MOST IMPORTANT ADVICE:
GET AN EXPERT OR AT LEAST
READ AND UNDERSTAND THE DOCUMENTATION!

Like all power tools: Better RTFM than to lose an eye!

- At least be able to explain: “Hash vs. encryption”, “Integrity vs. encryption”, “Stream vs. block”, “Mode of operation”, “IV”, “Nonce”, “Padding”, “Key derivation”
- Identify and name your trust anchors

SOME WORDS THAT I MIGHT DROP AND THEN FORGET TO EXPLAIN

- **Cleartext**: What you can read. Not encrypted
- **Chiphertext**: Encrypted cleartext.
- **Hash**: Calculated from a text. Always the same length, regardless of the length of the text. Assumption: H(A) = H(B) => A = B
- **Key length**: length of the key/secret. E.g. “128 bits” for AES_128
- **Symmetric key length equivalence**: Asymmetric keys are much longer (e.g. RSA 3072) but scale differently. RSA3072 is ~128bit “symmetric key length”, RSA2048 is 112bits
- Generally you want key lengths >100 bit