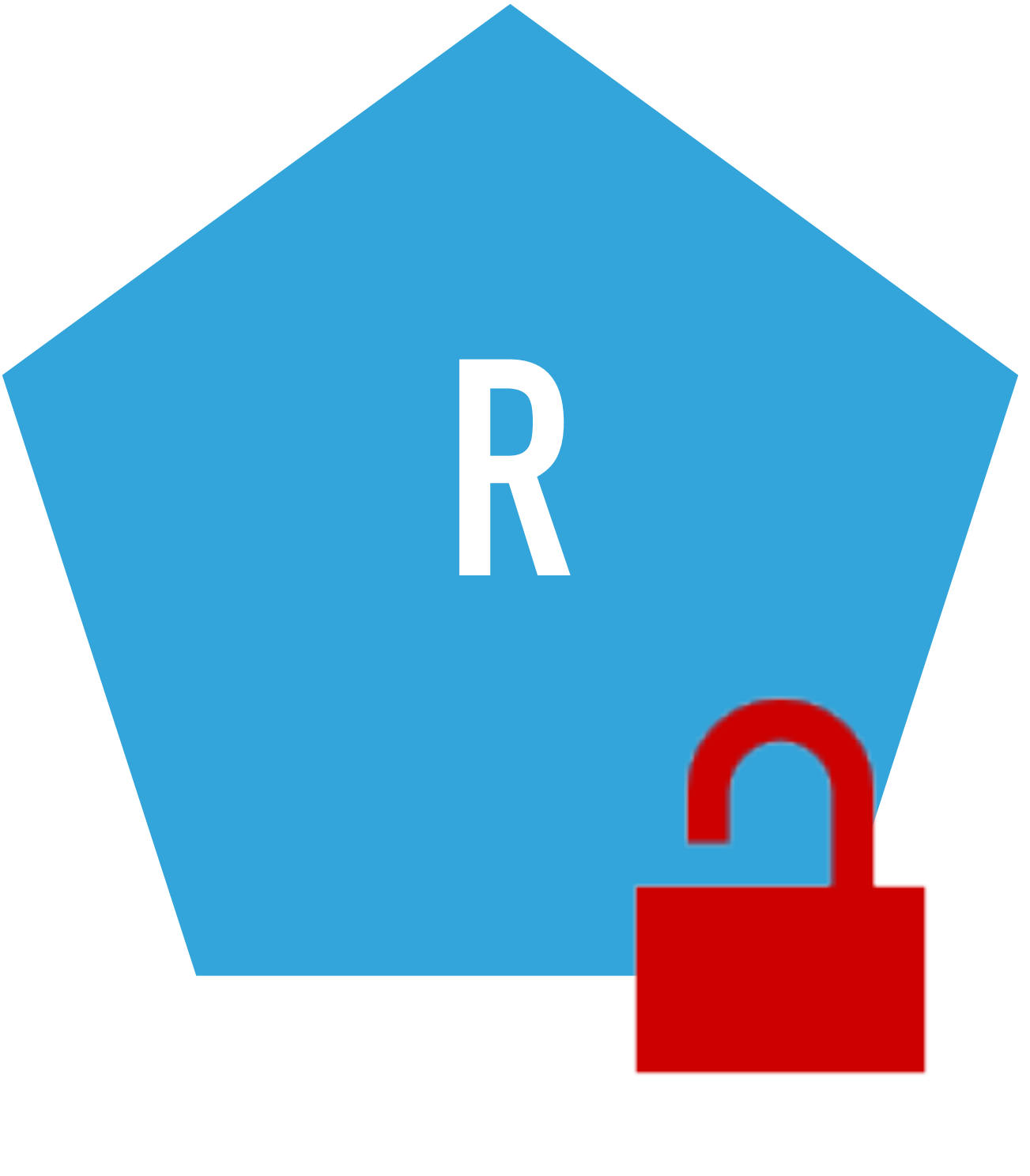
JENS NEUHALFEN

SLEEP BETTER WITH CONTENT ENCRYPTION

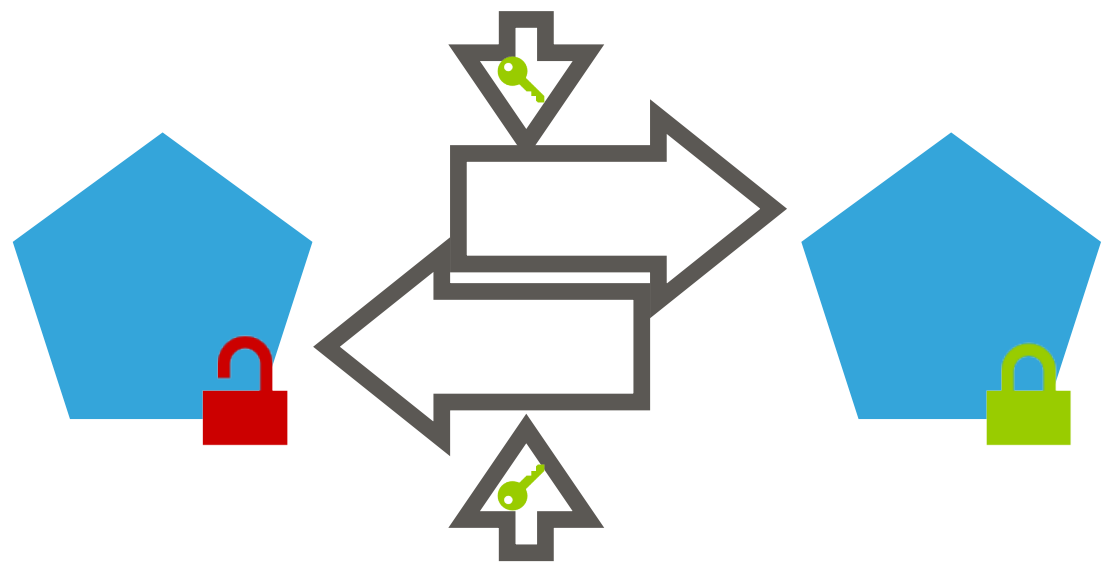

$E_K(R)$


R


E(R)

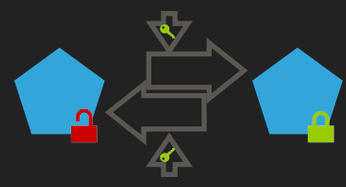
SECURE SMALL KEY(S)

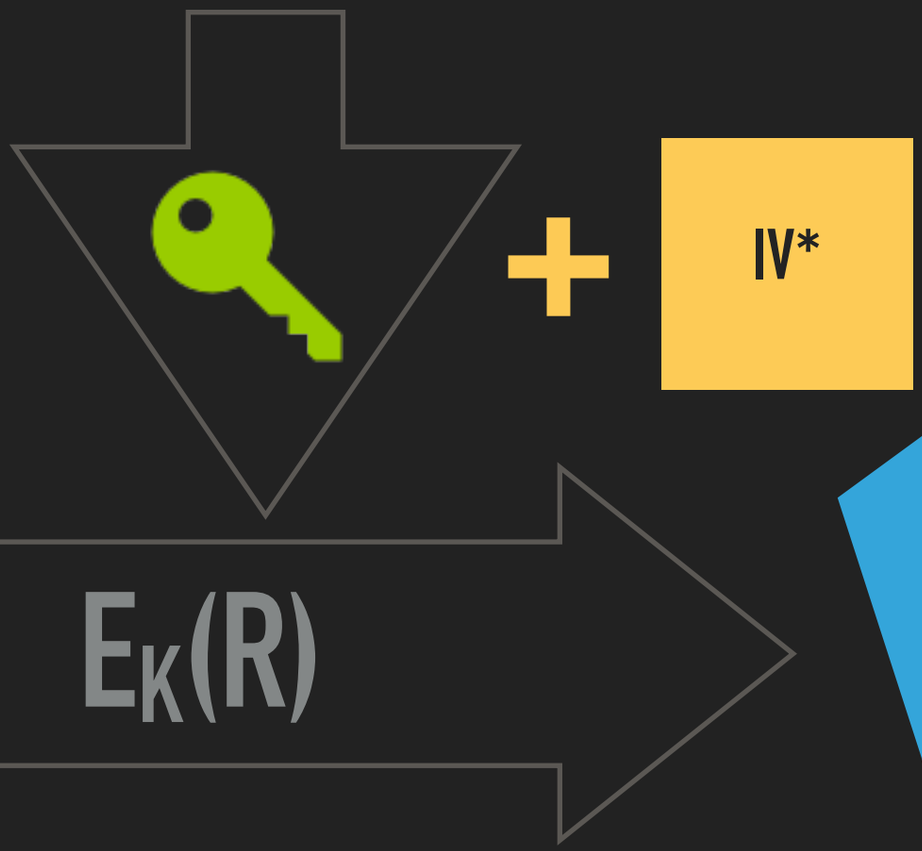
52



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

SECURE SMALL KEY(S)



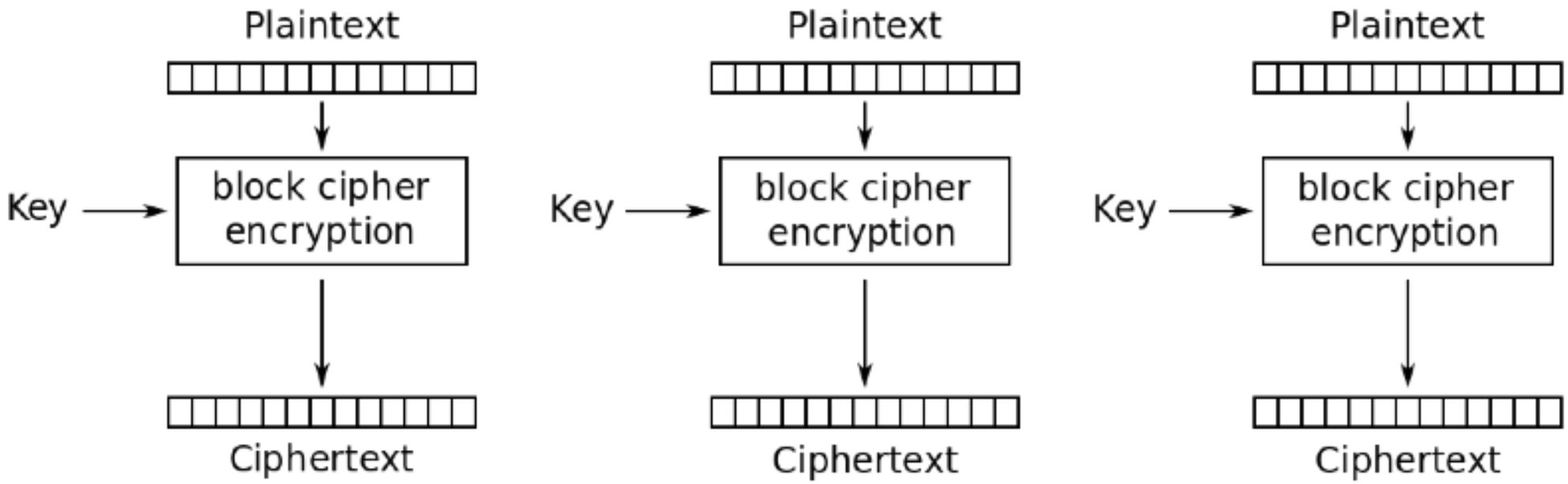


E(R)

IV

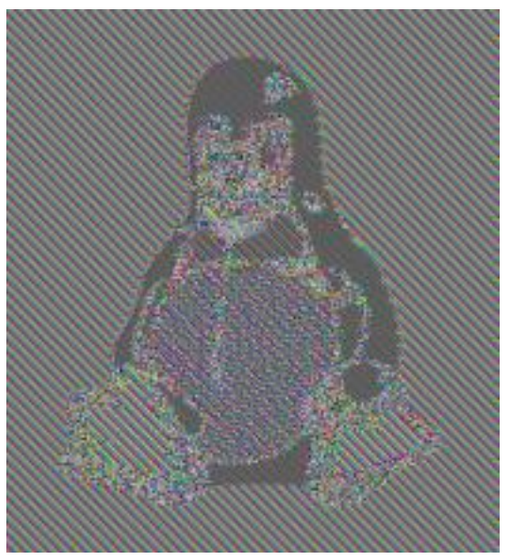
(*) IV - Initialisation Vector. Used in many cryptographic operations. Like a salt. Must be random, might be public.

BLOCK CIPHERS AND THE IV

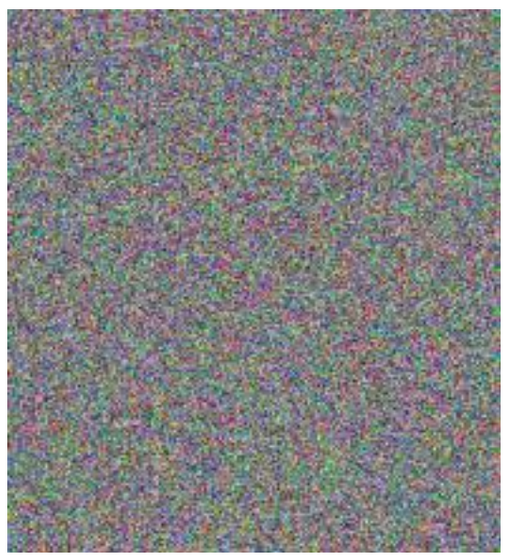


Electronic Codebook (ECB) mode encryption

Original



ECB



CBC (or other)

https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation