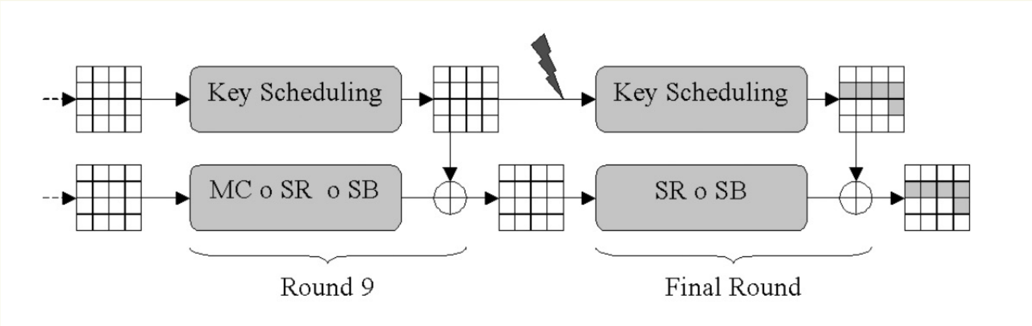
2.4/ 2.5 :: Bit fault attack - Description

-> Fault occurs on one bytes of K9, right before key scheduling to get K10



-> We want the Fault to occur on last 4 bytes of K9

-> If "C" is the correct cipher text without any faults then the equation of C comes out as:

- if $i = 0$:

$$C_i = SubByte(M^9_{ShiftRow^{-1}(i)}) \oplus SubByte(K^9_{(i+1 \ mod \ 4)+12}) \oplus K^9_i \oplus 0\text{x}36$$

- if $i \in \{1, 2, 3\}$:

$$C_i = SubByte(M^9_{ShiftRow^{-1}(i)}) \oplus SubByte(K^9_{(i+1 \ mod \ 4)+12}) \oplus K^9_i$$

-> If "D" is the correct cipher text without any faults then the equation of D comes out as:

- if $k = 0$:

$$D_k = SubByte(M^9_{ShiftRow^{-1}(k)}) \oplus SubByte(K^9_j \oplus e_j) \oplus K^9_k \oplus 0\text{x}36$$

- if $k \in \{1, 2, 3\}$:

$$D_k = SubByte(M^9_{ShiftRow^{-1}(k)}) \oplus SubByte(K^9_j \oplus e_j) \oplus K^9_k$$

Where, k in shiftrow^{-1}(k) is the position of non zero bytes of C XOR D.

Talking XOR of the above equations::

$$C_k \oplus D_k = SubByte(K_j^9) \oplus SubByte(K_j^9 \oplus e_j)$$

-> Finding K9 (round key value at 9th round) that satisfies the above equation will get us the round key RK9.

-> Applying reverse key scheduling will give us original key as output.