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

Unauthorized disclosure

- Improper storage of long-term keys e.g SSH private keys with weak access permissions, keys on disk unencrypted, keys in memory unencrypted
- Bribery; insider threat
- Improper destruction; key can be reconstructed
- Improper implementation; transmitting keys in plaintext