RSA

Historique

- Inventé par Rivest, Shamir et Adleman dans les années 70s
- Une des premières solutions au problème d'établissement de clé avec Diffie-Hellman
- Initialement présenté comme un algorithme de signature digitale
- Tous deux encore largement utilisés sur internet pour la communication https
- Rivest et Adleman ont aussi introduit le concept de privacy homomorphisms
- La sécurité repose sur la difficulté réputée de la factorization entière

RSA

Génération de clé

- Chiffrement asymétrique, on génère deux clés
  - Une **publique** (n, e) pour chiffrer / Une **privée** d pour déchiffrer
- On choisi deux grands nombres premiers $p, q \in \mathbb{Z}$ (par Miller-Rabin)
  - On calcule $n = pq$ et $\varphi(n) = (p-1)(q-1)$
  - On choisi un $e \in \mathbb{Z}^{\times}_{\varphi(n)}$ (i.e. $e \perp \varphi(n)$) et calcule son inverse $d \in \mathbb{Z}^{\times}_{\varphi(n)}$ (par Euclide)
- La sécurité dépend de la difficulté de retrouver $p, q, \varphi(n)$ étant donné seulement n, e