Diffie Hellman

Alice Eve Bob

$\xrightarrow{17,61}$ $\xrightarrow{17,61}$

$b_1 = 3$ b_2

$B_1 = 17^3 \bmod 61$ $5 = 17^{b_2} \bmod 61$

$\xleftarrow{B_1 = 33}$ $\xleftarrow{B_2 = 5}$

a_1 $a_2 = 3$

$A_1 = 17^{a_1} \bmod 61$ $A_2 = 17^3 \bmod 61$

$\xrightarrow{A_1 = 46}$ $\xrightarrow{A_2 = 33}$

$K_1 = B_1^{a_1} \bmod p$ $K_1 = 46^3 \bmod 61$ $K_2 = 5^3 \bmod 61$ $K_2 = A_2^{b_2} \bmod p$

$= g^{a_1 b_1} \bmod p$ $= 41$ $= 3$ $= g^{a_2 b_2} \bmod p$

$41 = 17^{a_1 3} \bmod 61$ $9 = 17^{6 b_2} \bmod 61$

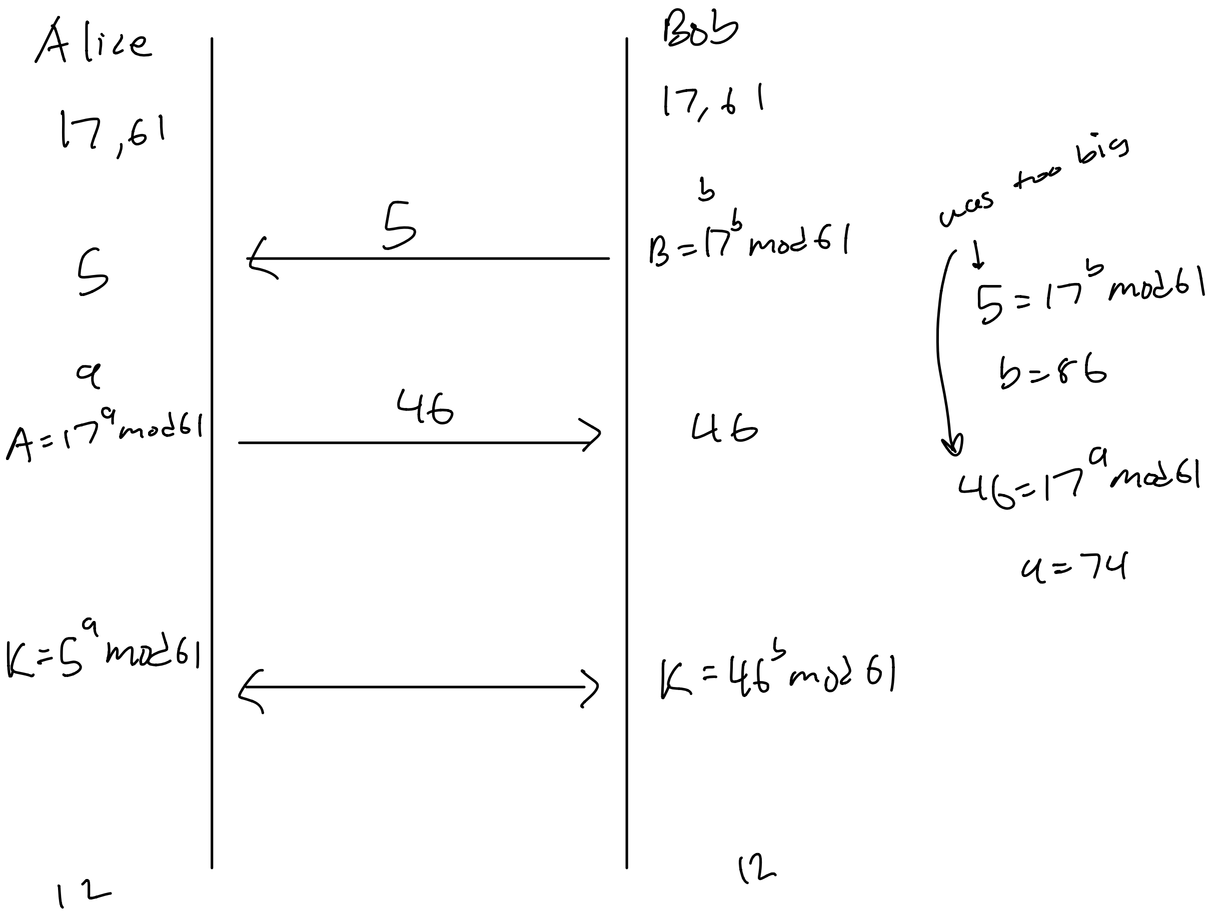
46

$5 = 17^b \bmod 61$ $x = 86$

$46 = 17^a \bmod 61$ $y = 74$

problem if 5, 46 is bigger

Diffie-Hellman



$K=12$

RSA

↙ if it was toobig

$p_B , q_B = 4661 = n_B$

↓ ↓

59×79

$e_B = 31$, find $d_B = 2335$

↓

one that's smaller than n_B

$31 d_B \bmod (58)(78) = 1$

Concert to ASCII → string