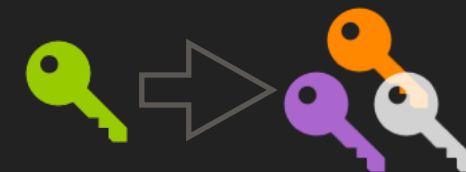


PATTERNS

**KEY DERIVATION 2:
FROM 1 TO N**

DERIVE PER RECORD KEYS



Problem: Use different keys for different records, only store master key.

Solution: Use key derivation to derive per-record keys.

 + $r_1.id + r_1.ver$  

 + $r_2.id + r_2.ver$  

...

 + $r_n.id + r_n.ver$  

IMPORTANT: NEVER USE THE SAME KEY/IV TO ENCRYPT DIFFERENT DATA

MAKE SURE THAT THE MASTER KEY HAS ENOUGH ENTROPY FOR DERIVED KEY AND DERIVED IV