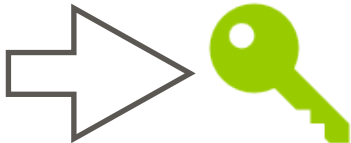




JENNS NEURHALFEN



FROM PASSWORD TO KEY

GOODCRYPTOGRAPHY

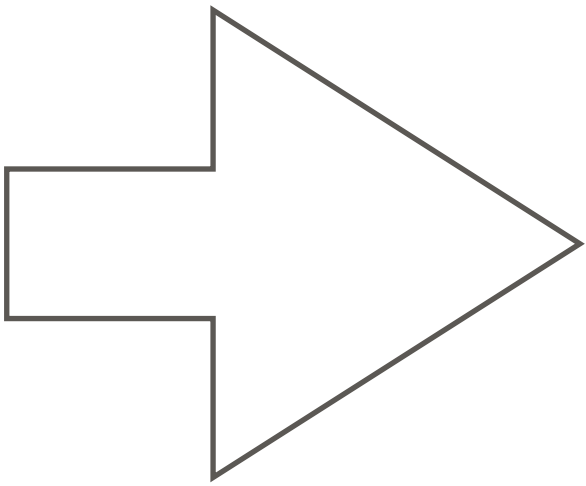
48

128bitkey





password





- ▶ *A random password has
~ 6 bits per character (*)*
- ▶ A 128 bit key needs ≥ 21 character passwords

(*) a-zA-Z0-9 \rightarrow ~64 different values per character (2^6). A 128 bit passwords must be ≥ 21 characters long ($128/6$)

Secure passwords are *very* long

FROM PASSWORD TO KEY



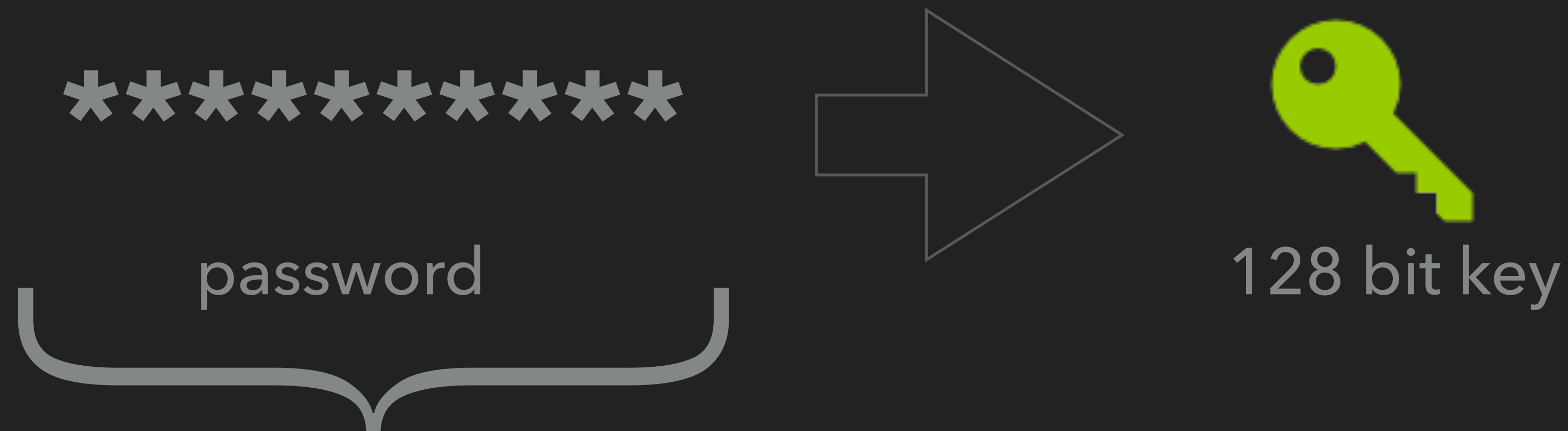
- ▶ A *random* password has
~ 6 bits per character (*)
- ▶ A 128 bit key needs ≥ 21 character passwords

Secure passwords are very long

(*) a-zA-Z0-9 \rightarrow ~64 different values per character (2^6). A 128 bit passwords must be ≥ 21 characters long ($128/6$)

FROM PASSWORD TO KEY

***** ➡ 



▶ aw92SDAVg1kqusabvgw38 

▶ 128 bit

▶ 3o8uGsdA 

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

CREATE YOU PERSONAL PASSWORDS USING A PASSWORD MANAGER!