E = (E,D) cipher defined over (K,M,C). For b=0,1 define EXP(b): for i=1,...,q: Chal. Adv. (1) CPA query: k←K  $m_{i,0}$ ,  $m_{i,1} \in M$ :  $|m_{i,0}| = |m_{i,1}|$  $c_i \leftarrow E(k, \mathbf{m}_{i,b})$ 

