

# Common implementation pitfalls

- ➡ DO NOT re-invent the wheel “Roll your own cryptography”
- ➡ USE well maintained cryptography libraries and adhere to any and all documentation warnings
- ➡ DO NOT use known weak/broken cryptographic algorithms
- ➡ USE cryptographically secure randomness for the generation of nonces, IV etc
- ➡ DO NOT re-use nonces, IV etc. Cryptographic algorithms rely on some principles to be effective. DO NOT compromise the principles
- ➡ DO NOT hard-code cryptographic keys
- ➡ ENSURE the encryption strength in use is sufficient for the data protected
- ➡ Exercise caution when using time as a variable for cryptographic computation

