Man in the middle

- Le problème de DH est sa vulnérabilité à l’attaque de l’homme du milieu
- DSA règle ce problème
  - Assumant qu’Alice possède la clé publique de Bob
  - Bob peut émettre une nouvelle clé publique pour DH de manière vérifable

Références

- https://curves.xargs.org/
- https://fr.wikipedia.org/wiki/Courbe_elliptique
- https://doc.sagemath.org/html/en/reference/arithmetic_curves/index.html