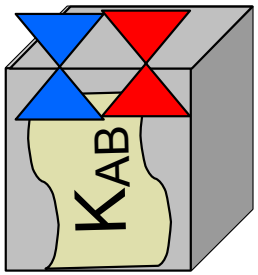
Bob's Padlock Key

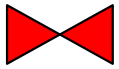
Padlocked Boxes

$E_B(E_A(M))$

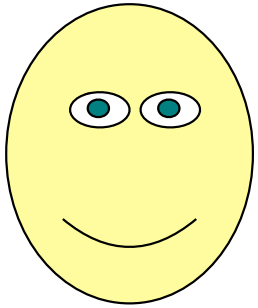


Alice

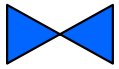




Alice's Padlock Key



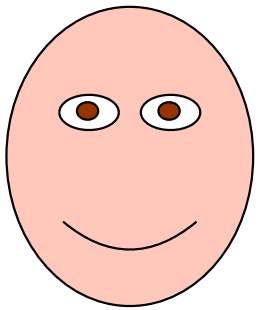
Bob



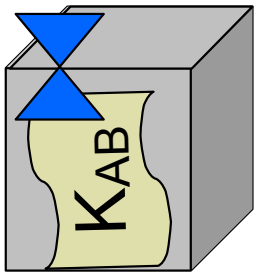
Bob's Padlock Key

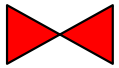
Padlocked Boxes

$$D_A(E_B(E_A(M))) = E_B(M)$$

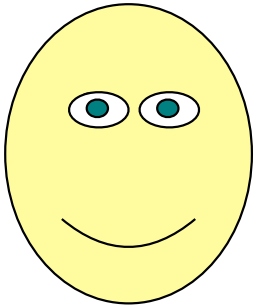


Alice

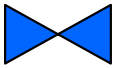




Alice's Padlock Key

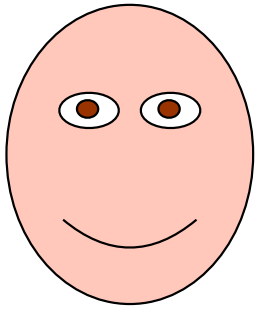


Bob



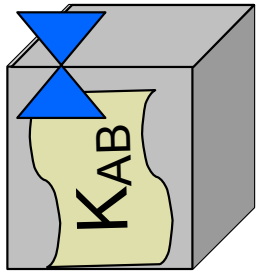
Bob's Padlock Key

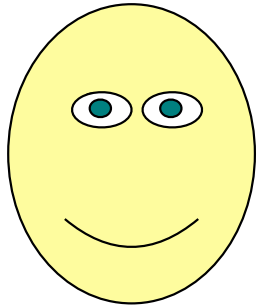
Padlocked Boxes



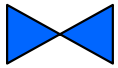
Alice

$E_B(M)$



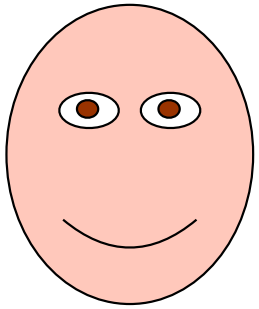


Bob

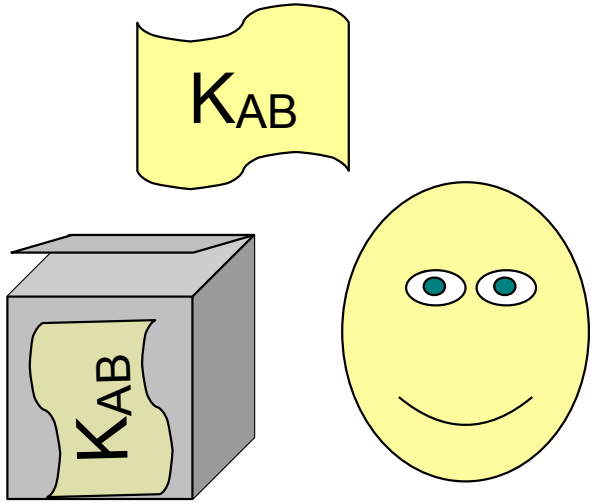


Bob's Padlock Key

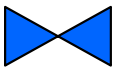
Padlocked Boxes



Alice



Bob

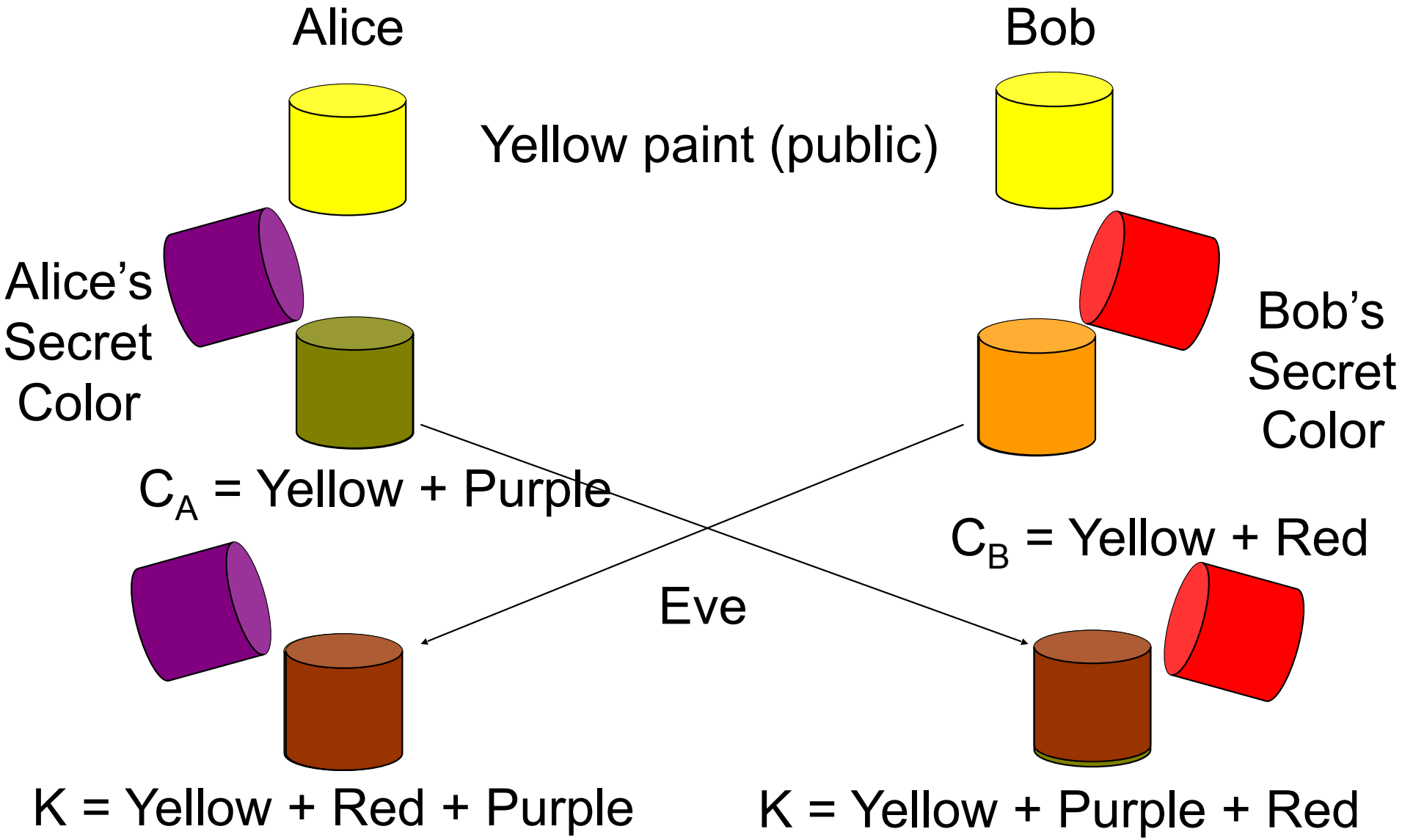


Bob's Padlock Key

Whitfield **Diffie** and Martin E. **Hellman**, the recipients of the 2015 ACM A.M. Turing Award, for critical contributions to modern cryptography. The ability for two parties to communicate privately over a secure channel is fundamental for billions of people around the world.

Analogy due to Simon Singh, *The Code Book*.

Secret Paint Mixing



Diffie-Hellman Key Agreement

1. Choose public numbers: q (large prime number), α (*primitive root* of q)
2. A generates random X_A and sends B:

$$Y_A = \alpha^{X_A} \bmod q.$$

3. B generates random X_B and sends A:

$$Y_B = \alpha^{X_B} \bmod q.$$

4. A calculates secret key: $K = (Y_B)^{X_A} \bmod q.$
5. B calculates secret key: $K = (Y_A)^{X_B} \bmod q.$

What's a primitive root?

- α is a primitive root of q if

$$\left|\{\alpha^m \bmod q \mid 1 \leq m < q\}\right| = q - 1$$

- Given α, $(\alpha^m \bmod q)$ and q can we solve for m?
  - Yes: there is only one possible m
  - But, it might be very hard for large q
- Discrete logarithm: given α, $(\alpha^m \bmod q)$, and q find m $(0 \leq m < q)$.

Example

What is a primitive root for $q = 11$?

$2^1 \equiv_{11} 2$

$2^2 \equiv_{11} 4$

$2^3 \equiv_{11} 8$

$2^4 = 16 \equiv_{11} 5$

$2^5 = 32 \equiv_{11} 10$

$2^6 = 64 \equiv_{11} 9$

$2^7 = 128 \equiv_{11} 7$

$2^8 = 256 \equiv_{11} 3$

$2^9 = 512 \equiv_{11} 6$

$2^{10} = 1024 \equiv_{11} 1$

Diffie-Hellman Example

1. Choose public numbers: q (large prime number), α(generator mod q):

   $q = 11,\ \alpha = 2$

2. A generates random X_A and sends B:

   $$Y_A = \alpha^{X_A} \bmod q.$$

   $$X_A = 4,\ Y_A = 2^4 \bmod 11 = 16 \bmod 11 = 5$$

3. B generates random X_B and sends A:

   $$Y_B = \alpha^{X_B} \bmod q.$$

   $$X_B = 6,\ Y_B = 2^6 \bmod 11 = 64 \bmod 11 = 9$$

Example from Tom Dunigan's notes: http://www.cs.utk.edu/~dunigan/cs594-cns00/class14.html

Diffie-Hellman Example, cont.

$q = 11,\ \alpha = 2$

$X_A = 4, Y_A = 5 \quad X_B = 6, Y_B = 9$

4. A calculates secret key: $K = (Y_B)^{X_A} \bmod q$.

$K = 9^4 \bmod 11 = 6561 \bmod 11 = 5.$

5. B calculates secret key: $K = (Y_A)^{X_B} \bmod q$.

$K = 5^6 \bmod 11 = 15625 \bmod 11 = 5.$

Is it magic? Things to Prove:

1. **Correctness** — They generate the same keys:

$$K = (Y_B)^{X_A} \bmod q = (Y_A)^{X_B} \bmod q$$

2. **Security** — An eavesdropper cannot know anything about the shared key from the transmitted values:

$$q,\ \alpha,\ Y_A,\ Y_B$$

Correctness

- Prove $K = (Y_B)^{X_A} \bmod q = (Y_A)^{X_B} \bmod q$.

$$(Y_B)^{X_A} \bmod q \qquad (Y_A)^{X_B} \bmod q$$

$$= (\alpha^{X_B} \bmod q)^{X_A} \bmod q \qquad = (\alpha^{X_A} \bmod q)^{X_B} \bmod q$$

$$= (\alpha^{X_B})^{X_A} \bmod q \qquad = (\alpha^{X_A})^{X_B} \bmod q$$

$$= \alpha^{X_B X_A} \bmod q \qquad = \alpha^{X_A X_B} \bmod q$$

QED.

Modular Exponentiation

- First prove:

  $(a * b) \bmod q = (a \bmod q) * (b \bmod q) \bmod q$

- Then, by induction,

  $(a \bmod q)^b \bmod q = a^b \bmod q$

  since $a^b = a * a^{b-1}$ and $a^1 = a$.

Modular Arithmetic

$(a * b) \bmod n = x$

$x + (n * d0) = a * b$

$x = a * b - (n * d0)$

$a \bmod n = y \Rightarrow y = a - (n * d1)$

$b \bmod n = z \Rightarrow z = b - (n * d2)$

$(a \bmod n) * (b \bmod n) \bmod n$

$= (a - (n * d1)) * (b - (n * d2)) \bmod n$

$= (a * b + (a * (n * d2)$

$- b * (n * d1) + (n * d1)(n * d2)) \bmod n$

$= a * b \bmod n$ (all terms with $n *$ are $0 \bmod n$)

Security

- An eavesdropper knows

  q, α, $Y_A = \alpha^{X_A}$, $Y_B = \alpha^{X_B}$

  but cannot find

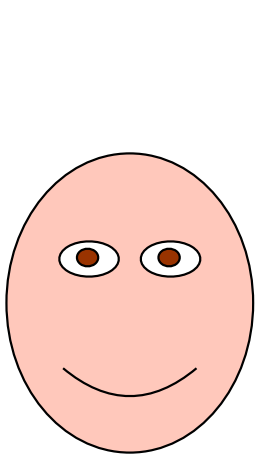
  $$K = (Y_B)^{X_A} \bmod q = (Y_A)^{X_B} \bmod q$$

- Decisional Diffie-Hellman (DDH) assumption:
  $(q, \alpha, \alpha^{X_A}, \alpha^{X_B}, \alpha^{X_A \cdot X_B}) \approx (q, \alpha, \alpha^{X_A}, \alpha^{X_B}, h)$
  where h is uniformly randomly sampled from

  $\{\alpha^x \mid x$ is any positive integers$\}$

- DDH is (probably) hard!

Secure from Active Eavesdropper?

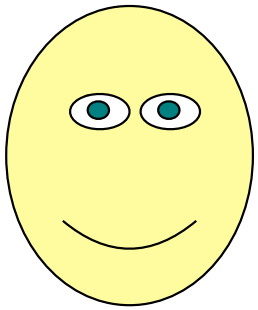


Alice

Secret: X_A

Public: q, α

$Y_A = \alpha^{X_A} \bmod q$



Bob

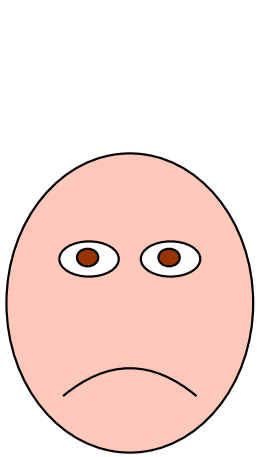
Secret: X_B

$Y_B = \alpha^{X_B} \bmod q$

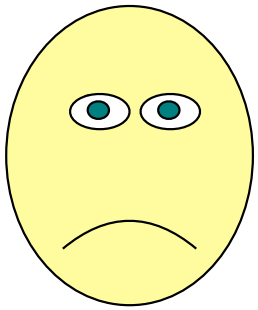
$K = (Y_B)^{X_A} \bmod q$

$K = (Y_A)^{X_B} \bmod q$

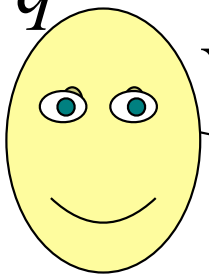
Secure from Active Eavesdropper?



Alice



Bob



Public: q, α

$Y_A = \alpha^{X_A} \bmod q$

$Y_E = \alpha^{X_E} \bmod q$

$Y_E = \alpha^{X_E} \bmod q$

Secret: X_B

Secret: X_A

$K_{AE} = (Y_E)^{X_A} \bmod q$

$Y_B = \alpha^{X_B} \bmod q$

$K_{EB} = (Y_E)^{X_B} \bmod q$

Secret: X_E

Diffie-Hellman Use

- SSL
- Cisco encrypting routers
- Sun secure RPC
- etc...

Does D-H solve all problems?

- Only key agreement
- Cannot do:
  - Authentication
  - Signatures