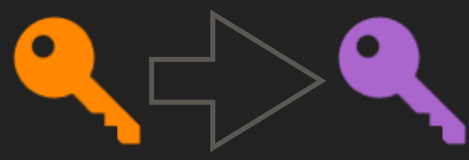
KEY REFRESH



Problem: Keys must only be used for a limited amount of data

Solution: Design for (constant but not frequent) key rollover

Record-ID	Version	Masterkey ID	(Data…)
B9E10DEE-C97E-…	1	**B874920B-E801…**	…
FDE0C6E3-8BF0-…	1	**9A6580FC-1248…**	…
…	3	**9A6580FC-1248…**	…

ATTENTION: REENCRYPTING OPENS A WINDOW OF ATTACK — BEST USE THE NEW KEY FOR NEW DATA!

DES BLOWFISH AES

MD5 SHA-1 SHA-256

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

PATTERNS

ALGORITHM ROLLOVER