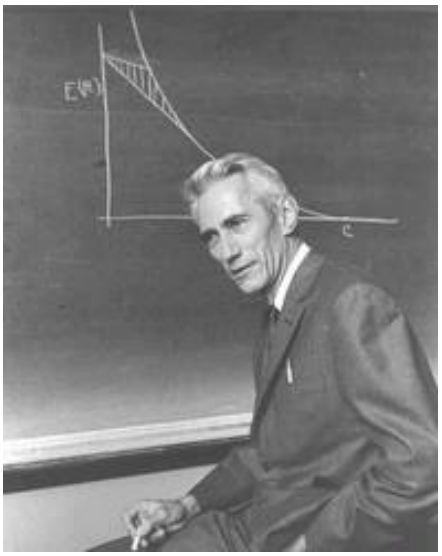
Communication Theory of Secrecy Systems

- 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!

esempio

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

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

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

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

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

- Teorema di Shannon
- nel caso in cui $|\mathcal{K}| = |\mathcal{C}| = |\mathcal{P}|$, un crittosistema è a segretezza perfetta se e solo se
  1. $\forall x \in \mathcal{P}\ \forall y \in \mathcal{C}$, $\exists!\ \ k \in \mathcal{K}$ tale che $e_k(x) = y$
  2. le chiavi sono scelte con probabilità uniforme (pari a $\frac{1}{|\mathcal{K}|}$)

one-time pad

- L'one-time pad o cifrario di Vernam (1917) è il crittosistema tale che
- $\mathcal{P} = \mathcal{C} = \mathcal{K} = (\mathbb{Z}_2)^m$
- se $k = (k_1, k_2, \ldots, k_m)$ si ha
  - $e_k(x_1, x_2, \ldots, x_m) = (x_1 + k_1, x_2 + k_2, \ldots, x_m + k_m)$
  - $d_k(y_1, y_2, \ldots, y_m) = (y_1 - k_1, y_2 - k_2, \ldots, y_m - k_m) = (y_1 + k_1, y_2 + k_2, \ldots, y_m + k_m)$
- è un crittosistema a segretezza perfetta

one-time pad

- Vantaggi:
  - Cifratura e decifratura molto semplici da calcolare.
  - A segretezza perfetta.
- Svantaggi:
  - La chiave è lunga quanto il testo in chiaro.
  - La chiave può essere usata una sola volta.
  - Si ha il problema di distribuire e conservare in modo sicuro le chiavi.