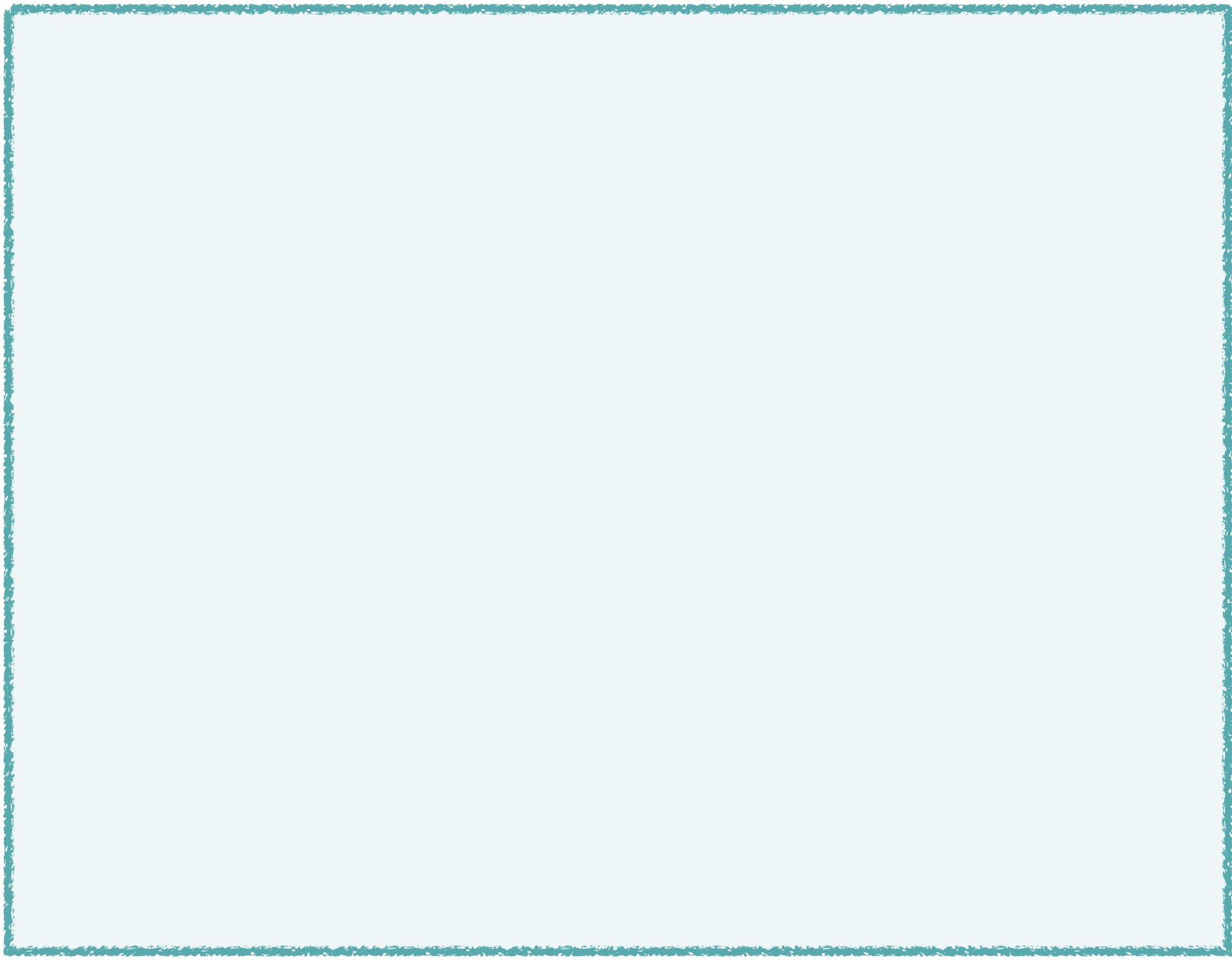








JENNER





TIGER

SCOTT

USER LOGIN: MIGRATE PASSWORDS







**Problem:** Migrate password hashes to new algorithms

**Solution:** Chain hashing functions









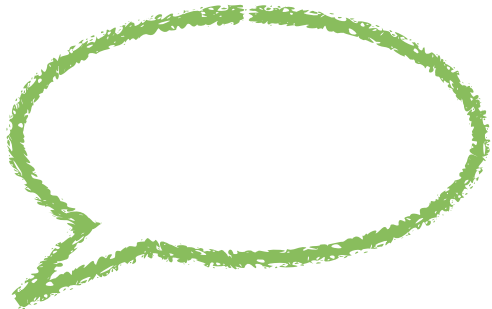
*Handwritten text, likely bleed-through from the reverse side of the page.*











User	Algorithm	Hash
SCOTT	▶ MD5(PWD)	3959dc9...
...	...	...



validated Password



hashpassword.MD5





cheek vs. data base

TIGER

SCOTT

3959DC9. . .





**PURE HASH CONSIDERED HARMFUL**





User	Algorithm	Hash
SCOTT	MD5(✓)	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://www.owasp.org/index.php/Password_Storage_Cheat_Sheet)
- ▶ [https://en.wikipedia.org/wiki/Pepper\\_\(cryptography\)](https://en.wikipedia.org/wiki/Pepper_(cryptography))

# USER LOGIN: MIGRATE PASSWORDS



**Problem:** Migrate password hashes to new algorithms

**Solution:** Chain hashing functions

