DES BLOWFISH AES

MD5 SHA-1 SHA-256

RSA-1024 RSA-2048 ?? POST QUANTUM ??

PATTERNS

ALGORITHM ROLLOVER

DES	BLOWFISH	AES
MD5	SHA-1	SHA-256
RSA-1024	RSA-2048	?? POST QUANTUM ??
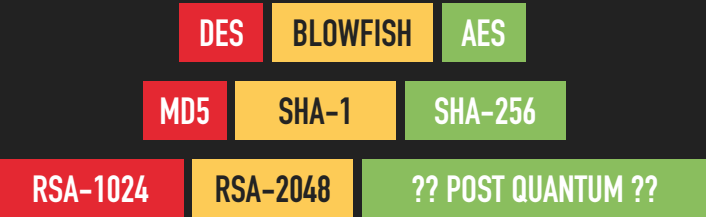
ALGORITHM ROLLOVER

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-...	...