Diffie-Hellman key protocol example

January 22, 2024

This is all public information:

$$p = 37 \tag{1}$$
$$\mathbb{Z}_p \tag{2}$$
$$\overline{g} = \overline{3} \tag{3}$$

Person A:

$$\overline{a} = \overline{51} \tag{4}$$
$$\overline{A} = \overline{g}^a \tag{5}$$

Person A now shares A with Person B and keeps a private.

Person B:

$$\overline{b} = \overline{14} \tag{6}$$
$$\overline{B} = \overline{g}^b \tag{7}$$

Person B now shares B with person A and keeps b private.

Person A:

$$\overline{key} = \overline{B}^a \tag{8}$$

Person B:

$$\overline{key} = \overline{A}^b \tag{9}$$