



JENNER

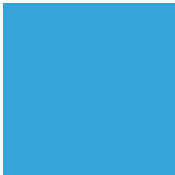




MOST IMPORTANT ADVICE:

GET AN EXPERT OR AT LEAST

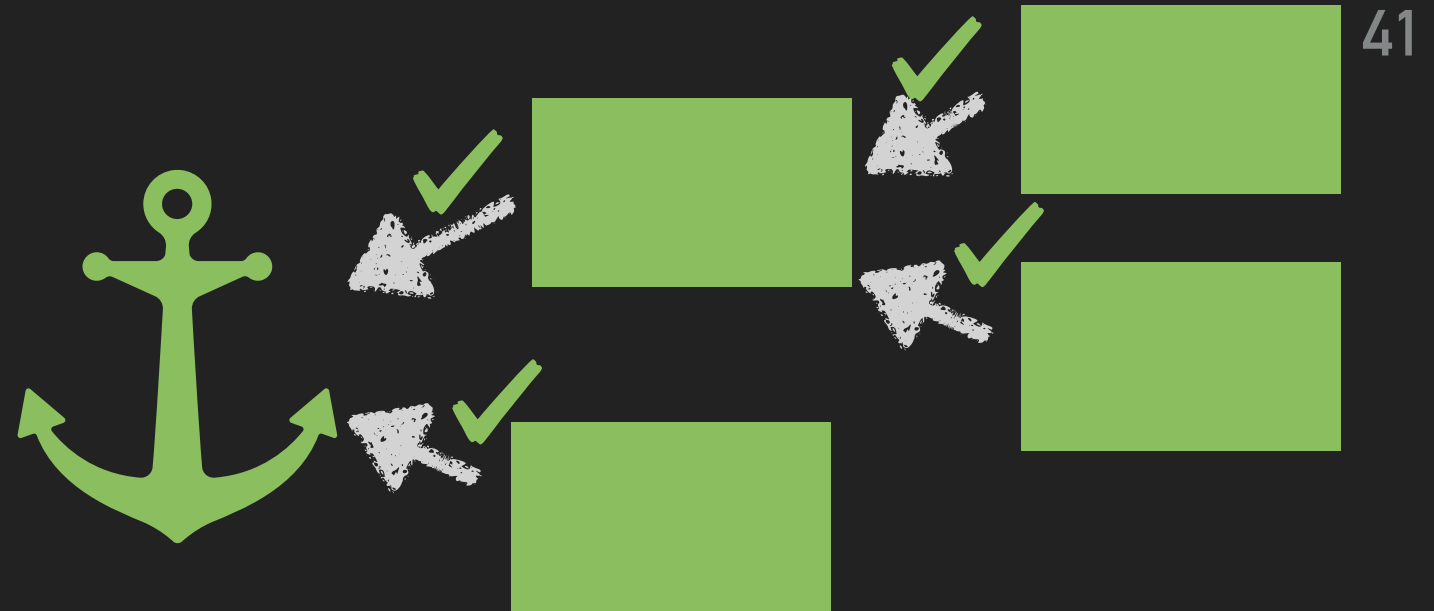
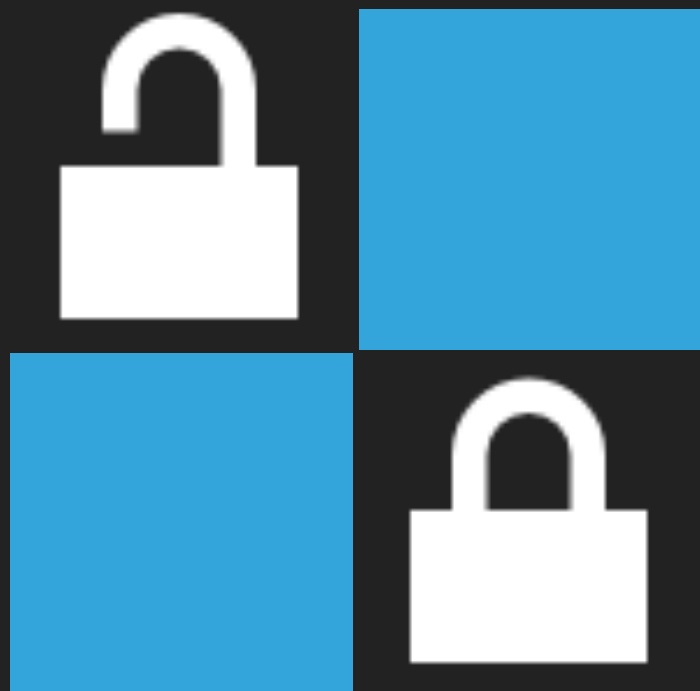
READ AND UNDERSTAND THE DOCUMENTATION!



40

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

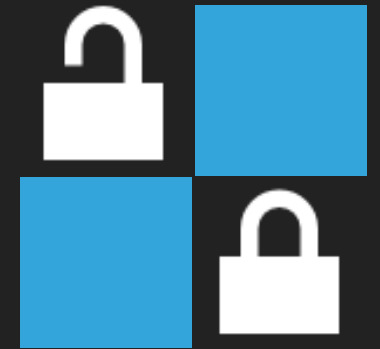
- ▶ At least be able to explain: "Hash vs. encryption", "Integrity vs. encryption", "Stream vs. block", "Mode of operation", "IV", "Nonce", "Padding", "Key derivation"
- ▶ Identify and name your trust anchors



41

PATTERNS

TRUST ANCHORS



**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