Crypto moderne

https://xkcd.com/1181/

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