暗号化・復号，鍵について

[コンピュータ基礎Ⅰ]

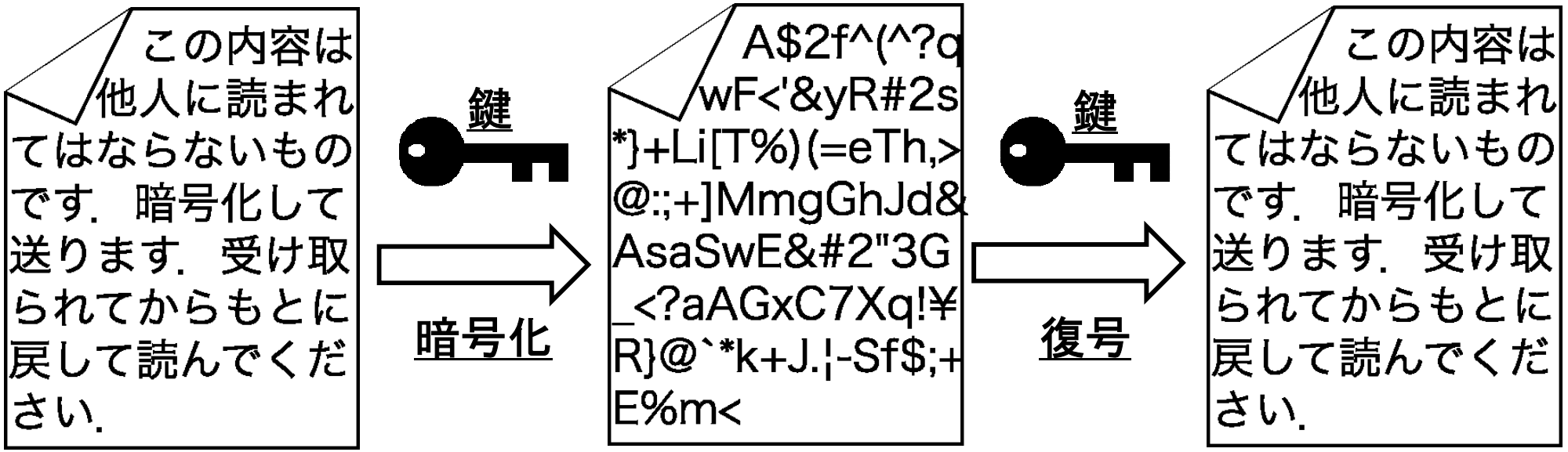
中村勝則

武庫川女子大学

暗号化技術

■ 通信内容を「スクランブル」する

- 内容を盗み見られても安全



元の内容
「平文」

暗号文

元の内容
「平文」

※「鍵」の中身は特殊なデータ

「共通鍵暗号」と「公開鍵暗号」

■ 基本：

- データの秘密を守りたい人が鍵を作成して，自分と通信相手だけが保持する

■ 共通鍵暗号方式　（鍵は1つ）

- 鍵は厳重に管理しなければならない！
  - ◆鍵が他人の手に渡ると大事な内容が解読されてしまう！

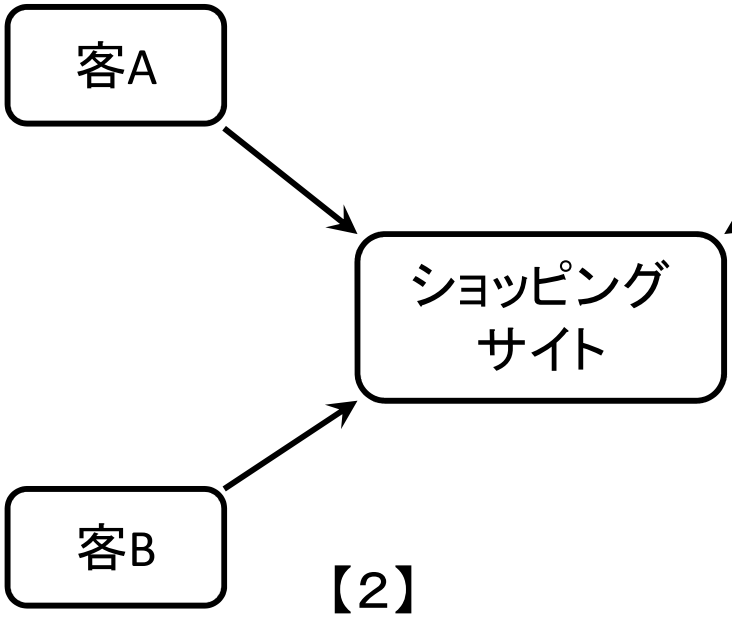
■ 公開鍵暗号方式　（鍵は2種類）

- スクランブルするための鍵1と，元に戻す鍵2が別のもの
- 1方を通信相手に渡し（公開鍵），もう片方を自分が厳重に管理する（秘密鍵）

公開鍵暗号方式

■ 応用例:

- 多数の人が個人情報を信頼できる団体に送信するためのセキュリティ
- 不特定多数の客が，個人情報をショッピングサイトに送信する場合に公開鍵暗号が利用される



【1】
個人情報は，ショッピングサイトが
配布する公開鍵で暗号化されて
送信される

【2】
個人情報を受け取ったショッピングサイトは
社内だけで管理される秘密鍵を用いてそれを
復元する