AES [Advanced Encryption Standard]
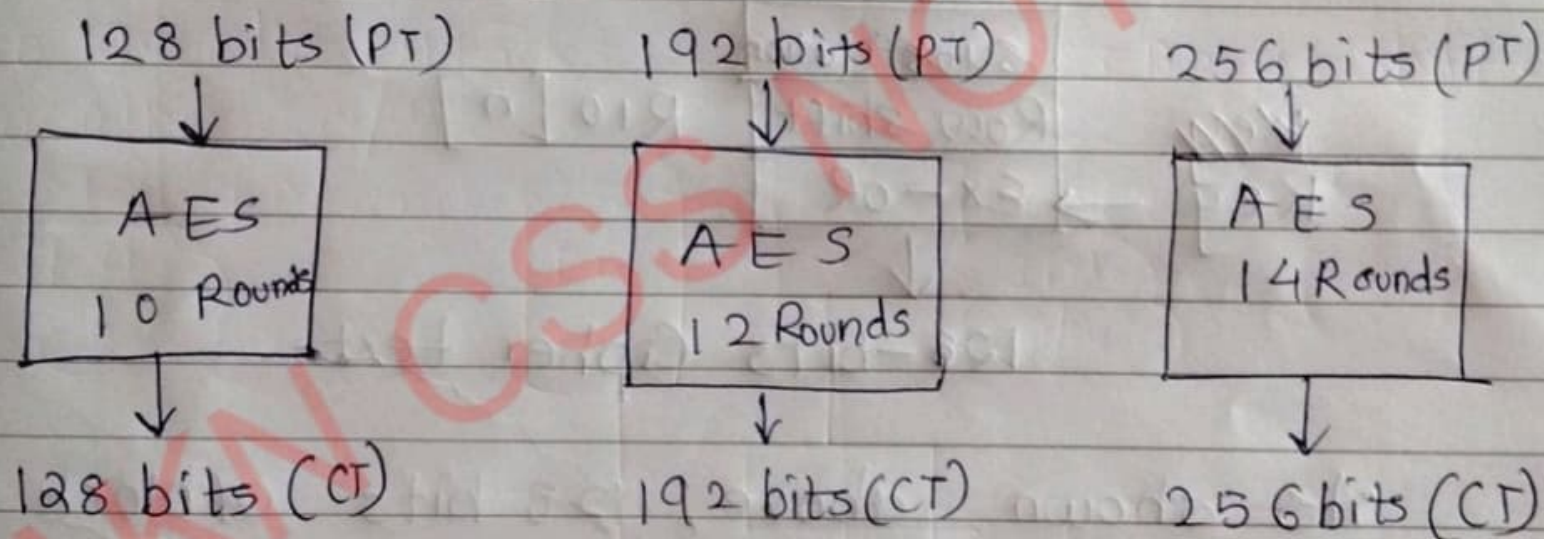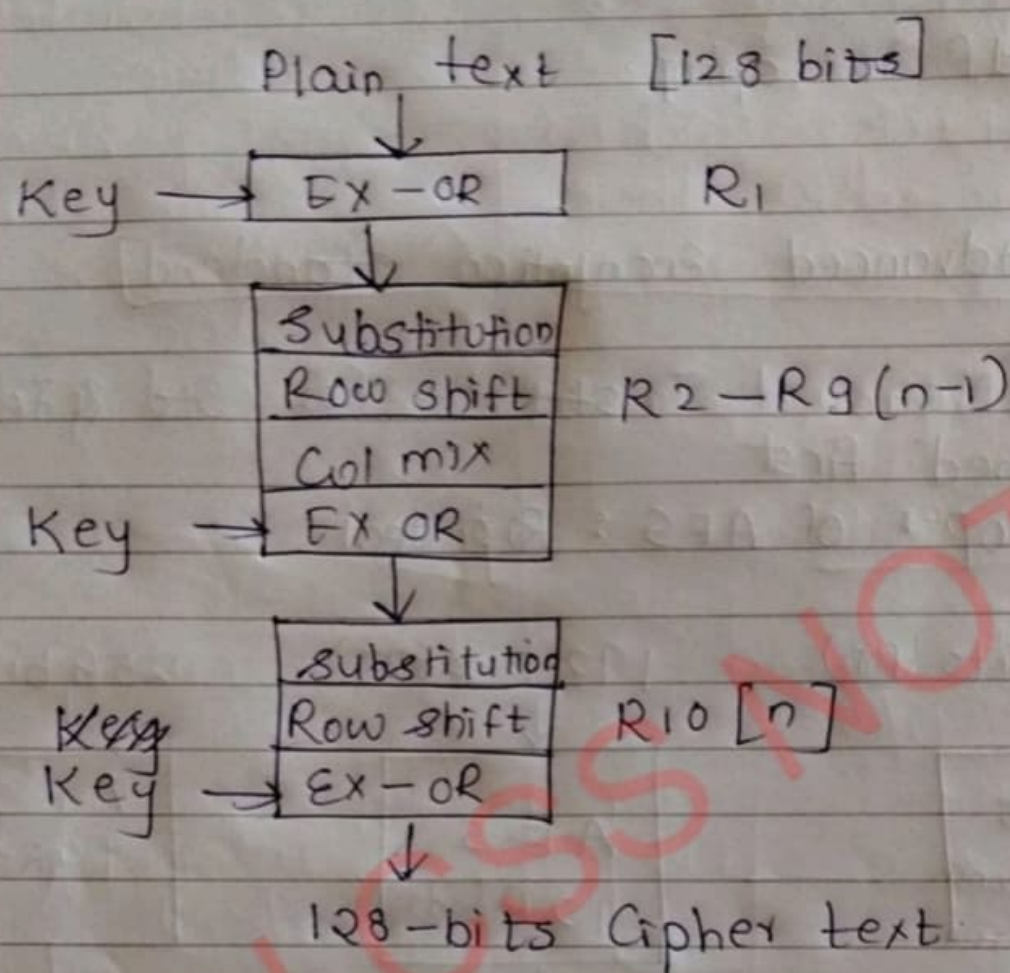
→ NIST [National Institute for Std & Tech.] published first.

→ Developer of AES : Rigndeal

128 bits (PT)	192 bits (PT)	256 bits (PT)
↓	↓	↓
AES 10 Rounds	AES 12 Rounds	AES 14 Rounds
↓	↓	↓
128 bits (CT)	192 bits (CT)	256 bits (CT)

#

→ Block Diag:-

Plain text [128 bits]

Key → | EX - OR | R1

| Substitution |
| Row shift | R2 — R9 (n-1)
| Col mix |
Key → | EX OR |

| Substitution |
Key | Row shift | R10 [n]
Key → | EX - OR |

128 - bits Cipher text

- As shown above, 128 bits of block of Plain Text in Round 1 EX-OR with key
- From Round 2 - 9, 128 bits block will be mapped to 4×4 state Array ¿At a time 16 bits? will be processed with substitution, row shift & mixing of col elements, when all 128 bits are processed they will be EXORed with key.
- For last round only column mixing is skipped.