Weak / Insecure key generation

- Where applicable, all keys in the key space should be equally likely and provide the strong encryption

- Use cryptographically safe mechanisms to create random values when needed.

- Consider using cryptographically secure PRNGs to generate keys from an easy to remember but obscure (hard to guess) seed.

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

Attack on transmission

- Good key transmission algorithms include some form of error detection
- Nonces, certificate authorities and web of Trust can be leveraged to ensure integrity and ownership of transmitted keys