Diffie-Hellman Key Exchange

* Code Book Version of This Story

Alice $\rightarrow$ Bob

Eve $\leftarrow$

Proven that one-way functions do exist. (easy to calculate forward, hard to invert)

$$\text{Red} \uparrow + \text{Blue} \downarrow \Rightarrow \text{Purple}$$

In any public key scheme, there must be

1. Some public info (accessible to all)

2. Some private info
   - Alice's private key (only Alice knows)
   - Bob's private key (only known to Bob)
   - Each other's private key!

Public info can't compromise either private key AND

Messages sent between Alice + Bob can't compromise either private key.
Eve knows $g^A \equiv \mod p$

$p^A \cdot p^B \equiv g^A \cdot g^B \equiv g^{A+B} \mod p$

$(p^A)^{p^B} = (g^A)^{g^B} = g^{A \cdot g^B} \neq g$

$p = 13$

$(g = 2)$

$2^6 = 64 \equiv -1 \mod 13$

$2^3 = 8 \equiv 1 \mod 13$

$2^4 = 16 \equiv 1 \mod 13$

$A = 5$, $B = 7$

Alice → Bob $2^5 = 32 \equiv 6 \mod 13$

Alice ← Bob $2^7 = 128 \equiv 11 \mod 13$

Alice computes $1^5 \equiv (-2)^5 = -32 \equiv -6 \equiv 7 \mod 13$

Bob computes $6^7 \equiv (36)^3 \cdot 6 \equiv (-3)^3 \cdot 6 = -27 \cdot 6 = -6 \equiv 7$
Public Keys

$p$: large prime  $g$: generator for that prime!

Private Keys

$A_e = Alice's$ Exp  $0 < A_e < p$  
$B_e = Bob's$ Exp  $0 < B_e < p$

Alice sends $g^{A_e} \mod p$ to Bob

Alice sends $g^{B_e} \mod p$ to Bob

Discrete Log problem (Given these Eve can't figure out $A_e$ because Discrete Log is hard!)

Then, Alice calculates

$(PUB)^{A_e} \mod p$

Bob calculates $(PUB)^{B_e} \mod p$

$(PUB)^{A_e} = (g^{B_e})^{A_e} = g^{A_eB_e} \mod p$

$(PUB)^{B_e} = (g^{A_e})^{B_e} = g^{A_eB_e} \mod p$

This is the shared key.