RSA

Chiffrement et déchiffrement

$$n = pq$$

$$ed \equiv 1 \pmod{\varphi(n)}$$

$$Enc(m) = m^e \mod n$$

$$Dec(c) = c^d \mod n$$

$$\begin{aligned} Dec(Enc(m)) &= m^{ed} \mod n \\ &= m^{k\varphi(n)+1} \mod n \\ &= m \mod n \end{aligned}$$

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