JENS NEUHALFEN


TIGER


SCOTT

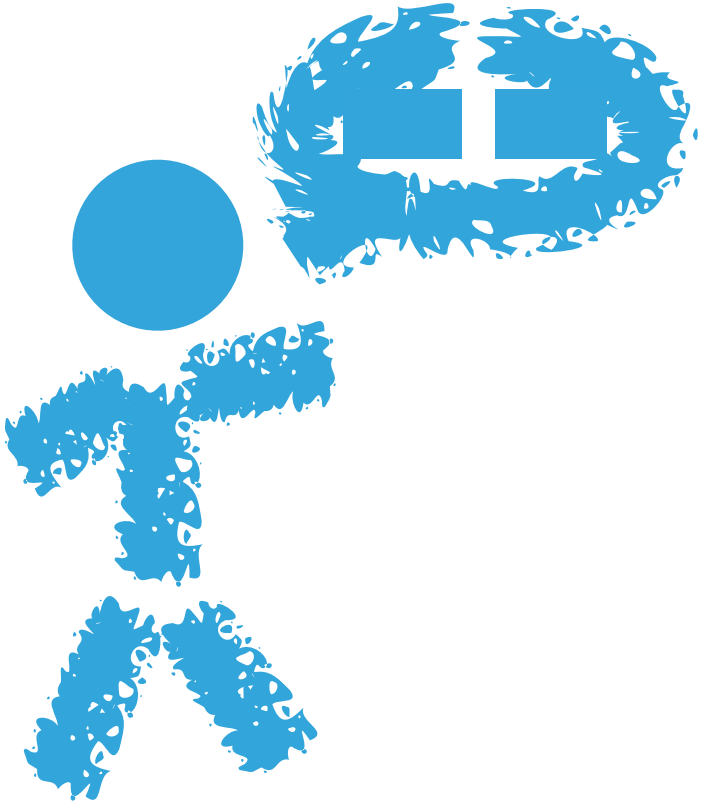
USER LOGIN: MIGRATE PASSWORDS

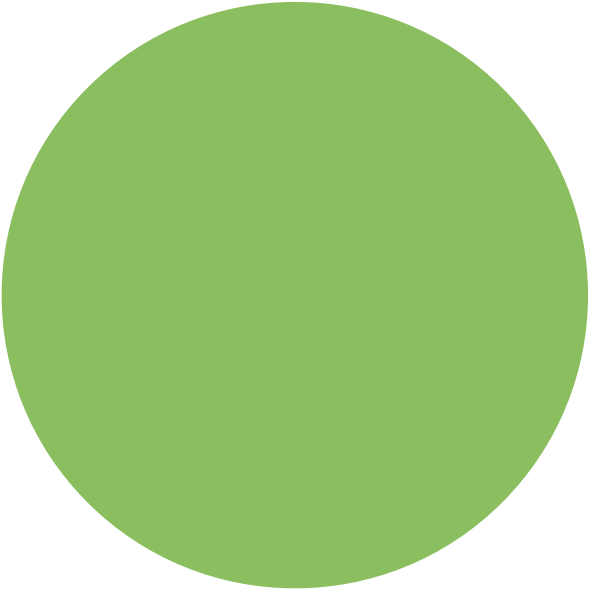
GOOD CRYPTOGRAPHY

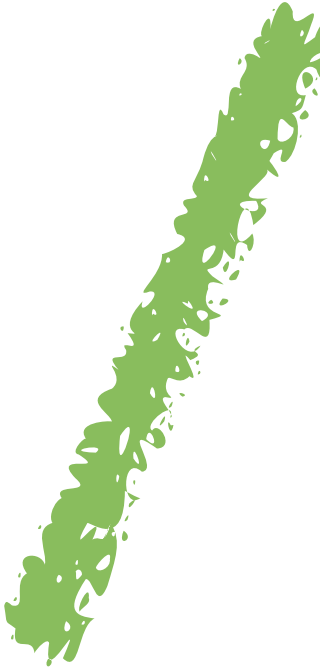
56

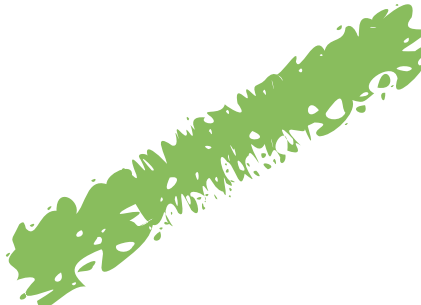
Problem: Migrate password hashes to new algorithms

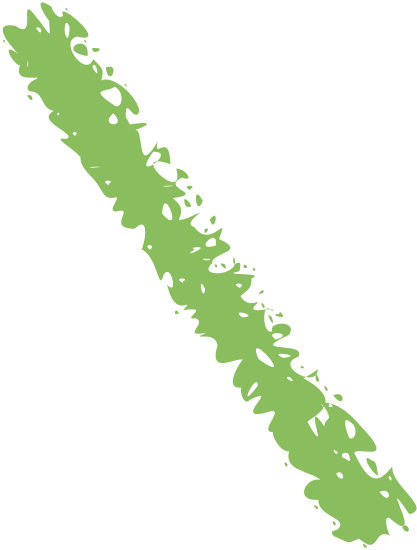
Solution: Chain hashing functions

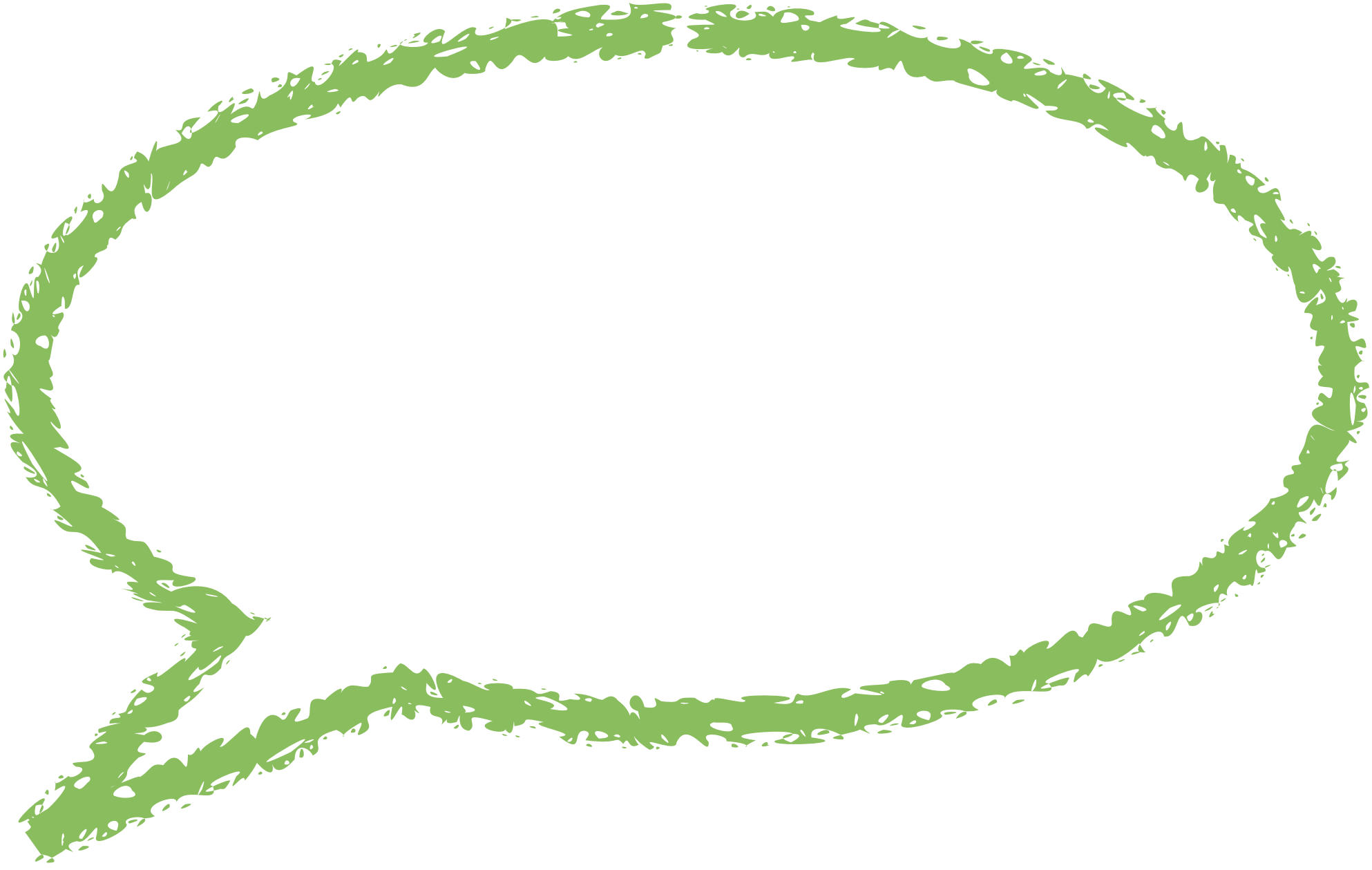












User	Algorithm	Hash
SCOTT	▸ **MD5(PWD)**	3959dc9...
...	...	...

ValidatePassword

hash password w. MD5

check vs. database


TIGER


SCOTT

3959DC9...

PURE HASH CONSIDERED HARMFUL

USER LOGIN: MIGRATE PASSWORDS

Problem: Migrate password hashes to new algorithms

Solution: Chain hashing functions

ValidatePassword

hash password w. MD5

check vs. database

User	Algorithm	Hash
SCOTT	MD5(PWD)	3959dc9…
…	PURE HASH CONSIDERED HARMFUL	…

Even consumer grade graphic cards calculates giga-hashes (2^30) per second.

- https://www.troyhunt.com/our-password-hashing-has-no-clothes/
- https://gist.github.com/epixoip/a83d38f412b4737e99bbef804a270c40
- http://cynosureprime.blogspot.de/2017/08/320-million-hashes-exposed.html
- https://www.owasp.org/index.php/Password_Storage_Cheat_Sheet
- https://en.wikipedia.org/wiki/Pepper_(cryptography)