



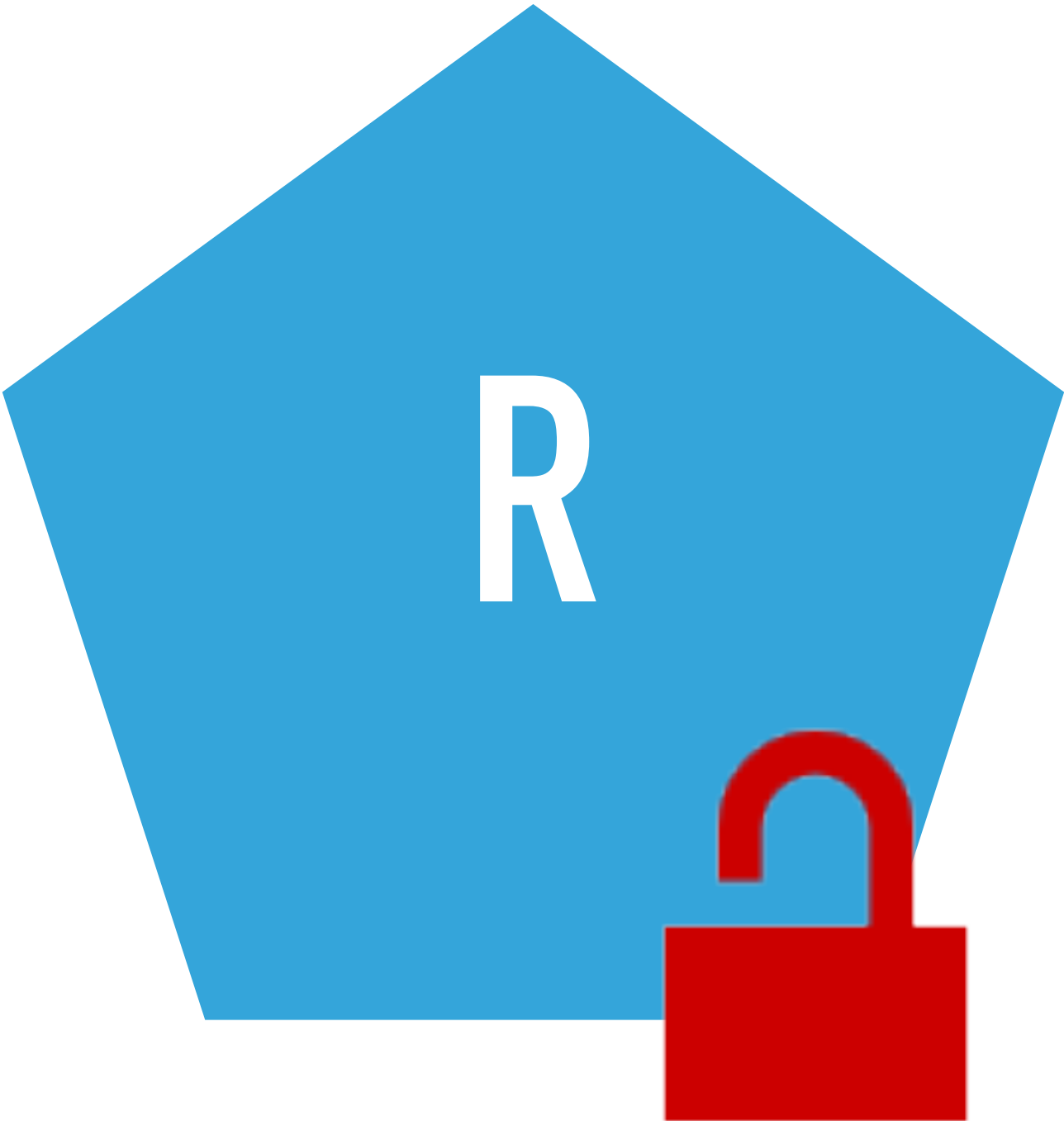
JENS NEURHAALFEN



SLEERBETTERVITHCORNTERENTION



$E_k(R)$



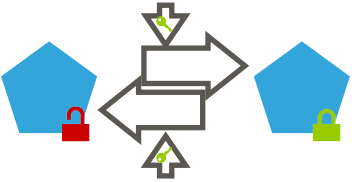
$E(R)$





SECURESMALLKEY(S)





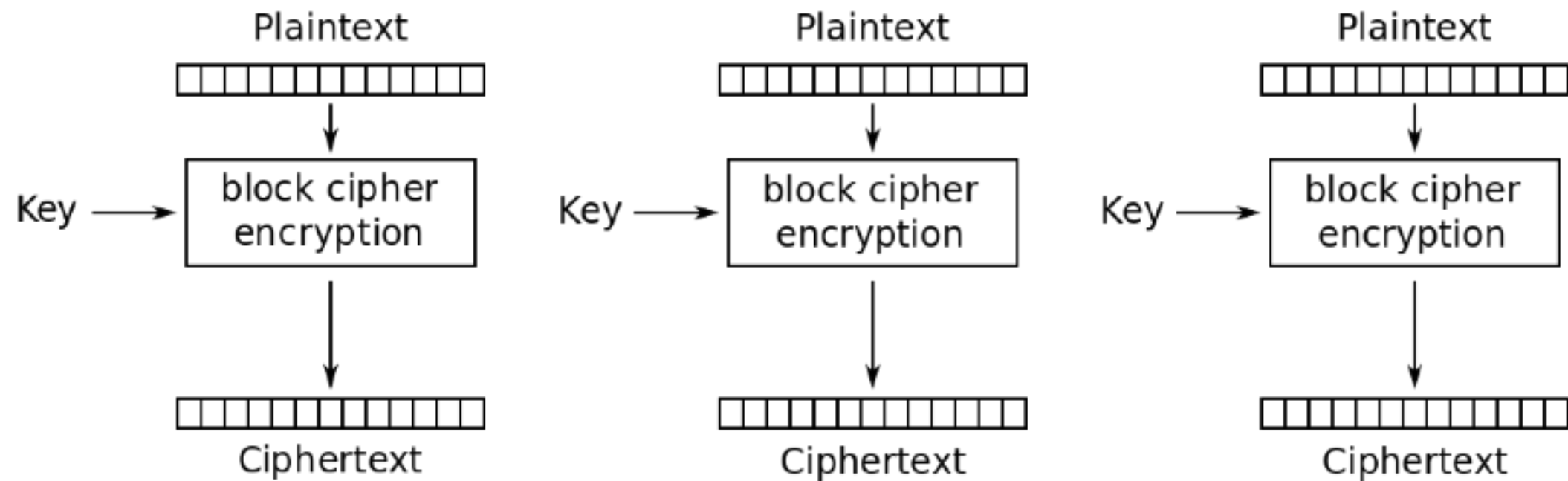
+

IV*

IV

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

BLOCK CIPHERS AND THE IV



Electronic Codebook (ECB) mode encryption



Original

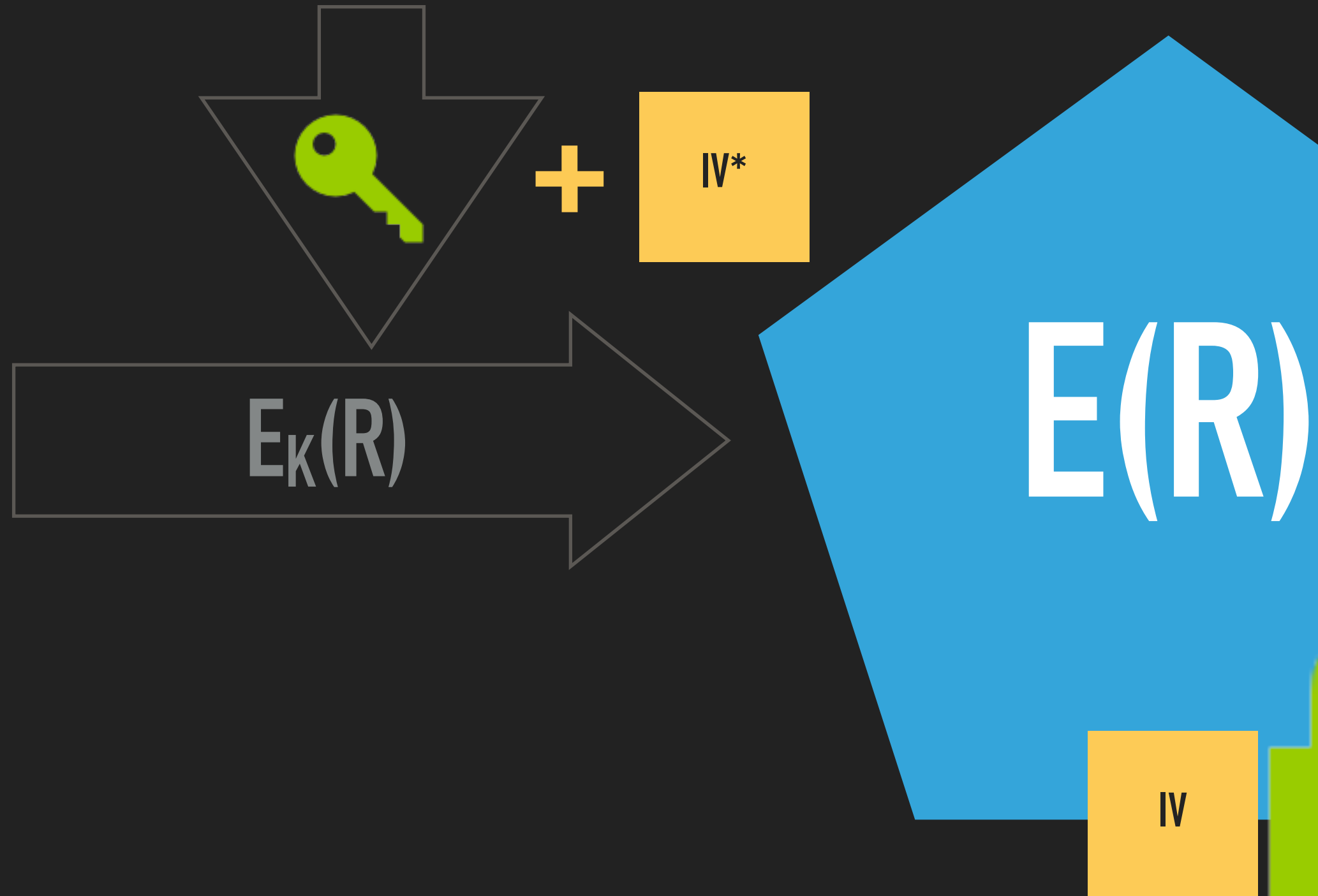
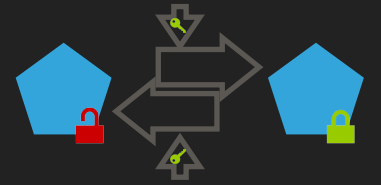


ECB



CBC (or other)

SECURE SMALL KEY(S)



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