

CSCI 3330: Diffie-Hellman by Hand

Do all computations by hand!

1 Constants

Suppose you have chosen modulus $p = 7$ and base $g = 3$.

2 Picking secrets

1. Person on the left: pick a secret a such that $1 \leq a < 6$.
2. Person on the right: pick a secret b such that $1 \leq b < 6$.

Try not to let each other know your secrets!

3 Sharing material

1. Person on the left: compute $A = g^a \% p$ and share this with the person on the right.
2. Person on the right should compute $B = g^b \% p$ and share this with the person on the left.

4 Computing shared secret

1. Person on the left: call what you received B . Compute $S = B^a \% p$.
2. Person on the right: call what you received A . Compute $S = A^b \% p$.

S is your shared secret. If you performed your computations accurately, you both should have arrived at the same S , despite only sharing with each other $g^a \% p$ and $g^b \% p$, which are not enough for an eavesdropper to reconstruct S .