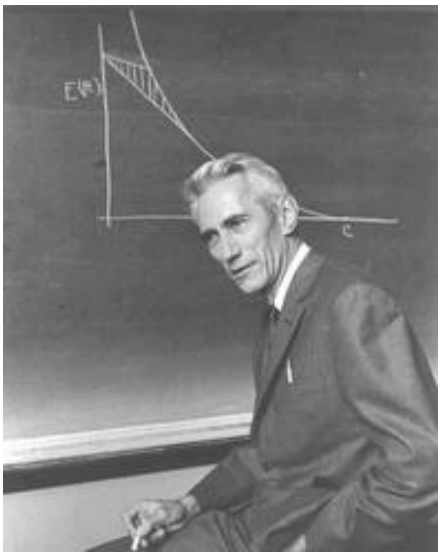
Communication Theory of Secrecy Systems

- nel 1949, Shannon pubblica *Communication Theory of Secrecy Systems*
- è un lavoro fondamentale per la crittografia moderna
- introduce numerosi concetti chiave
- definisce la **segretezza perfetta**



Claude Shannon

- consideriamo un crittosistema $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$
- su $\mathcal{P}$ è data una distribuzione di probabilità $\mathbf{Pr}_{\mathcal{P}}$
- anche su $\mathcal{K}$ è data una distribuzione di probabilità $\mathbf{Pr}_{\mathcal{K}}$
- la scelta della chiave è indipendente dalla scelta del plaintext
- questo induce una distribuzione di probabilità sullo spazio dei testi cifrati $\mathcal{C}$
- un crittosistema è a **segretezza perfetta** se $\forall x \in \mathcal{P}$ e $\forall y \in \mathcal{C}$

$$\mathbf{Pr}(x|y) = \mathbf{Pr}(x)$$

- cioè se la probabilità a posteriori che il testo in chiaro sia x, dato il testo cifrato y, è uguale alla probabilità a priori che il testo in chiaro sia x
- dallo studio del testo cifrato non si ottiene nessuna informazione sul testo in chiaro!