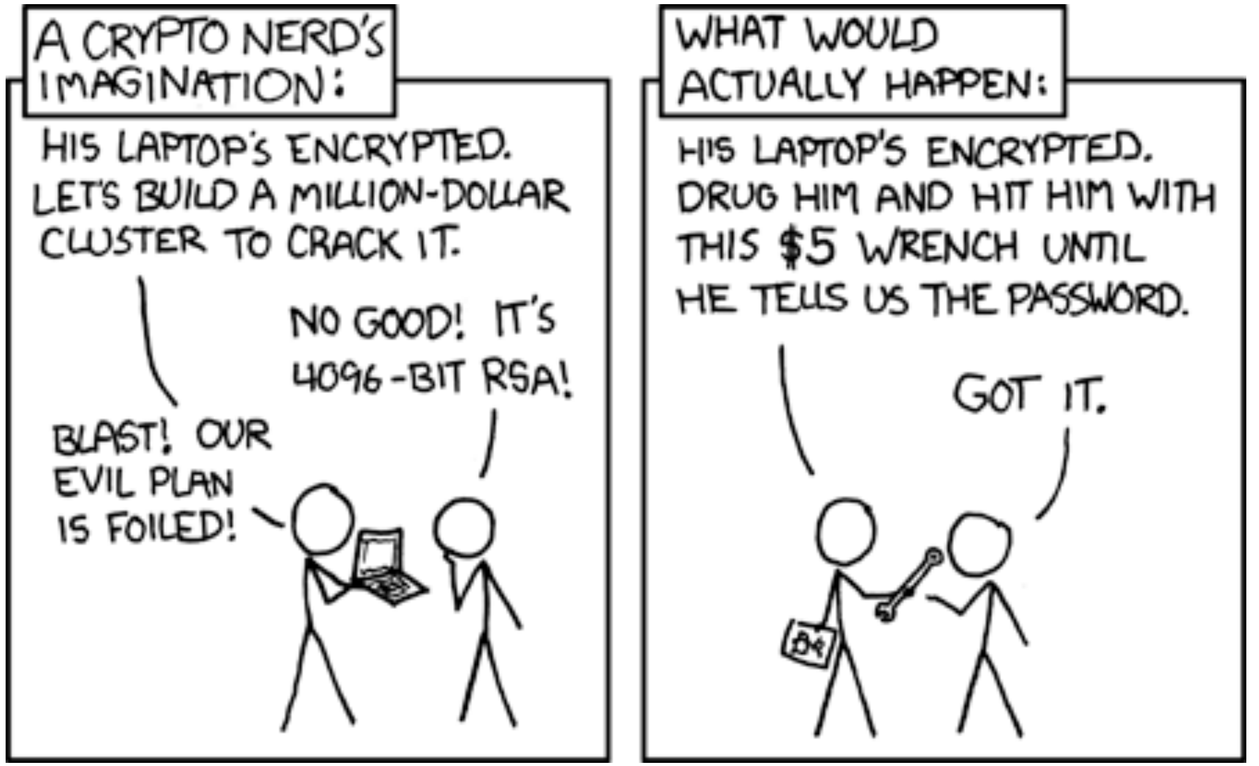
Crypto moderne



https://xkcd.com/538/

Schéma de chiffrement

Définition

- Un schéma de chiffrement Π est défini par un tuple $(\mathscr{P}, \mathscr{C}, \mathscr{K}, \mathscr{E}, \mathscr{D})$ où
  - $\mathscr{P}$ l'espace des messages clairs
  - $\mathscr{C}$ l'espace des cryptogrammes
  - $\mathscr{K}$ l'espace des clés
  - $\mathscr{E} = \{E_k \mid k \in \mathscr{K}\}$avec $E_k : \mathscr{P} \to \mathscr{C}$ fonctions de chiffrement
  - $\mathscr{D} = \{D_k \mid k \in \mathscr{K}\}$avec $D_k : \mathscr{C} \to \mathscr{P}$ fonctions de déchiffrement
- On demande que $\forall k \in \mathscr{K}, \forall m \in \mathscr{M} : D_k(E_k(m)) = m$