



JENNER

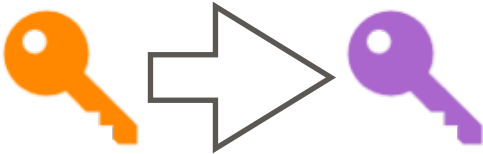


KEY REFRESH

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

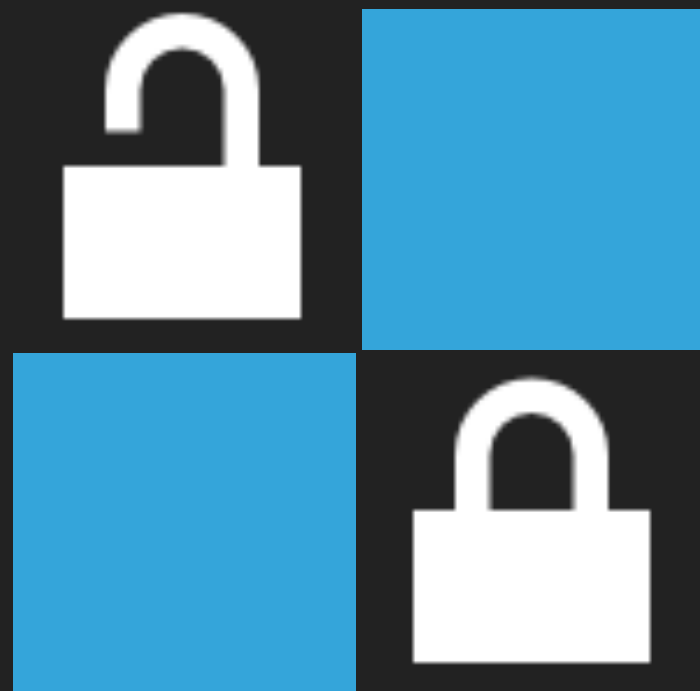
Solution: Design for (constant but not frequent) key rollover

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





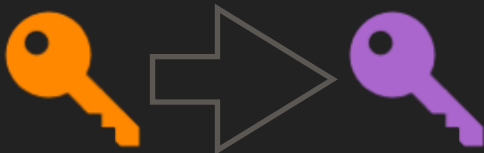
ATTENTION: REENCRYPTING OPENS A WINDOW OF ATTACK



PATTERNS

ALGORITHM
ROLLOVER

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...	...