RSA

Chiffrement homomorphe

- Habituellement le chiffrement n'est utile qu'en transit ou au repos
  - Pour utiliser l'information il faut la déchiffrer
- La notion de **privacy homomorphism** remet en question cette certitude
- Si on connait une relation entre les espaces de messages clairs et chiffrés
  - On peut effectuer des calcul **en aveugle** sur les cryptogrammes, sans les déchiffrer

RSA

Chiffrement homomorphe

- Par exemple, le produit de chiffrés RSA est un homomorphisme multiplicatif

$$\begin{aligned} Enc(m_1) \times Enc(m_2) &= m_1^e \times m_2^e \mod n \\ &= (m_1 \times m_2)^e \mod n \\ &= Enc(m_1 \times m_2) \end{aligned}$$

- $\Longrightarrow$ On peut faire faire une multiplication de deux nombres secrets en aveugle par quelqu'un d'autre sans lui révéler les nombres

- Pas si révolutionnaire en soi mais ça a lancé un nouveau domaine de recherche