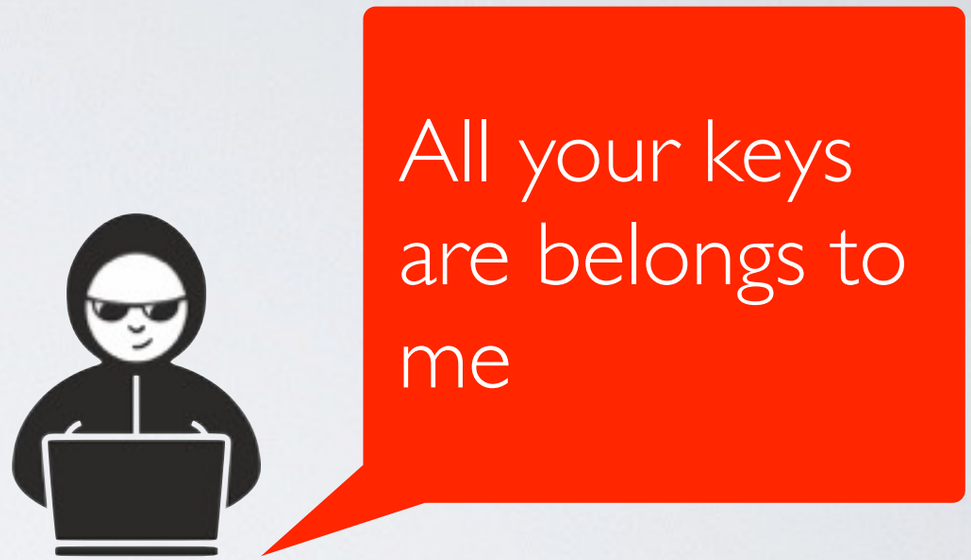
Threats to Cryptographic Keys



- Weak/Insecure generation
- Attack on transmission
- Unauthorized disclosure
- Loss

Weak / Insecure key generation

- The security of cryptographic algorithms rests in the key. Weak keys => Easy cryptanalysis on key space

- Sometimes, not using all keys in the key space may result in weakness

- Poor key choices e.g use of mutations of dictionary strings

- Weak/non-cryptographically safe randomization for key generation