Principi di Shannon

Alla base di cifrari simmetrici come DES e AES:

diffusione il testo in chiaro si deve distribuire su tutto il crittogramma – idealmente ogni carattere del crittogramma deve dipendere da tutti i caratteri del blocco di messaggio.

confusione messaggio e chiave sono combinati in modo complesso per impedire di separare le due sequenze – ogni bit del crittogramma deve dipendere da tutti i bit della chiave(? OTP no).

One-Time Pad non rispetta la diffusione, ma è una realizzazione perfetta del principio di confusione. Oggi sono realizzati con l'impiego di trasformazioni non lineari.

Il principio di diffusione implica che piccoli cambiamenti nell'input da cifrare portano a grandi differenza nel crittogramma.