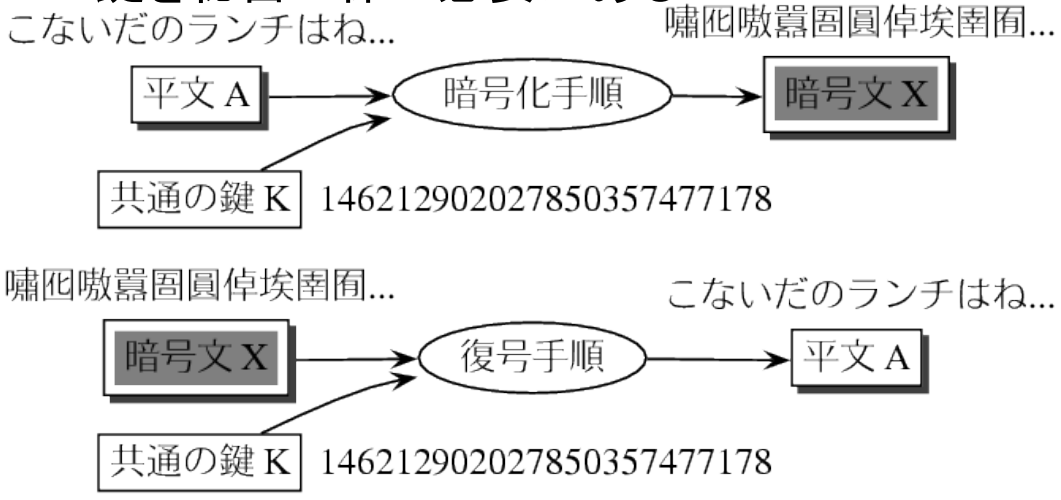
暗号

- 平文：元のデータ。第三者に読まれたくないもの
  - 「明日のランチはね…」
- 暗号文：変換後のデータ。盗聴されても平文を(簡単には)取り出せない。
  - 「嘯囮噉囂圄圓倬埃圉囿…」
- 暗号化：平文から暗号文を作成すること
- 復号：暗号文から平文を取り出すこと
- 鍵：暗号化や復号の際に用いられるデータ

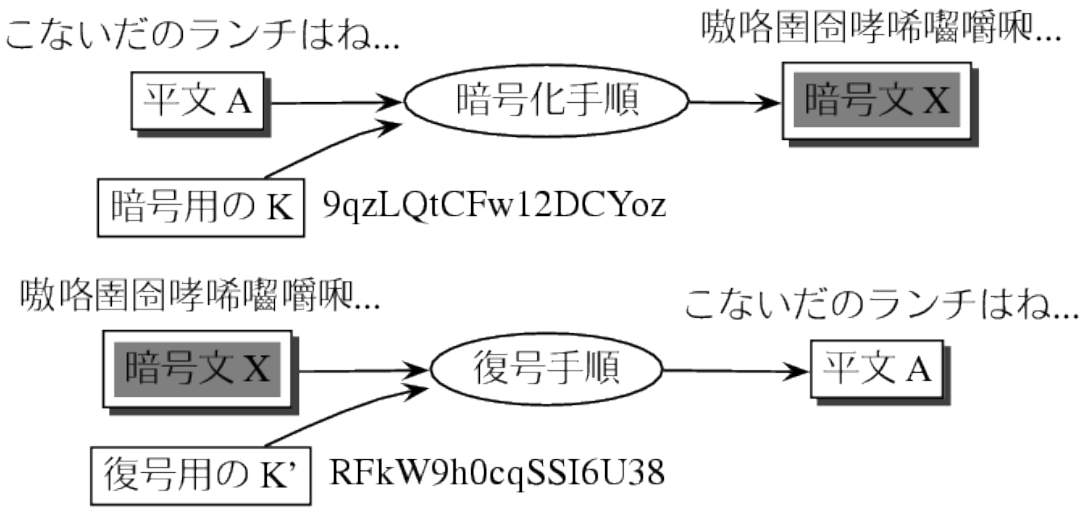
共通鍵暗号

- 一つの鍵で暗号化と復号化の両方を行うモデル
  - 鍵を秘密に保つ必要がある

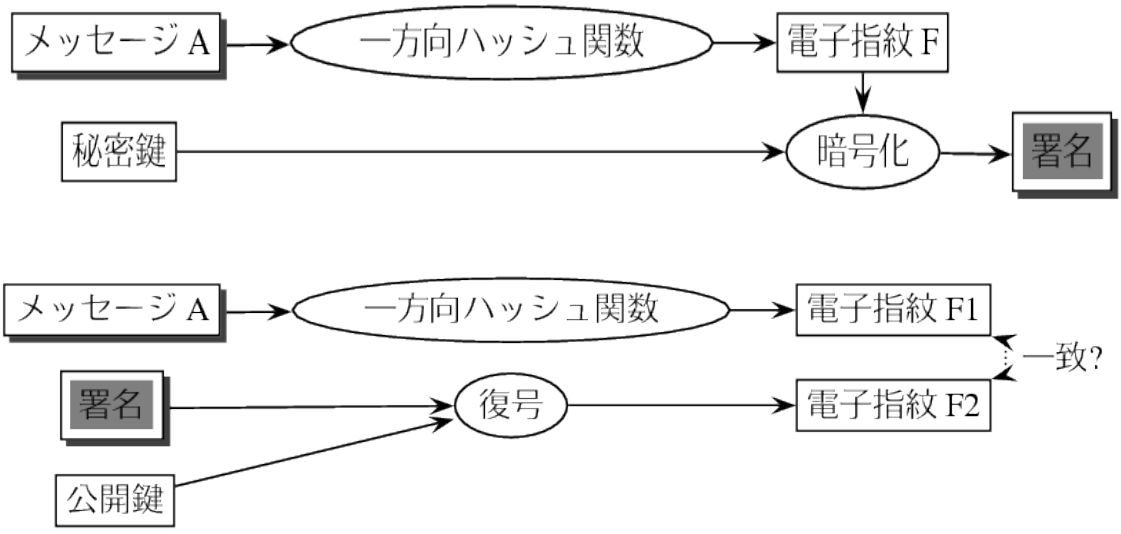


公開鍵暗号

↘ 暗号化の鍵を公開し，復号化の鍵を秘密にする方法



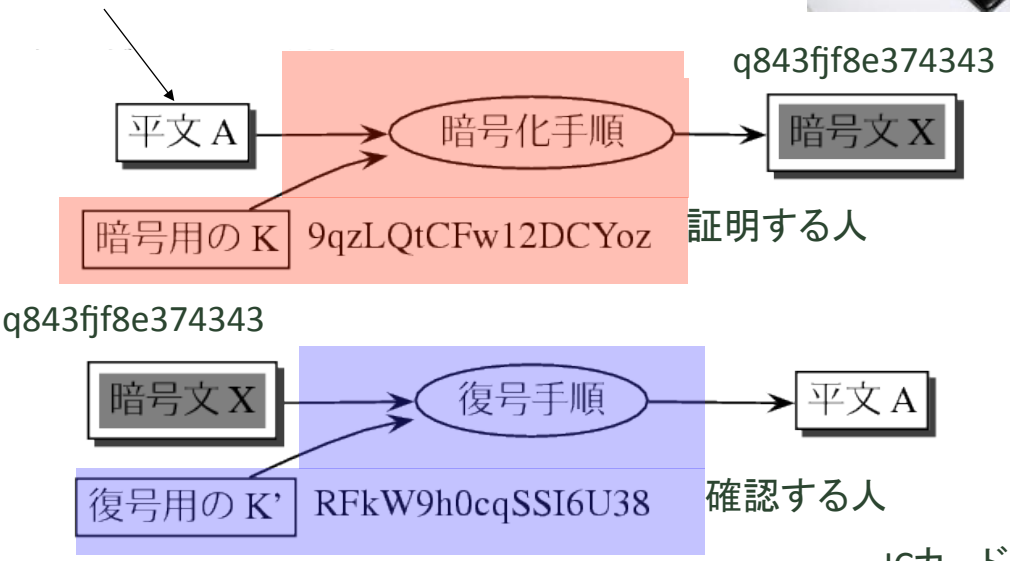
デジタル署名と検証



- 鍵を渡さずに鍵を持っていることを証明する

チャレンジ・レスポンス

確認する人がランダムに選ぶ



ICカード学生証

配布不可