Fundamentals of Information & Network Security
ECE 471/571

Lecture #20: Diffie-Hellman Key Agreement

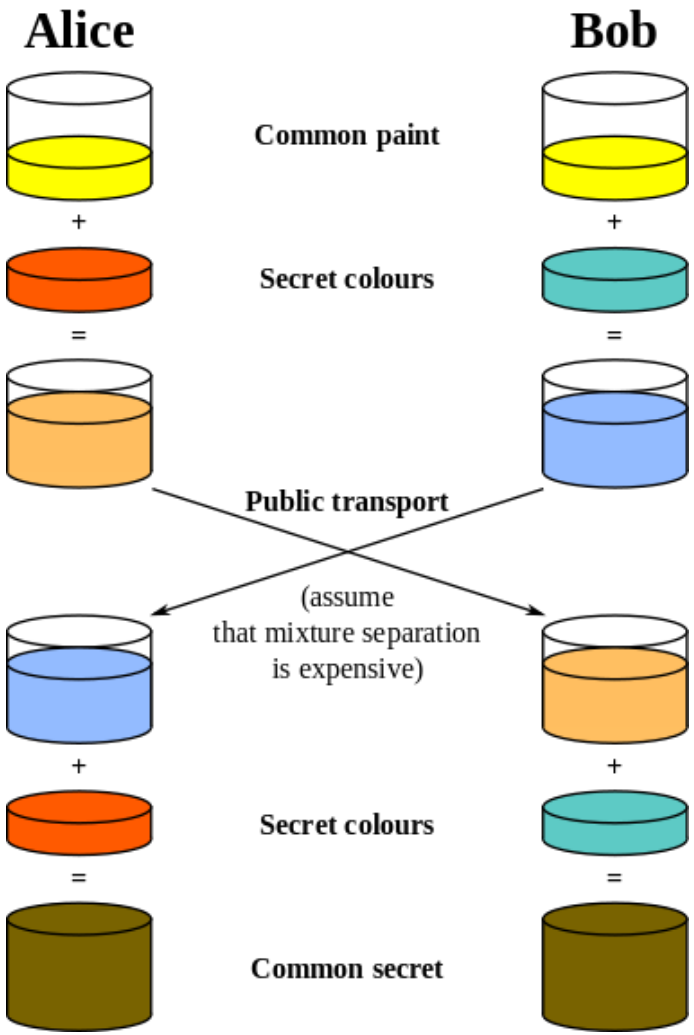
Instructor: Ming Li
Dept of Electrical and Computer Engineering
University of Arizona

Diffie-Hellman Key Exchange/Agreement

- First public-key cryptographic algorithm
  - Diffie & Hellman, "*New directions in Cryptography*", IEEE Trans. on IT. ,Vol. 22, pp. 644-654, Nov., 1976.

- To establish a shared secret number between two parties using a public communication channel.

Intuition: Exchange of Colors



Source: Wikipedia

Diffie-Hellman Key Exchange

Global Public Elements

q	prime number
α	$\alpha < q$ *and* α a primitive root of q

User A Key Generation

Select private X_A	$X_A < q$
Calculate public Y_A	$Y_A = \alpha^{X_A} \bmod q$

User B Key Generation

Select private X_B	$X_B < q$
Calculate public Y_B	$Y_B = \alpha^{X_B} \bmod q$

Calculation of Secret Key by User A

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

Calculation of Secret Key by User B

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

Example

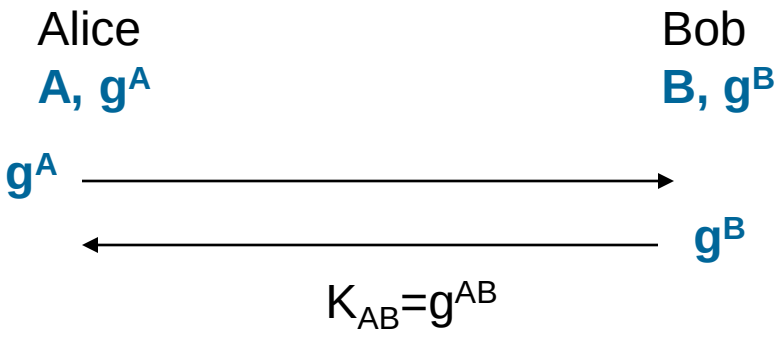
- Alice and Bob agree to use a modulus p = 23 and base g = 5 (which is a primitive element modulo 23).
- Alice chooses a secret integer $\boldsymbol{a} = \mathbf{6}$, then sends Bob $A = g^a \bmod p$
  - $A = 5^{\mathbf{6}} \bmod 23 = 8$
- Bob chooses a secret integer $\boldsymbol{b} = \mathbf{15}$, then sends Alice $B = g^b \bmod p$
  - $B = 5^{\mathbf{15}} \bmod 23 = 19$
- Alice computes $\boldsymbol{s} = B^a \bmod p$
  - $\boldsymbol{s} = 19^{\mathbf{6}} \bmod 23 = \mathbf{2}$
- Bob computes $\boldsymbol{s} = A^b \bmod p$
  - $\boldsymbol{s} = 8^{\mathbf{15}} \bmod 23 = \mathbf{2}$
- Alice and Bob now share a secret (the number **2**).

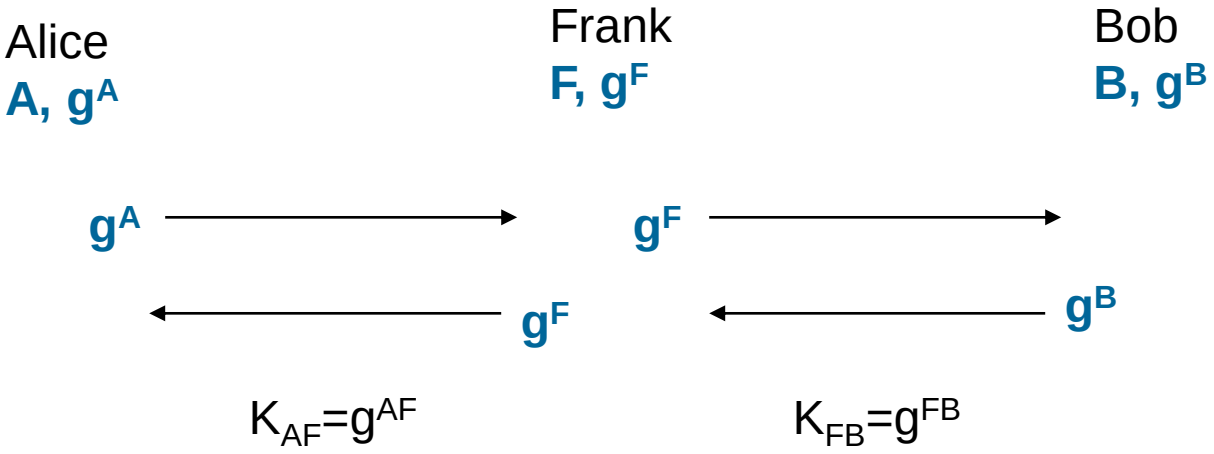
Why Diffie-Hellman is secure?

- It is difficult to compute discrete logarithm.
  - Knowing g^{S_A}, it is difficult to compute S_A.

- Safe Prime
  - 2p+1, p is also prime

Man-in-the-Middle Attack





Countermeasures

- Publish public numbers
- Authenticated Diffie-Hellman

Authenticated key agreement

Publish public numbers

- Agrees on a common p and g
- keeps S private, but publishes $T=g^S \bmod p$ through a reliable, trusted service such as PKI.
- retrieves T from the trusted service.
- No place for Frank to get in the middle. The key between Alice and Bob is in fact pre-determined.

This is key pre-distribution!

Authenticated Diffie-Hellman

- Encrypt the Diffie-Hellman exchange with the *pre-shared secret*
- Encrypt the Diffie-Hellman public number with the other side's *public key*
- Sign the Diffie-Hellman public number with your *private key*

Other solutions?

- Following the Diffie-Hellman exchange, transmit a hash of the agreed key and the *pre-shared secret*
- Following the Diffie-Hellman exchange, transmit a hash of the *pre-shared secret* and your public number
- ……

Encryption with Diffie-Hellman

- After the shared secret key is established, it can be used as the encryption key.