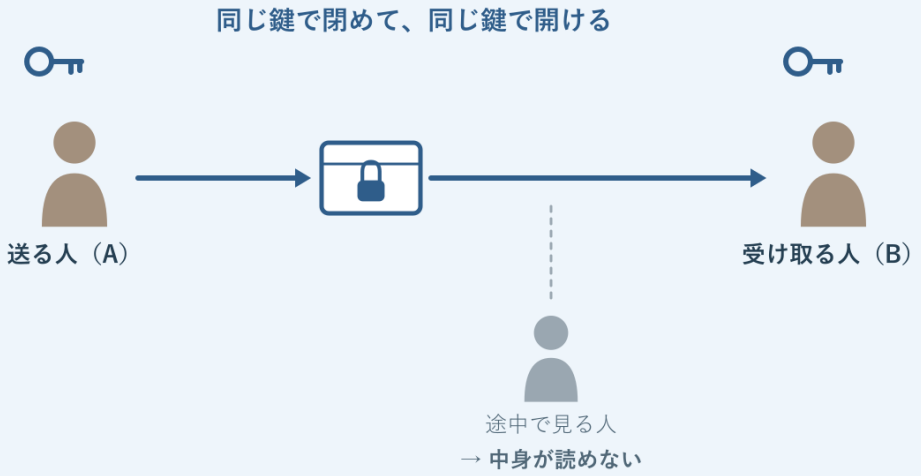
暗号化（共通鍵暗号と公開鍵暗号）

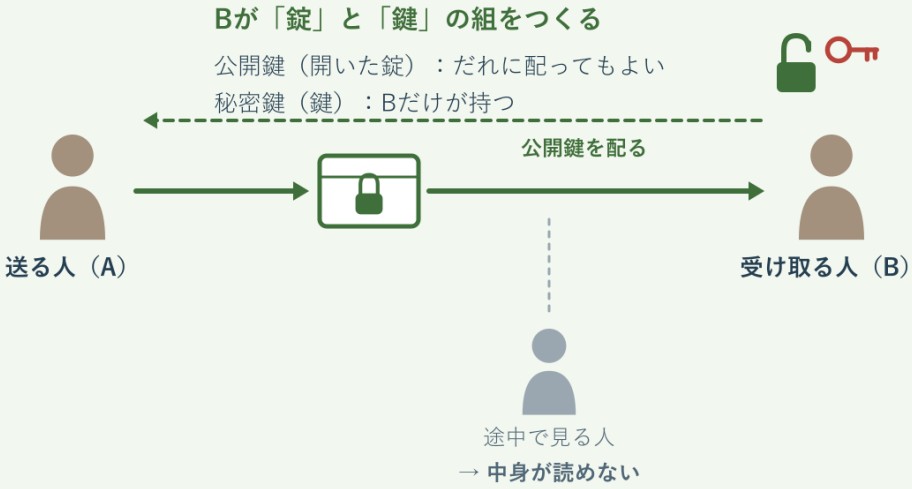
通信の途中で見られても、中身を読まれないようにするには、どうすればよいだろう

共通鍵暗号



◎ しくみが単純で、速く暗号化できる
△ 鍵を、相手に安全に渡すのがむずかしい
△ 相手ごとに、別の鍵が必要になる

公開鍵暗号



AはBの公開鍵で閉める → Bの秘密鍵でしか開かない
◎ 鍵を事前に渡さなくてよい
△ 計算に時間がかかる

実際の通信では、組み合わせて使う

公開鍵暗号で「共通鍵」を安全に渡し、本文は速い共通鍵暗号で暗号化する（Webの暗号化通信など）。

暗号化しても、相手が本物かどうかは別に確かめる必要がある → デジタル署名・デジタル証明書。

この図の「錠」と「鍵」はたとえ。実際の鍵は、とても大きな数でできている。

※ 模式図。錠と鍵のたとえで示した。