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

Conclusion

- La version présentée (appelée “textbook” RSA) n’est pas sûre
  - Beaucoup de détails passés sous le tapis nécessaire à la sécurité
  - Optimisations non mentionnées pour rendre le schéma plus performant en pratique
- Le chiffrement asymétrique moderne est souvent basé sur la méthode de Diffie-Hellman implémenté sur les courbes elliptiques
- Dans TLS, RSA est utilisé pour la signature de certificat et l’échange de clé symétrique
- OpenSSH supporte les clé RSA pour l’authentification et l’échange de clé symétrique
  - Était le protocole par défaut jusqu’à la version 9.5 (2023-10-04)