Diffie-Hellman key exchange

- If Alice and Bob can independently calculate the secret key s, so can an attacker who knows p, g, A, and B, right? — Not so easily

- If a, b, and p are large numbers, it's mathematically difficult to calculate a and b from p, g, A, and B only