Diffie-Hellman Protocol (any group)

Precomp.

a. G, $|G| = n$

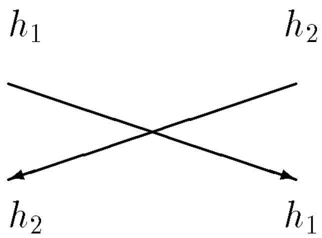
b. $g \in G$

A

1. secretly generates $a < n$
2. computes $h_1 = a \cdot g$
3. transmits h_1 to **B**

B

1. secretly generates $b < n$
2. computes $h_2 = b \cdot g$
3. transmits h_2 to **A**



A

4. computes k by

$$k = a \cdot h_2 = a \cdot bg$$

B

4. computes k by

$$k = b \cdot h_1 = b \cdot ag$$

Common Key: the group element $k = abg \in G$

Key Space: the subgroup generated by g

Eavesdropper: knows h_1, h_2, g; but **not** a, b or k.

DHP: given h_1, h_2, g; find $k = abg$

DLP: given some g, and let $h = ag$;
find $a = \mathrm{ind}_g(h)$.