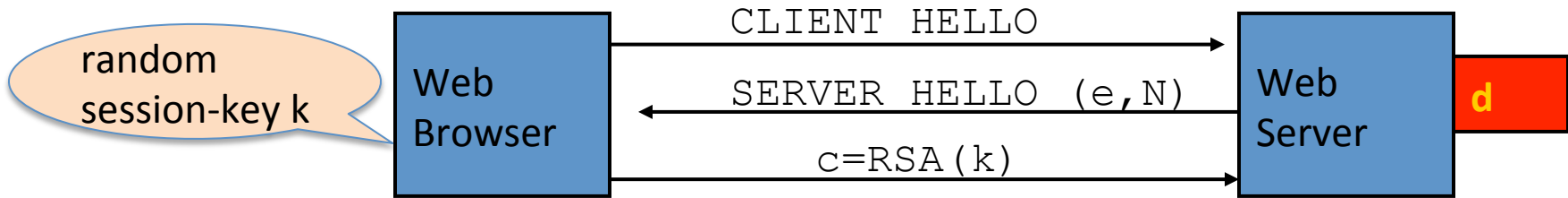


# A simple attack on textbook RSA



Suppose  $k$  is 64 bits:  $k \in \{0, \dots, 2^{64}\}$ . Eve sees:  $c = k^e$  in  $Z_N$

If  $k = k_1 \cdot k_2$  where  $k_1, k_2 < 2^{34}$  (prob.  $\approx 20\%$ ) then  $c/k_1^e = k_2^e$  in  $Z_N$

Step 1: build table:  $c/1^e, c/2^e, c/3^e, \dots, c/2^{34e}$ . time:  $2^{34}$

Step 2: for  $k_2 = 0, \dots, 2^{34}$  test if  $k_2^e$  is in table. time:  $2^{34}$

Output matching  $(k_1, k_2)$ .

Total attack time:  $\approx 2^{40} \ll 2^{64}$