



- nonce n : a value that changes from msg to msg.
(k, n) pair never used more than once
- method 1: nonce is a **counter** (e.g. packet counter)
 - used when encryptor keeps state from msg to msg
 - if decryptor has same state, need not send nonce with CT
- method 2: encryptor chooses a **random nonce**, $n \leftarrow \mathcal{N}$