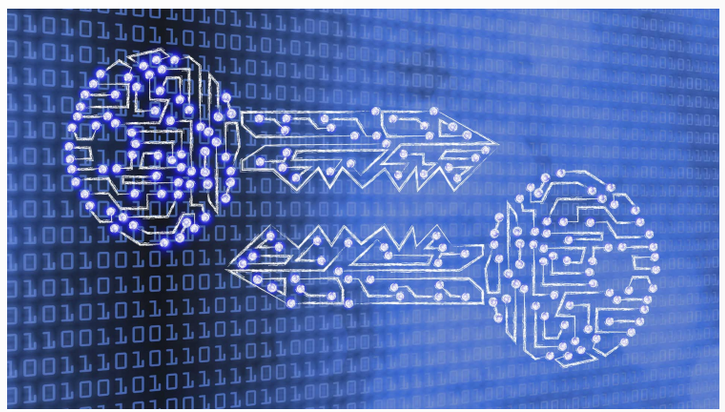
La crittografia simmetrica

Milani Francesco 5AI

Introduzione alla crittografia

La crittografia è la branca della crittologia che tratta delle “scritture nascoste”, ovvero dei metodi per rendere un messaggio “offuscato”, in modo da non essere comprensibile a persone non autorizzate a leggerlo.



Consente di:

- Identificare un utente;
- Autenticare un messaggio;
- Firmare digitalmente un messaggio;

Due processi principali:

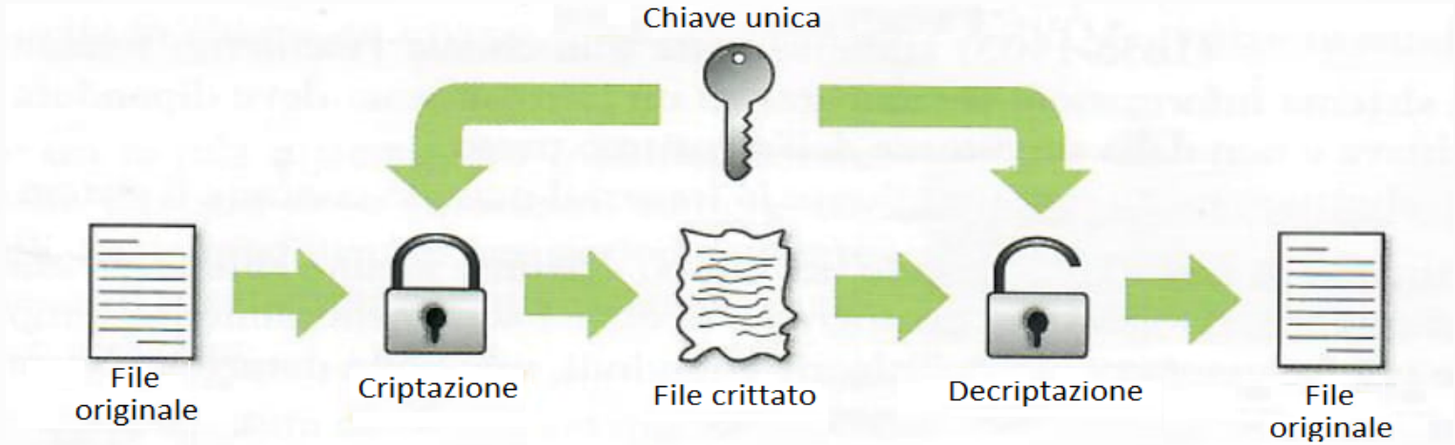
- cifratura: processo attraverso il quale un messaggio viene reso incomprensibile;
- decifratura: processo inverso della cifratura, attraverso il quale un messaggio cifrato viene reso comprensibile.

Regola di cifratura:

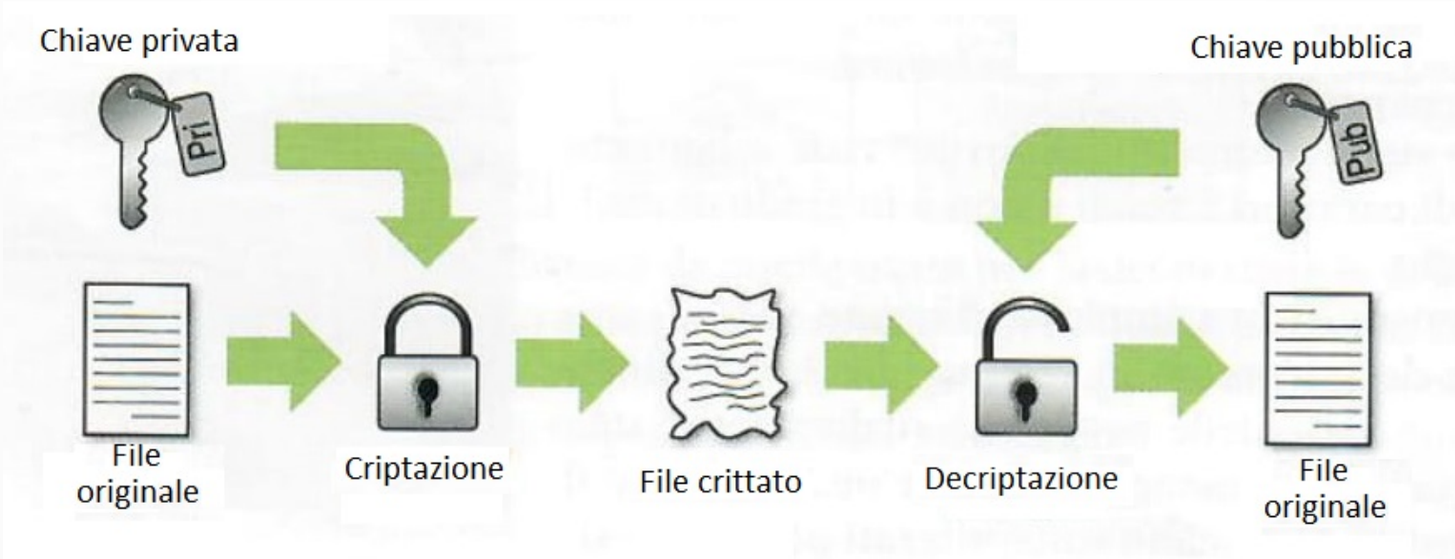
- regola vera e propria → algoritmo di criptazione
- parametri → chiave

Schemi crittografici:

- chiave di criptazione uguale a chiave di decriptazione → schema simmetrico



- chiave di criptazione diversa a chiave di decriptazione → schema asimmetrico



Crittoanalisi

La crittoanalisi è lo studio dei metodi per ottenere il significato di informazioni cifrate, senza aver accesso diretto all'informazione stessa.

Principio di Kerchoffs:

- La chiave è l'elemento fondamentale

Corollario di Shannon:

- "Il nemico conosce il sistema"

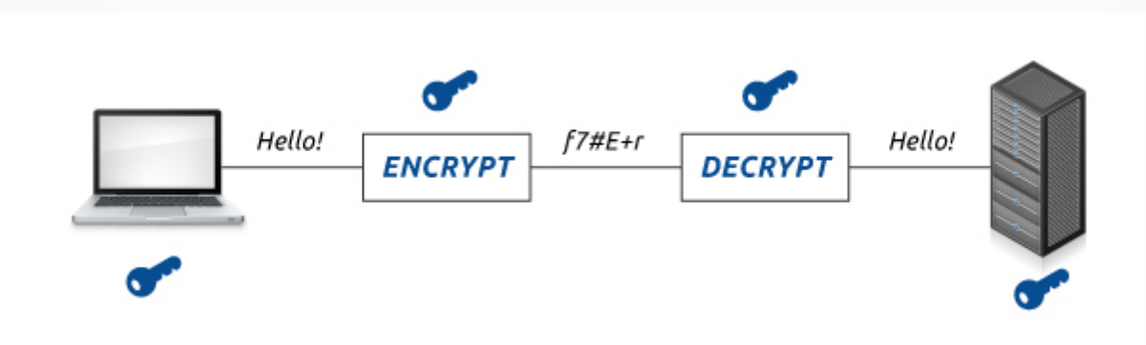
Proprietà fondamentali di Shannon:

- Confusione

- Diffusione

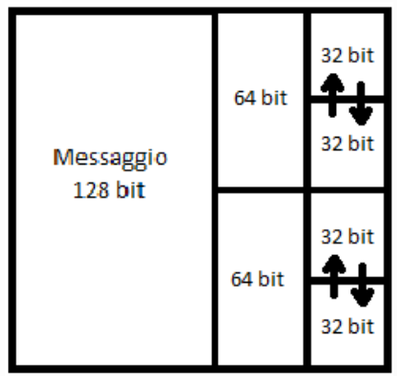
Cifrari a chiave simmetrica

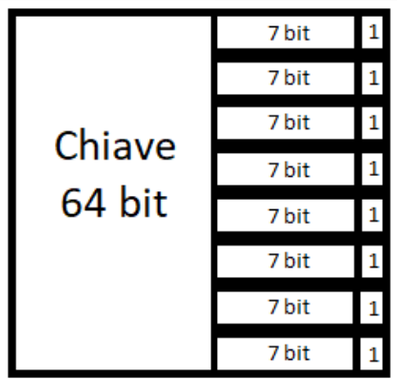
- DES
  - 1976
  - Horst Feisel
- 3-DES
  - 1999
  - IBM
- IDEA
  - 1991
  - Xuejja Lai – James L. Massey
- AES
  - 1997
  - Vincent Rijmen – Joan Daemen



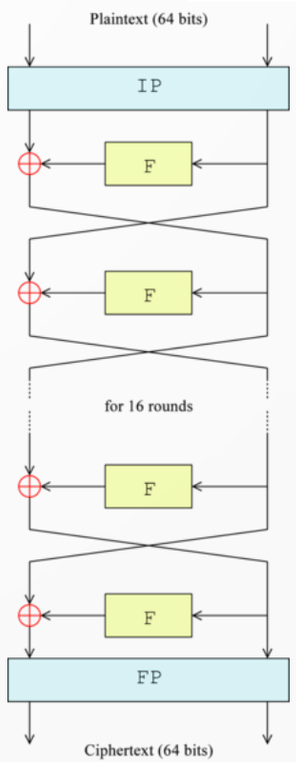
DES – Data Encryption Standard

- Cifrario a blocchi
- Chiave segreta a 64 bit: - 8 controllo di parità
  - 56 utili
- Messaggio: - diviso in blocchi da 8 byte
  - codifica in ASCII di ogni blocco, per ottenere blocchi da 64 bit





- Struttura dell'algoritmo : - Permutazione iniziale
  - Divisione dei blocchi in due metà di 32 bit processati in maniera alternata → "rete di Feistel"
  - Applicazione della funzione Feistel per 16 round consecutivi
  - Permutazione finale

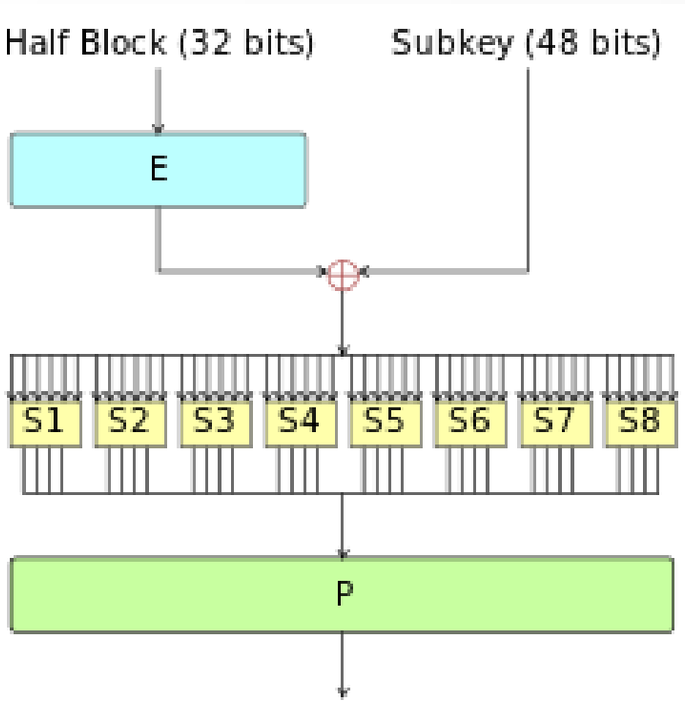


DES – Data Encryption Standard

Funzione Feistel

Consiste di 4 passi:

- Espansione
- Miscelazione con la chiave
- Sostituzione
- Permutazione o Trasposizione



Funzione creata rispettando i principi di Claude Shennon:

- Espansioni, miscelazioni, sostituzioni e permutazioni forniscono una “confusione” del messaggio con la chiave, quindi scarsamente attaccabile attraverso crittoanalisi.

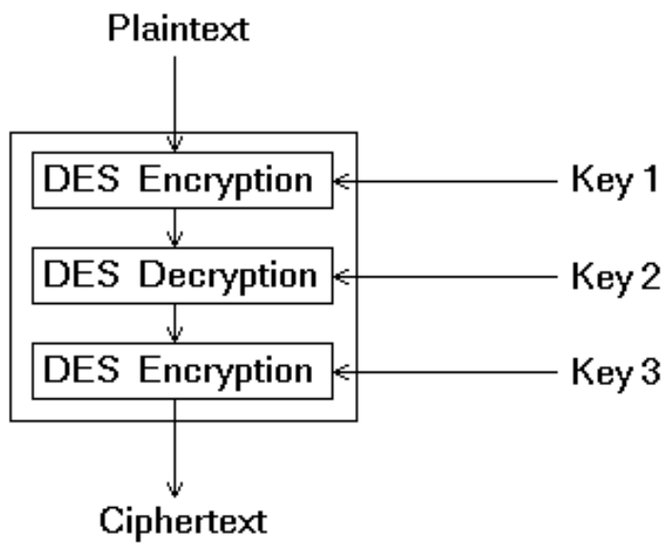
3-DES – Triple DES

- Cifrario a blocchi
- Introdotto per sostituire il DES non più sicuro
- Composto da 3 passi di cifratura DES consecutivi

- Utilizza 3 chiavi: - 168 bit utili

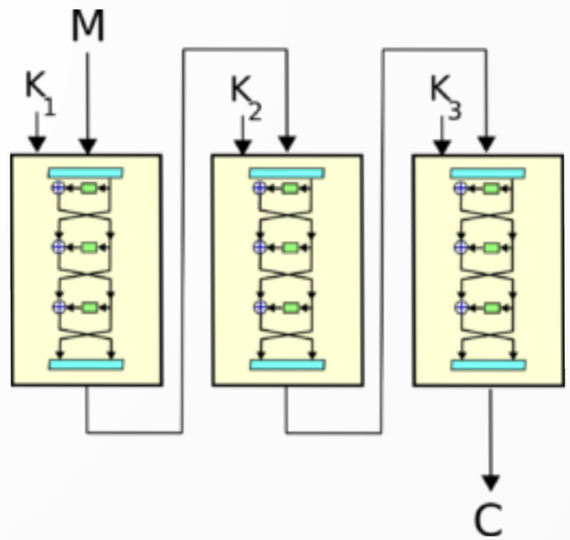
  - 24 bit di controllo

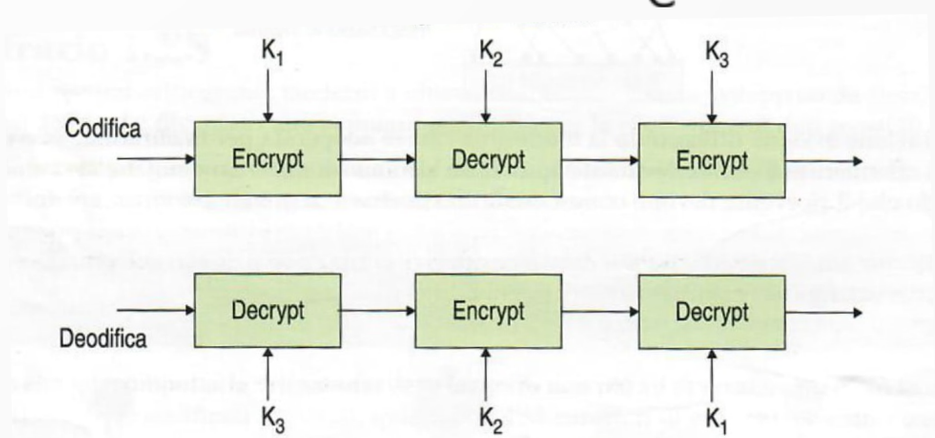
- Migliore rispetto al DES per la lunghezza tripla della chiave
- Compatibile con DES normale



3-DES – Triple DES

- Struttura dell'algoritmo: - Cifrazione con la prima chiave
  - Decifrazione con la seconda chiave
  - Cifrazione con la terza chiave
- La decifrazione viene eseguita per poter essere compatibile con DES
- 3 combinazioni di chiavi: - k1, k2, k3 diverse
  - k1 = k3, k2 diversa (112 bit di sicurezza)
  - k1 = k2 = k3 (solo per DES)





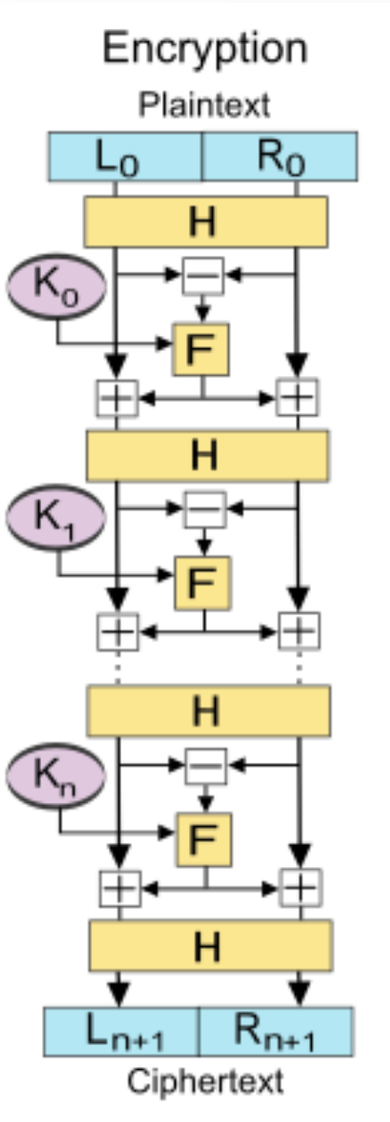
IDEA – International Data Encryption Algorithm

- Cifrario a blocchi
- Introdotto per sostituire il DES non più sicuro

- Simile al DES : - Chiave a 128 bit

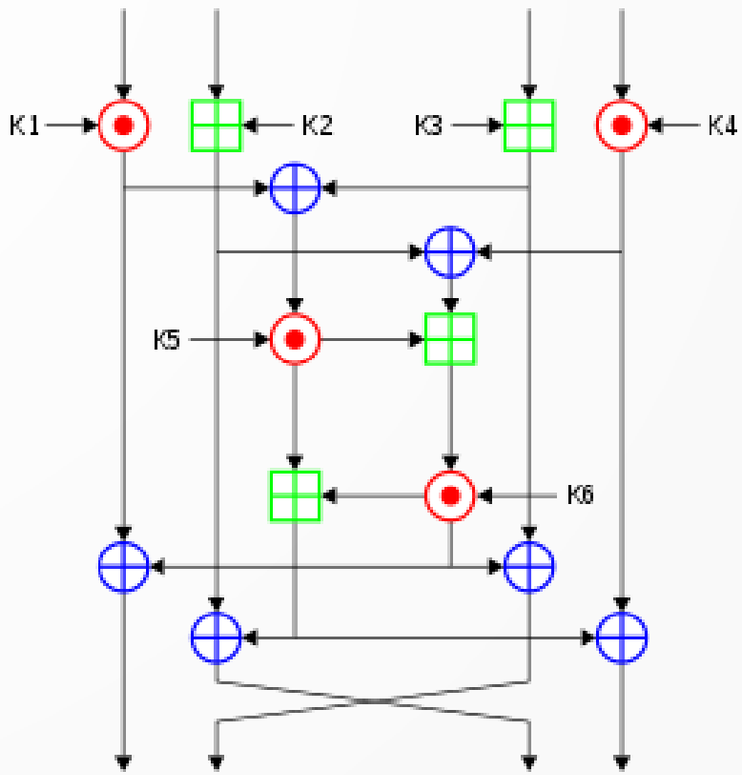
  - Messaggio diviso in blocchi da 64 bit

- Cifrario a chiave segreta più utilizzato nei software commerciali di crittografia, per la sua velocità e sicurezza



IDEA – International Data Encryption Algorithm

- Chiave: - 128 bit divisi in 8 sottochiavi da 16 bit
- Messaggio: - 64 bit divisi in 4 blocchi da 16 bit
- Struttura dell'algoritmo: - Serie di 8 round durante i quali si eseguono combinazioni di tre operazioni su numeri a 16 bit

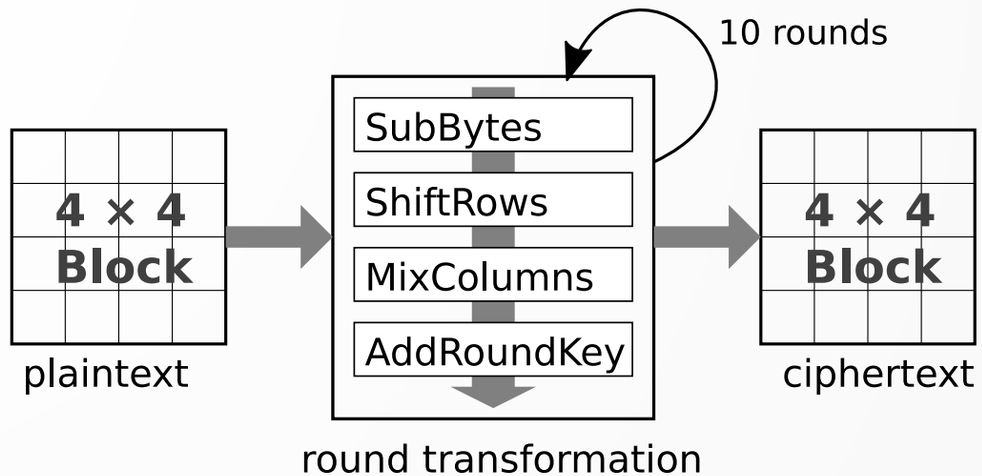


- Operazioni eseguite: - XOR (oppure OR esclusivo)
  - Addizione senza riporto modulo 2^{16}
  - Moltiplicazione modulo $2^{16}+1$
- Rotazione della chiave: - Chiave divisa in 16 bit ad ogni passaggio
  - Utilizzo di 6 chiavi, quindi di 96 bit dei 128 totali
  - Dopo ogni passaggio viene ruotata di 25 bit a sinistra, riprendendo i primi 6 blocchi di 16 bit

AES – Advanced Encryption Standard

- Cifrario a blocchi
- Standard USA
- Progettato sulla base di tre caratteristiche: - resistenza
  - velocità e compattezza
  - semplicità progettuale
- Creato per il concorso indetto dal NIST

  per la sostituzione del DES come standard



Valutato dal NIST secondo due giudizi:

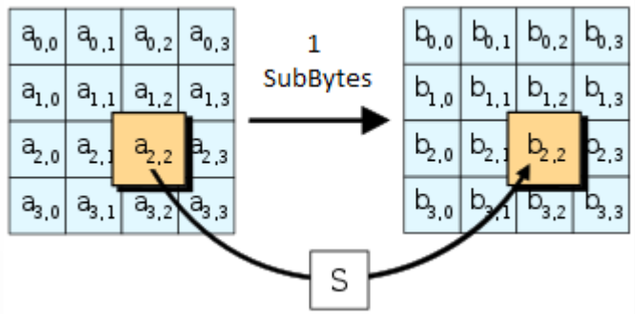
- Prima valutazione: - sicurezza
  - costo
  - caratteristiche dell'algoritmo
  - caratteristiche dell'implementazione
- Seconda valutazione: - sicurezza generale
  - implementazioni software
  - ambienti con spazio limitato
  - crittografia e decrittografia
  - agilità della chiave
  - versatilità e flessibilità
  - potenzialità di sfruttamento del parallelismo

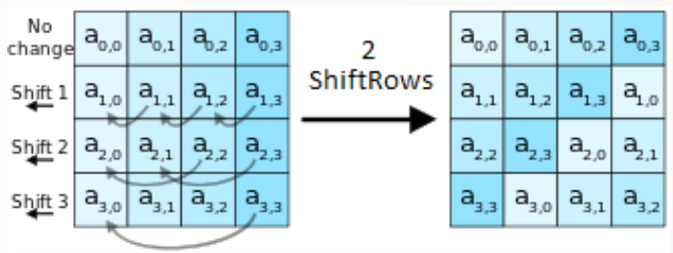
AES – Advanced Encryption Standard

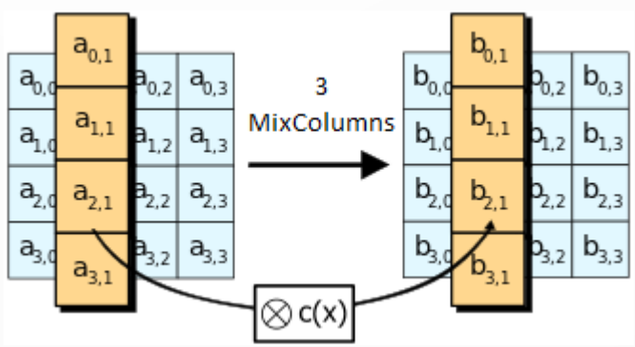
- Messaggio: diviso in blocchi da 128 bit
- Chiave: può essere di 128, 192 o 256 bit
- Matrici 4x4 chiamate “stati” quando la chiave è a 128 bit.

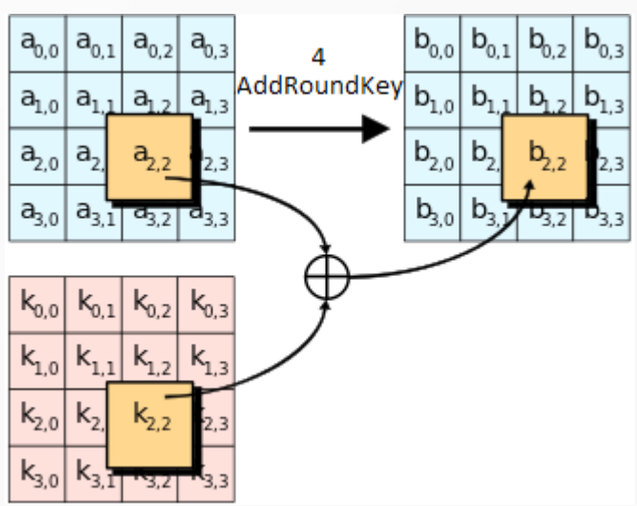
Struttura dell’algoritmo:

- Passaggio iniziale: - Add Round Key
- 10 round composti da 4 operazioni: - Substitute Bytes
  - Shift Rows
  - Mix Columns
  - Add Round Key
- L’ultimo round salta il passaggio Mix Columns









-

Vantaggi e svantaggi degli algoritmi simmetrici

Vantaggi

- Velocità di esecuzione
- Potenza di calcolo bassa

Svantaggi

- Distribuzione della chiave

I sistemi a cifratura asimmetrica sono molto più lenti e richiedono una potenza di calcolo maggiore a causa delle chiavi più lunghe

I sistemi a cifratura asimmetrica sono superiori in quanto non è necessario concordare chiavi di cifratura