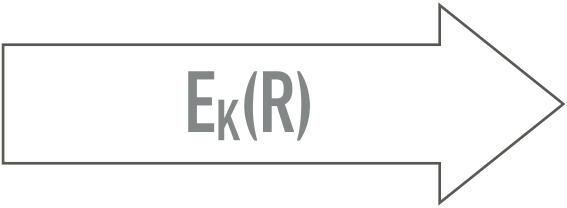
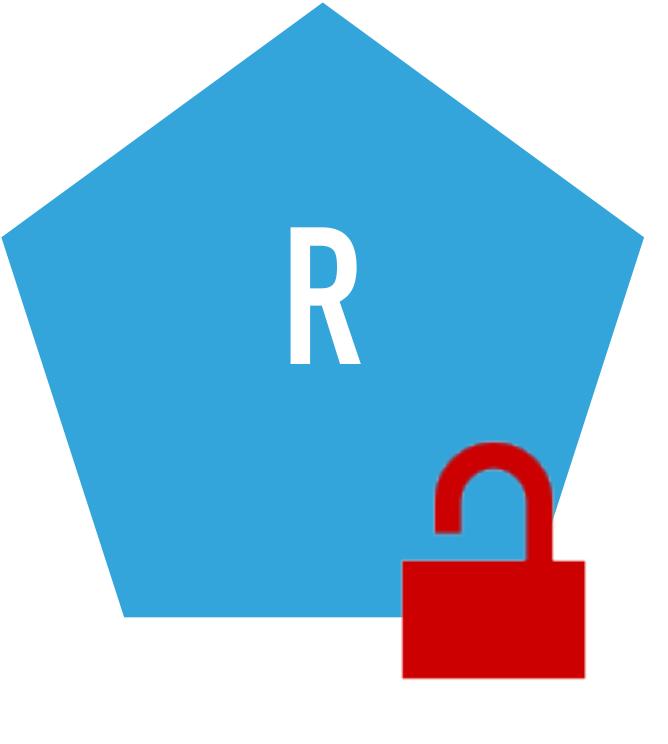




#### JENS NEUHALFEN

#### SLEEP BETTER WITH CONTENT ENCRYPTION









# SECURE SMALL KEY(S)



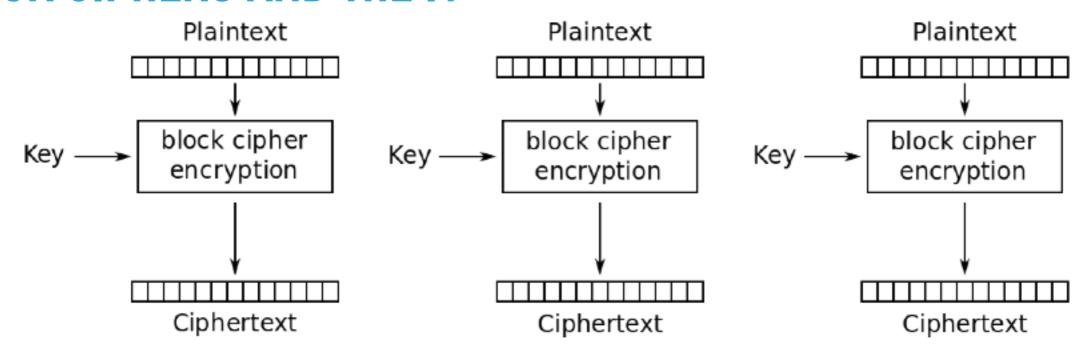


IV

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

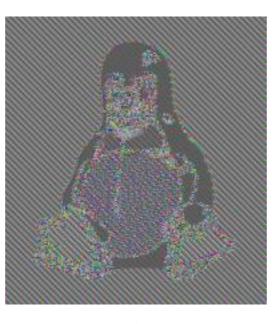
#### SLEEP BETTER WITH CONTENT ENCRYPTION

## **BLOCK CIPHERS AND THE IV**

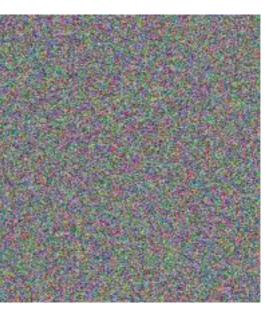


### Electronic Codebook (ECB) mode encryption



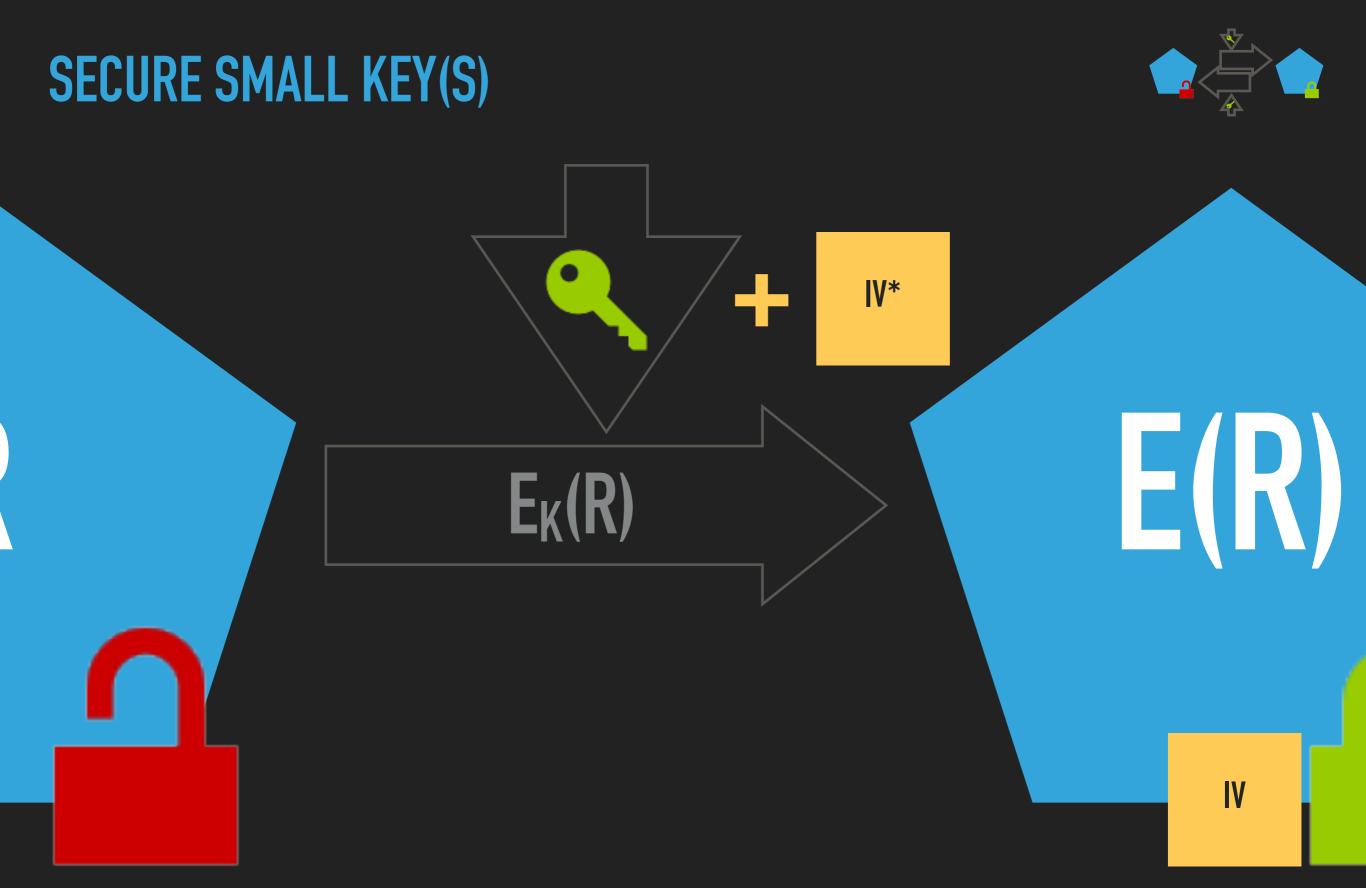


**ECB** 



CBC (or other)

https://en.wikipedia.org/wiki/Block\_cipher\_mode\_of\_operation



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