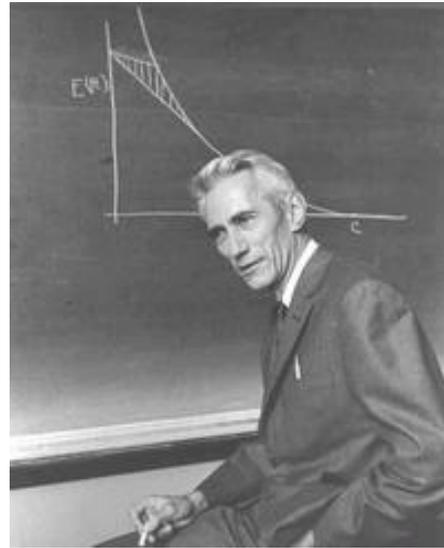


Communication Theory of Secrecy Systems

- 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 $\Pr_{\mathcal{P}}$
- anche su \mathcal{K} è data una distribuzione di probabilità $\Pr_{\mathcal{K}}$
- 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 $\forall y \in \mathcal{C}$

$$\Pr(x|y) = \Pr(x)$$

- 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!

esempio

- $\mathcal{K} = \mathcal{C} = \mathcal{P} = \mathbb{Z}_2^2$
- $e_k(x) = x \oplus k$, $d_k(y) = y \oplus k$, $\oplus = \text{XOR}$
- su \mathcal{K} , distribuzione uniforme; $\Pr(k) = \frac{1}{4} \forall k \in \mathcal{K}$
- su \mathcal{P} , sia $\Pr(00) = \Pr(11) = \frac{1}{6}$, e $\Pr(10) = \Pr(01) = \frac{1}{3}$
- si può vedere che la distribuzione indotta su \mathcal{C} è uniforme
- e che $\Pr(y|x) = \frac{1}{4} \forall x \in \mathcal{P}$ e $\forall y \in \mathcal{C}$
- dal teorema di Bayes, si ha allora

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

- il crittosistema è a segretezza perfetta (di fatto, per ogni ddp su \mathcal{P})

- se il CS è a segretezza perfetta, $\Pr(x|y) = \Pr(x)$
- dal teorema di Bayes,
 $\Pr(x|y) = \Pr(x) \iff \Pr(y|x) = \Pr(y)$
- $\forall y, \Pr(y|x) = \Pr(y) > 0$
- questo dice che, fissato x , $\forall y \in \mathcal{C}$ c'è una chiave $k \in \mathcal{K}$ tale che $e_k(x) = y$
- il numero di chiavi è maggiore o uguale al numero dei CT

$$|\mathcal{K}| \geq |\mathcal{C}| \geq |\mathcal{P}|$$