Cryptographie Moderne

Hypothèses de calcul classique

- Factorisation entière (retrouver p, q étant donné $N = pq$)
  - RSA
- Logarithme discret (retrouver x étant donné $y = g^x$)
  - Diffie-Hellman (Corps finis ou Courbes elliptiques)
  - El Gamal
  - DSA

Cryptographie Moderne

Informatique quantique

- Algorithme de Grover
  - Accélère la fouille exhaustive contre les schémas symétriques $n \rightarrow \sqrt{n}$
  - On peut doubler la taille des clés
- Algorithme de Shor
  - Efficace pour factoriser ou trouver le log discret
  - Nécessite de nouveaux schémas basés sur d’autres problèmes