Let F: K × {0,1}^{n} ⟶ {0,1}^{n} be a secure PRF.

E(k,m): choose a random IV ∈ {0,1}^{n} and do: