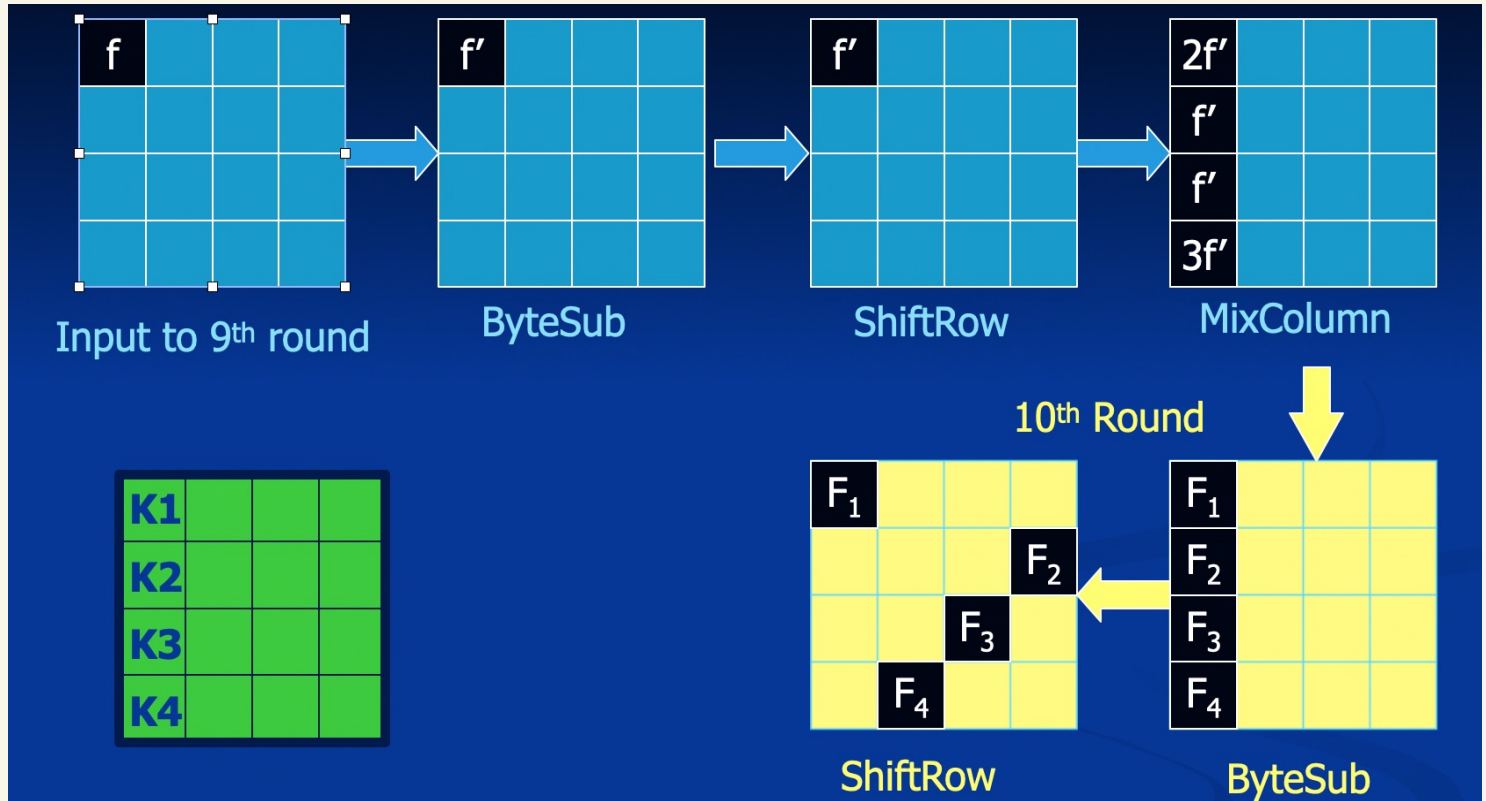## 2.2) Propagation of fault of the fault is injected at the input of 9th round.

2.3) How does location of fault injection affect the propagation of fault?

For a byte fault attack:

-> As in byte fault attack the fault is injected at the beginning of the 9th round, we have 7 operations: subByte, shiftrow, mix column, add round key rk9, subByte, shfitrow and add round key rk10.

-> unlike bit fault attack, 4 bytes are affected by the end of 10th round as seen on previous page.

-> This is mainly due to mix column which affects 4 bytes on its output. Having

Example of mix column: