







JENNER



SLEEPER WHEN CENTER POSITION

ALGORITHM ROLL OVER

**DES**

**BLOWFISH**

**AES**

**MD5**

**SHA-1**

**SHA-256**

**RSA-1024**

**RSA-2048**

**?? POST QUANTUM ??**

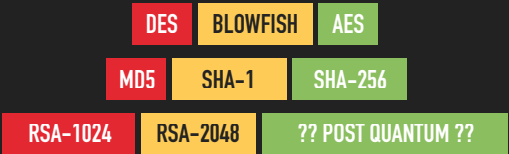
**Problem:** Algorithms must be changed and data migrated

**Solution:** Design for online data migration

Record-ID	...	Masterkey ID (Data...)	
B9E10DEE-C97E-...	...	B874920B-E801-...	...
FDE0C6E3-8BF0-...	...	9A6580FC-1248-...	...
...	...	9A6580FC-1248-...	...



# ALGORITHM ROLLOVER

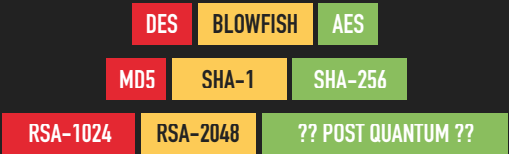


**Problem:** Algorithms must be changed and data migrated

**Solution:** Design for online data migration

Record-ID	Algorithms	Masterkey ID	(Data...)
B9E10DEE-C97E-...	<ul style="list-style-type: none"><li>▶ PBKDF2(...)</li><li>▶ AES128-GCM</li></ul>	B874920B-E801-...	...
FDE0C6E3-8BF0-...	<ul style="list-style-type: none"><li>▶ SCRYPT(...)</li><li>▶ AES256-CBC</li><li>▶ PKCS#5</li></ul>	9A6580FC-1248-...	...
...	...	9A6580FC-1248-...	...

# ALGORITHM ROLLOVER



**Problem:** Algorithms must be changed and data migrated

**Solution:** Design for online data migration

Record-ID	...	Masterkey ID (Data...)	
B9E10DEE-C97E-...	...	B874920B-E801-...	...
FDE0C6E3-8BF0-...	...	9A6580FC-1248-...	...
...	...	9A6580FC-1248-...	...