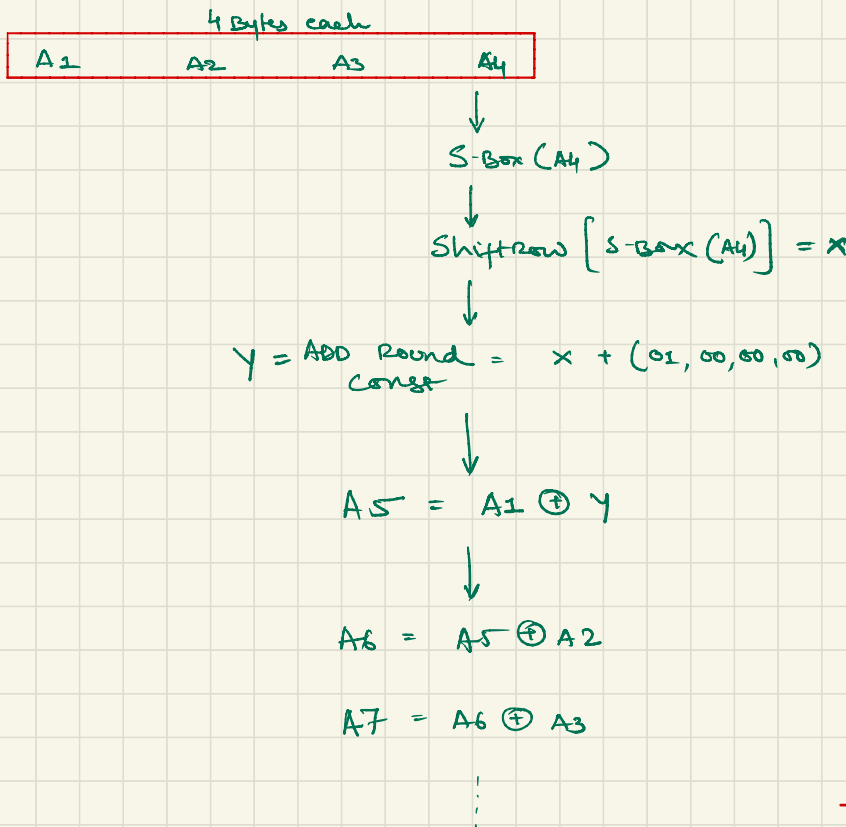


Reverse key scheduling

Key scheduling::

- Take last 4 bytes of the original key and left shift by 1
- Use byte substitution (s-box) for those 4 bytes
- Add round constant to those 4 bytes (round constant = (01,00,00,00))
- XOR with 1st 4 bytes of original key - The ans becomes 1st 4 bytes of your round key.
- Keep performing XOR operations of 4-4 bytes as shown in the example below to get 10 round keys.



For Reverse
Key
Scheduling
↓
Reverse
the
Steps