Preventing Key Reused Attacks

At best, use a fresh symmetric key every time

- Key exchange problem

At least, change the seed to never it use it twice

✓ All modern stream cipher (Salsa/Chacha) and good encryption mode for block cipher (CBC, CTR) take a nonce

➡ Generate this nonce randomly and sent it in clear with cyphertext

Are we secured?