アルゴリズムは秘密にするべきか?

- 昔の暗号と軍事目的の暗号
  - 限定されたグループ内で通信
  - アルゴリズムと鍵の両方が秘密
  - 標準化が困難
- これからの暗号
  - 不特定多数が通信
  - アルゴリズムは公開
  - 鍵は秘密
  - 標準化が容易