# 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

# Attack on transmission

- ➡ No error detection during transmission. May lead to garbled or partially decrypted cipher text. Violation of availability

- ➡ Malicious key swap. Malicious keys used for encryption. Violation of confidentiality. Man-in-the-middle attacks