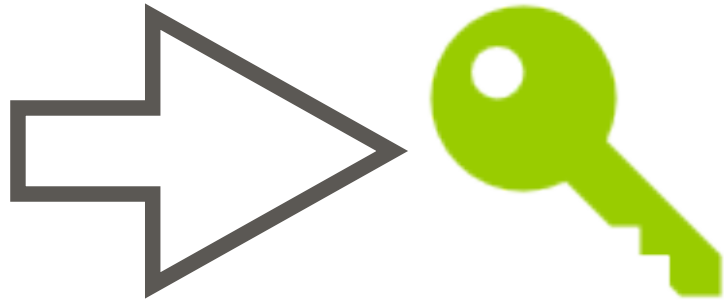
JENS NEUHALFEN

****

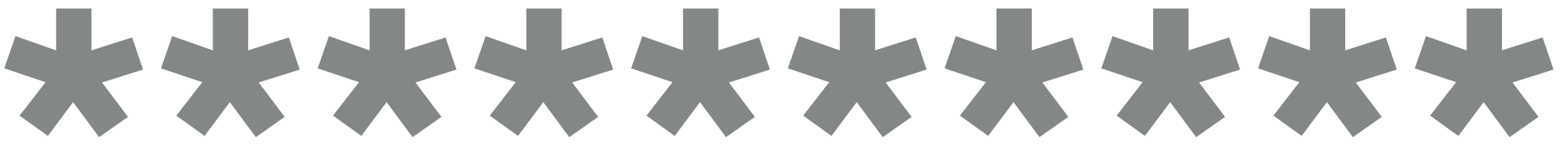


FROM PASSWORD TO KEY

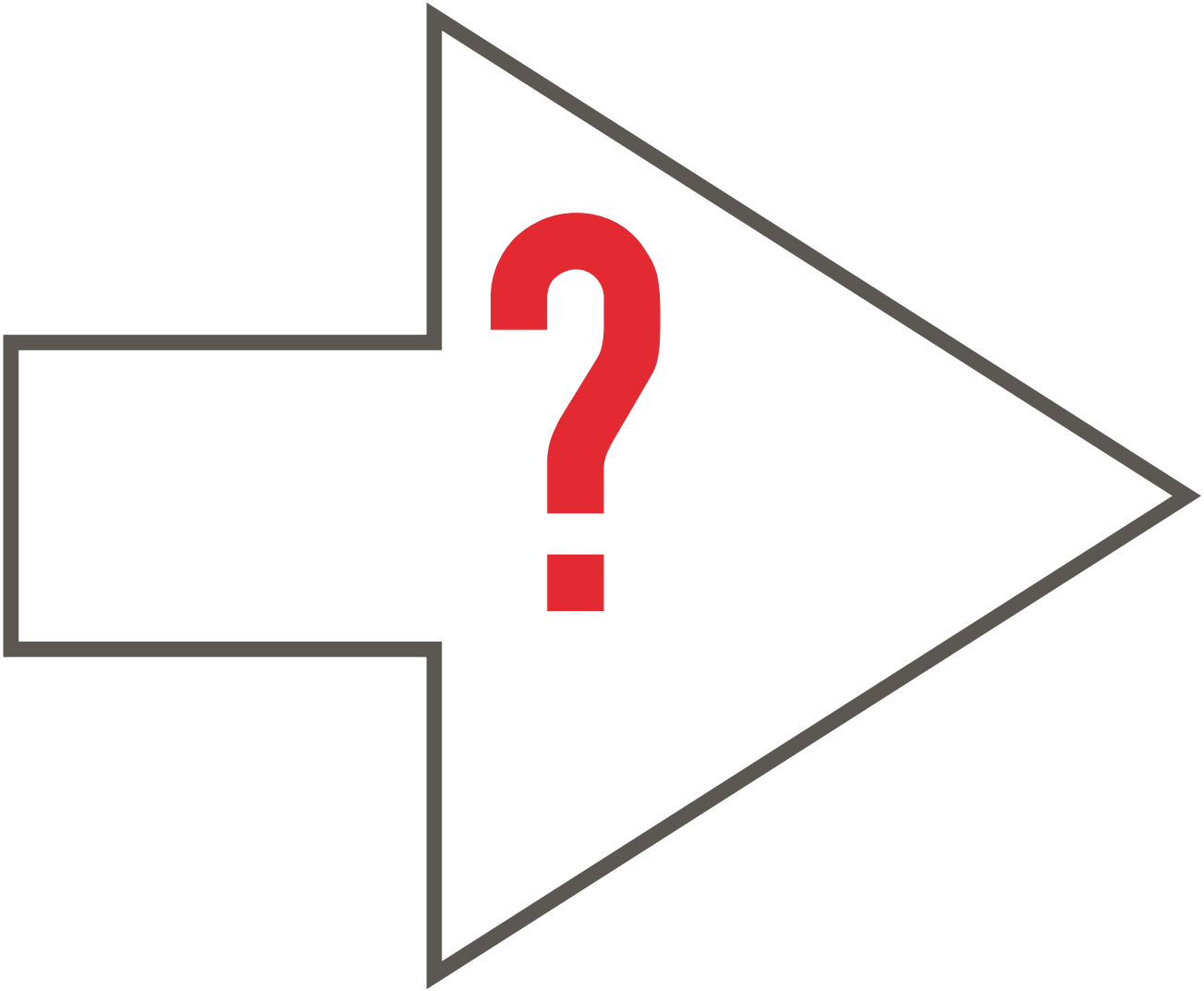
SLEEP BETTER WITH CONTENT ENCRYPTION

68

128 bit key

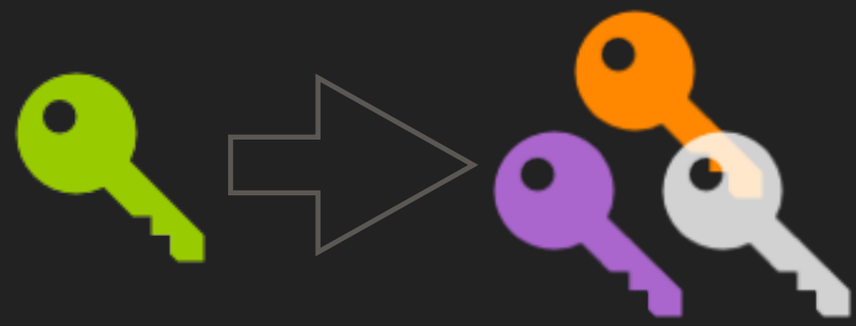


password



- Key derivation functions (KDF) convert passwords to keys
- For good (21+ chars) passwords use HKDF (RFC5869)
- Else: use a KDF with brute force protection (*)
  - SCRYPT (RFC7914)
  - PBKDF2 (RFC2898)

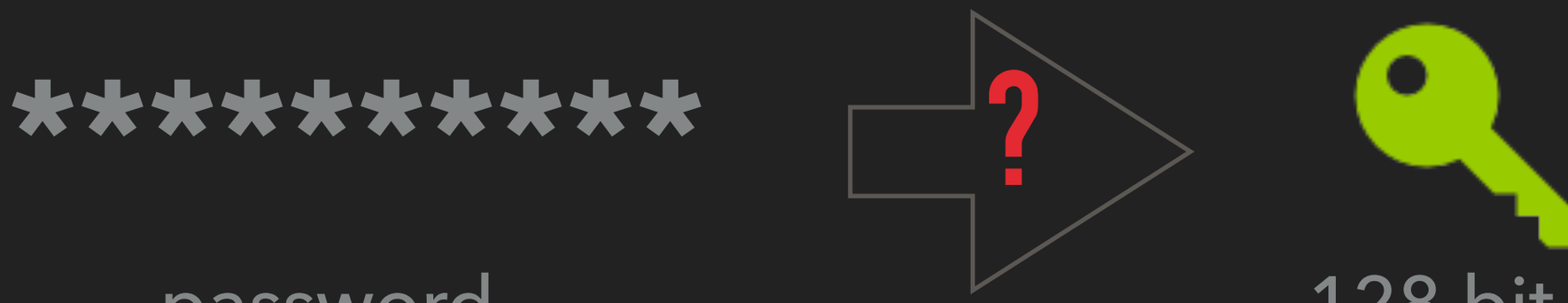
(*) *Brute force protection*: The function is designed to be very slow (up to seconds). This prevents enumeration attacks.



PATTERNS

KEY DERIVATION 2: FROM 1 TO N

FROM PASSWORD TO KEY



password

128 bit key

- Key derivation functions (KDF) convert passwords to keys
- For good (21+ chars) passwords use HKDF (RFC5869)
- Else: use a KDF with brute force protection (*)
  - SCRYPT (RFC7914)
  - PBKDF2 (RFC2898)

(*) *Brute force protection*: The function is designed to be very slow (up to seconds). This prevents enumeration attacks.