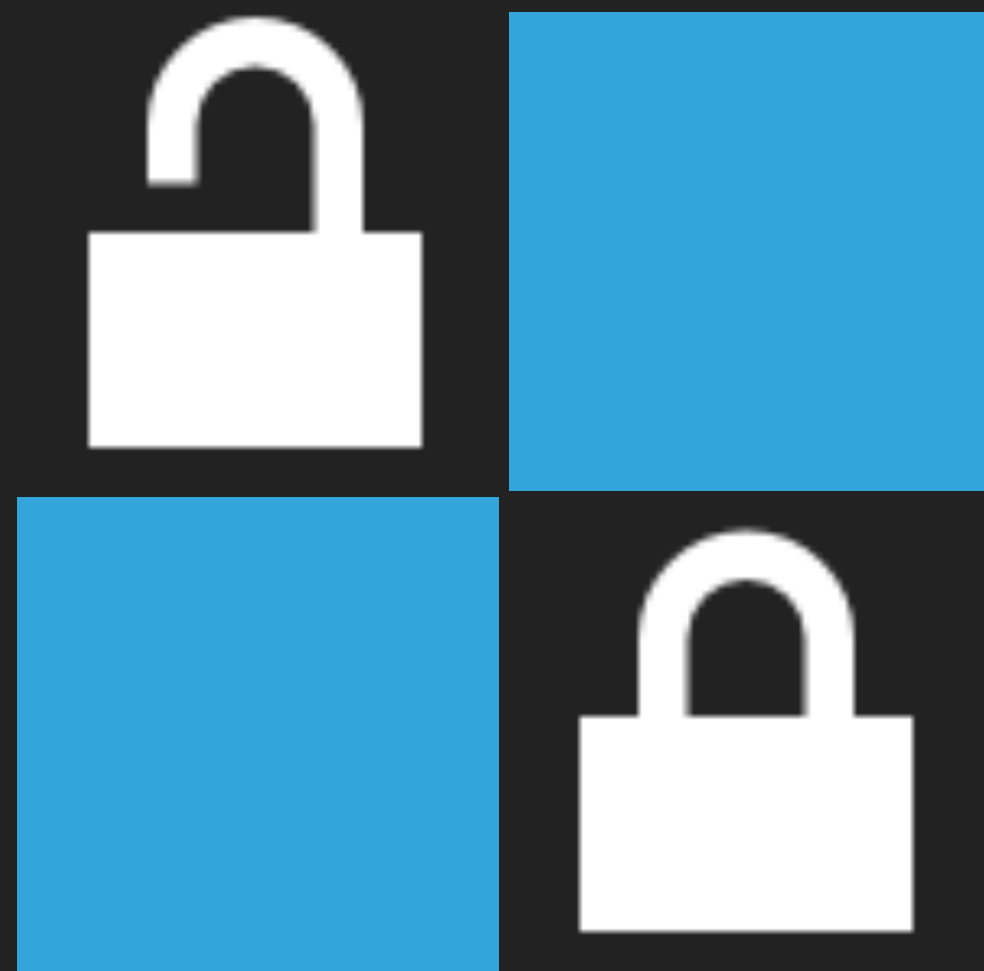


SOME WORDS THAT I MIGHT DROP AND THEN FORGET TO EXPLAIN

- ▶ **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: $H(A) = H(B) \Rightarrow A = B$
- ▶ **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



PATTERNS

TRANSPARENT ENCRYPTION