**Lez3 14/11/2024**

**Crittografia Simmetrica**

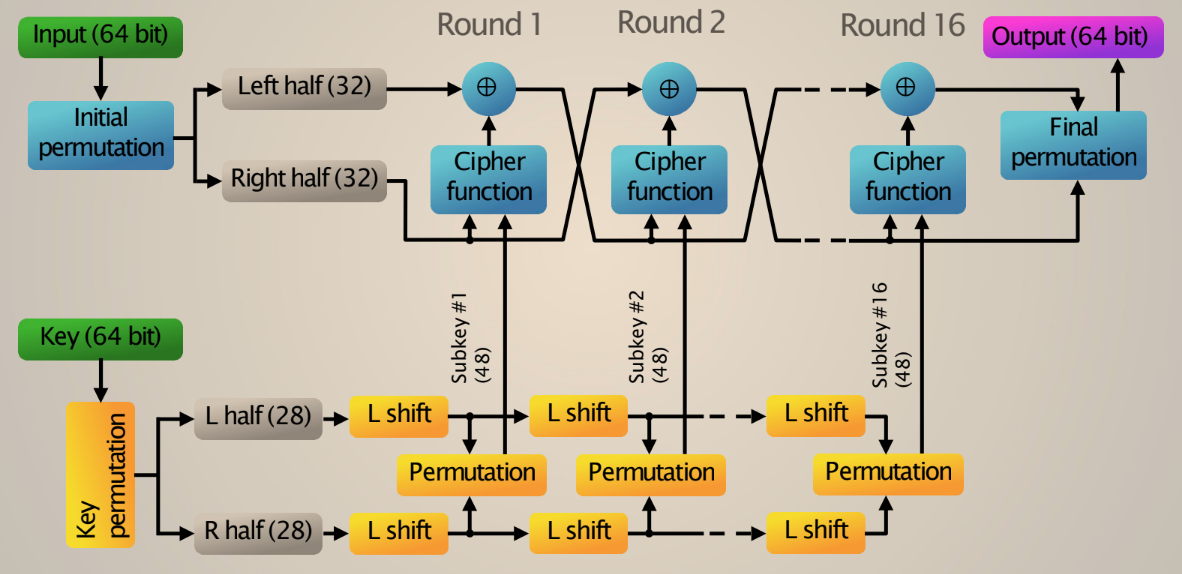
fa uso chiave sia per cifratura che decifratura (detta anche a chiave privata)

usata ancora oggi con algoritmo AES, deriva da

**DES: Data Encryption Standard,** è una cifratura a round(11 o 16), usata anche in cifrature hash

caratteristica: input e output hanno stessa lunghezza (in es 64 bit),   
msg + lungo = rifare ciclo + volte

*slide procedura*



**DES** rientra nella **Cifratura a blocchi:** Algoritmo che prende in ingresso una stringa di lunghezza fissa di testo in chiaro e la trasforma, con una serie di operazioni complesse, in una stringa di testo cifrato della stessa lunghezza.

(fine anni 90, msg criptabile con des, abbastanza veloce, molto rapida rottura)

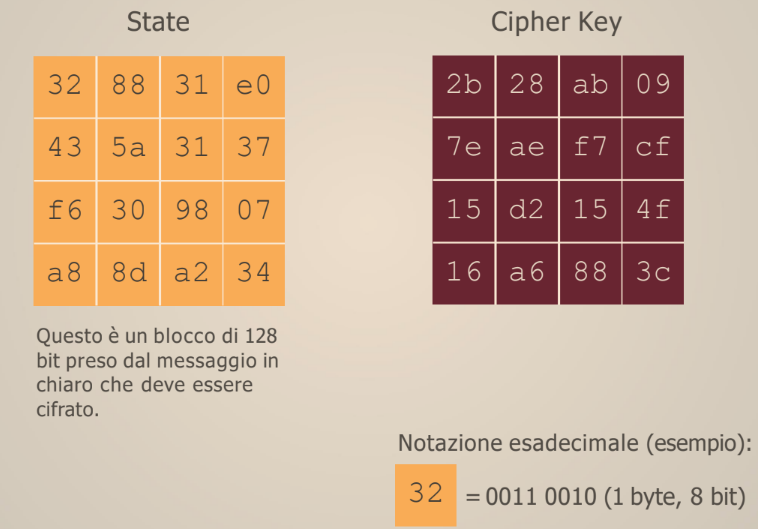
nascita di **AES: Advanced Encryption Standard**

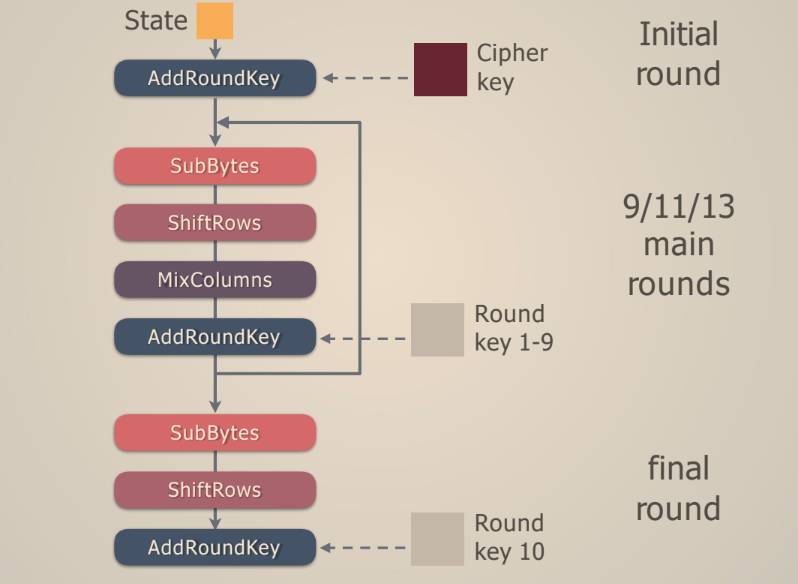
richieste: efficienza, consente cifrare msg più lunghi, chiavi più lunghe

cosa ricorda des? numero di round, inserimento messaggio e chiave(?)

(pag successiva input gestito e processo per il messaggio

per la chiave pagina ulteriormente successiva alla prossima)





procedura spiegazione dei passaggi subBytes, shiftrows, mixcolumns, addroundkey

AES usata ancora oggi, forzatura ma ridotta vulnerabilità all’aumento dei round

fare appunti 4ta slide

doppio lock

roba di diffie-hellmann metodo dei colori