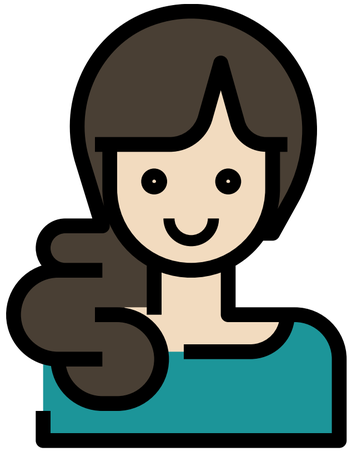
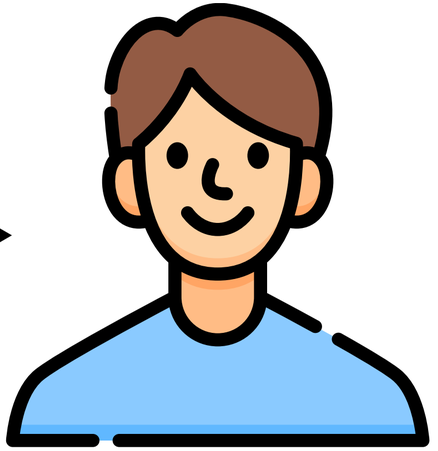
Alice

Bob



e, N = P * Q



C = m^e mod N

P, Q, d, ϕ

m = c^d mod N

m