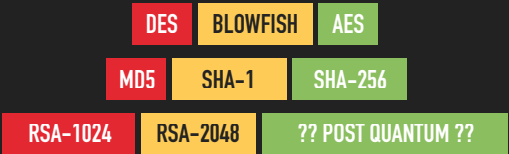


ALGORITHM ROLLOVER

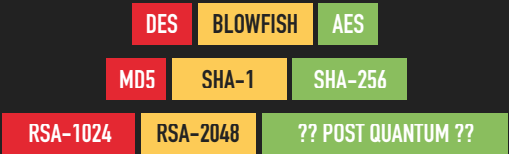


Problem: Algorithms must be changed and data migrated

Solution: Design for online data migration

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

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">▶ PBKDF2(...)▶ AES128-GCM	B874920B-E801-...	...
FDE0C6E3-8BF0-...	<ul style="list-style-type: none">▶ SCRYPT(...)▶ AES256-CBC▶ PKCS#5	9A6580FC-1248-...	...
		9A6580FC-1248-...	

ATTENTION: REENCRIPTING OPENS A WINDOW OF ATTACK — BEST USE THE NEW ALGORITHM FOR NEW DATA!