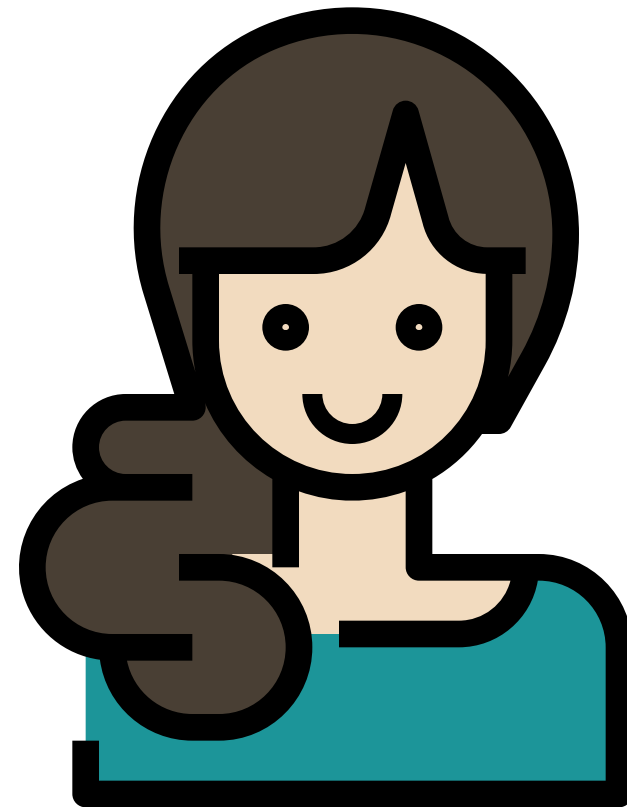
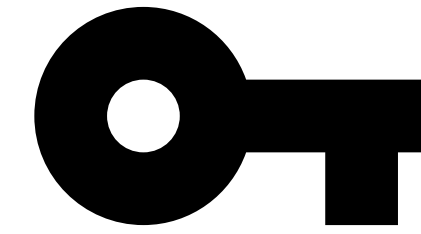
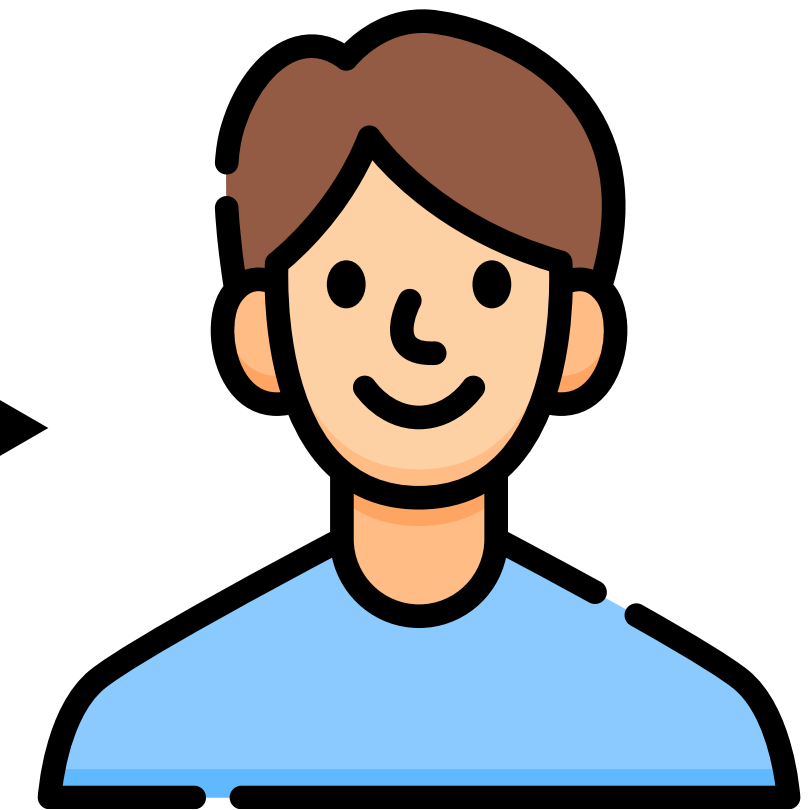


Alice



Bob



$e, N = P * Q$



P, Q, d, ϕ



$m = c^d \bmod N$



$C = m^e \bmod N$



m