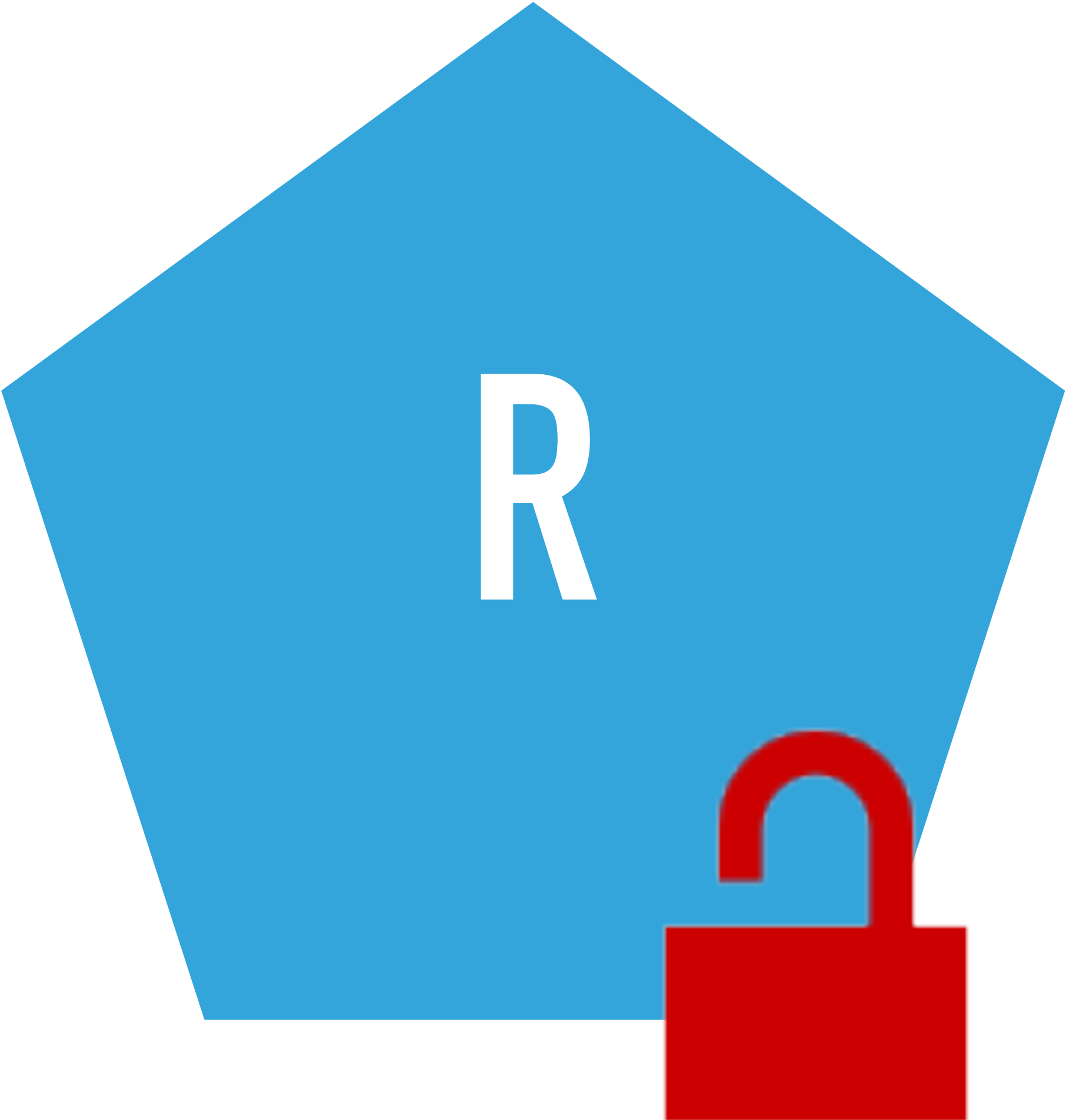




GOODCRYPTOGRAPHY



$E_k(R)$



$E(R)$

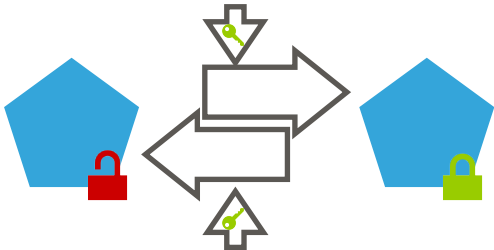




SECURESMALLKEY(S)

4

6



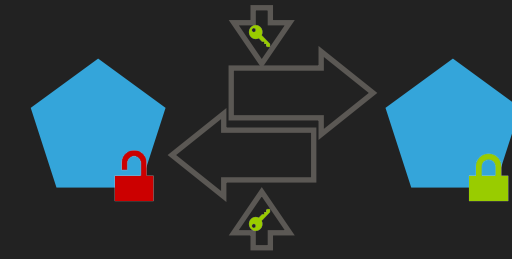
$$+ \text{IV}^*$$

IV

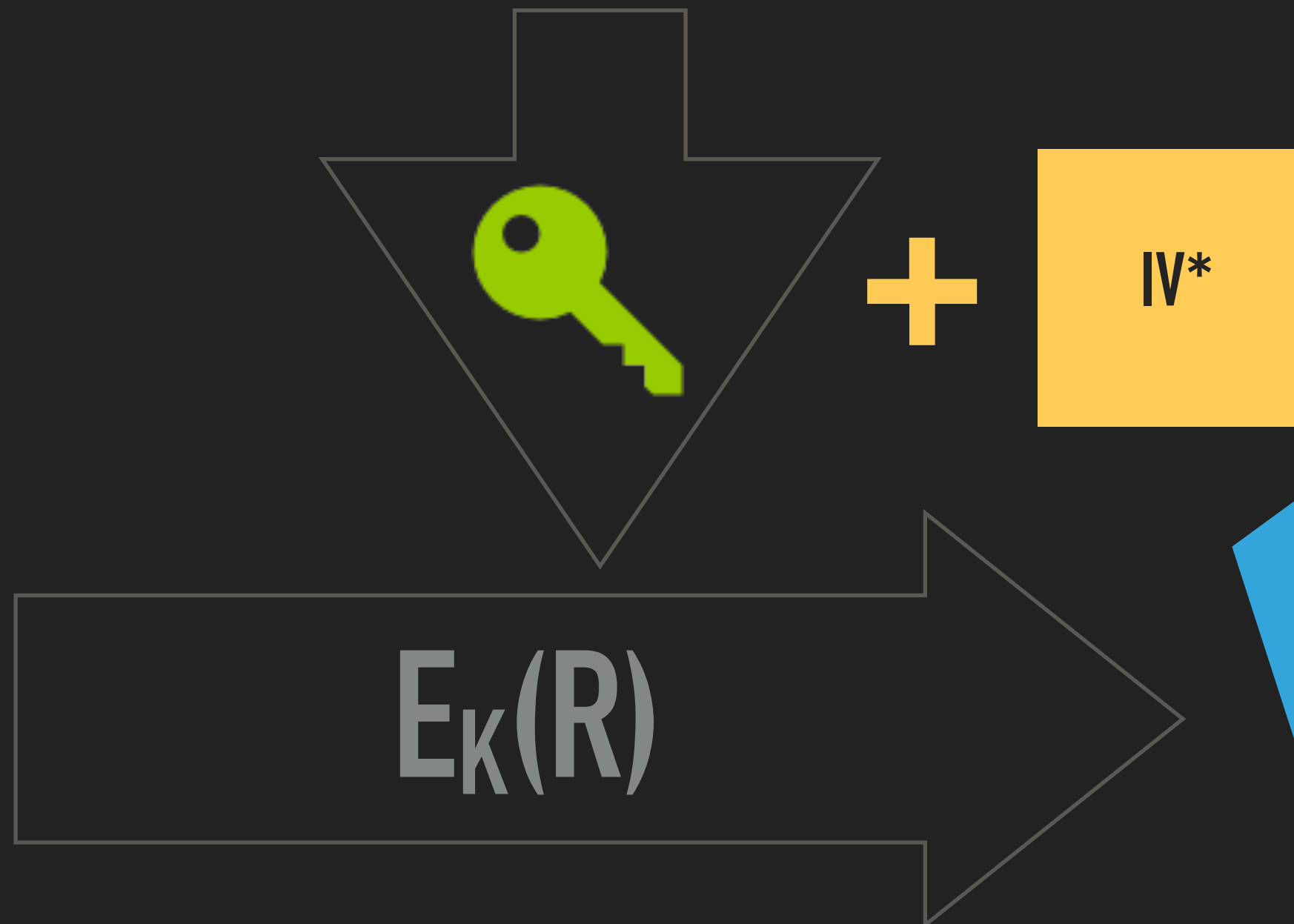
(*) IV - Initialisation Vector. Used in many cryptographic operations. Like a salt. Must be random, might be public.

Securing small keys is much easier
than securing large volumes of data

SECURE SMALL KEY(S)



R



E(R)

Securing small keys is much easier
than securing large volumes of data



(*) IV - Initialisation Vector. Used in many cryptographic operations. Like a salt. Must be random, might be public.



PATTERNS

**KEY DERIVATION 1:
PASSWORD TO KEY**