



JENNER

* * * * *



FROM PASSWORD TO KEY



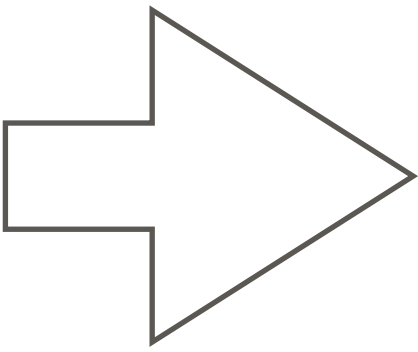


128bitkey





password





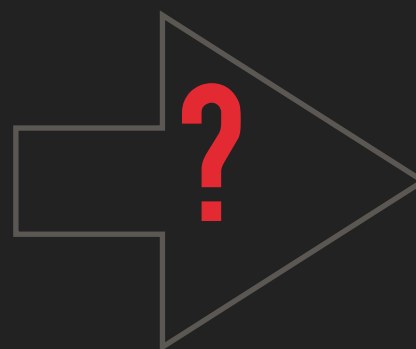
- ▶ aw92SDAVg1kqusabvgw38
 - ▶ 128 bit
- ▶ 3o8uGsdA
 - ▶ 8 chars, 48 bit (cracked in hours to days)
 - ▶





FROM PASSWORD TO KEY

password



128 bit key

***** ➡ 

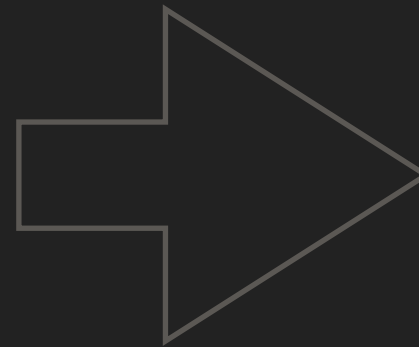
- ▶ Key derivation functions (KDF) convert passwords to keys
- ▶ For good (21+ chars) passwords use HKDF ([RFC5869](#))
- ▶ Else: use a KDF with brute force protection (*)
 - ▶ SCRYPT ([RFC7914](#))
 - ▶ PBKDF2 ([RFC2898](#))

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

FROM PASSWORD TO KEY



password



128 bit key

▶ aw92SDAVg1kqusabvgw38



▶ 128 bit

▶ 3o8uGsdA



▶ 8 chars, 48 bit (cracked in hours to days)