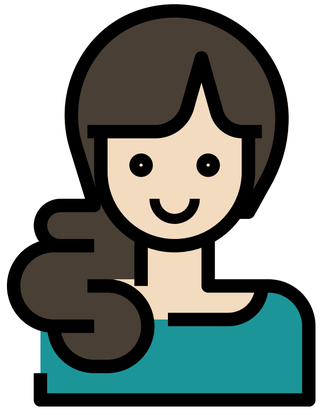
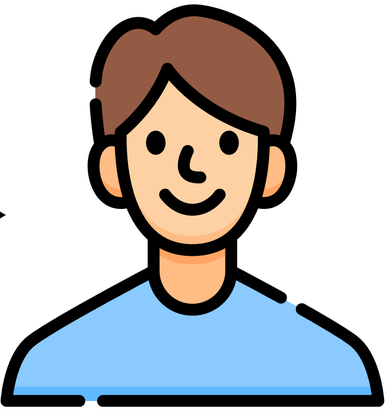
Alice



e, N = P * Q

Bob



P, Q, d, ϕ

m = c^d mod N

C = m^e mod N

m