TLS: Transport Layer Security

(a.k.a.: Secure Sockets Layer (SSL))

Network Security
総合情報学科

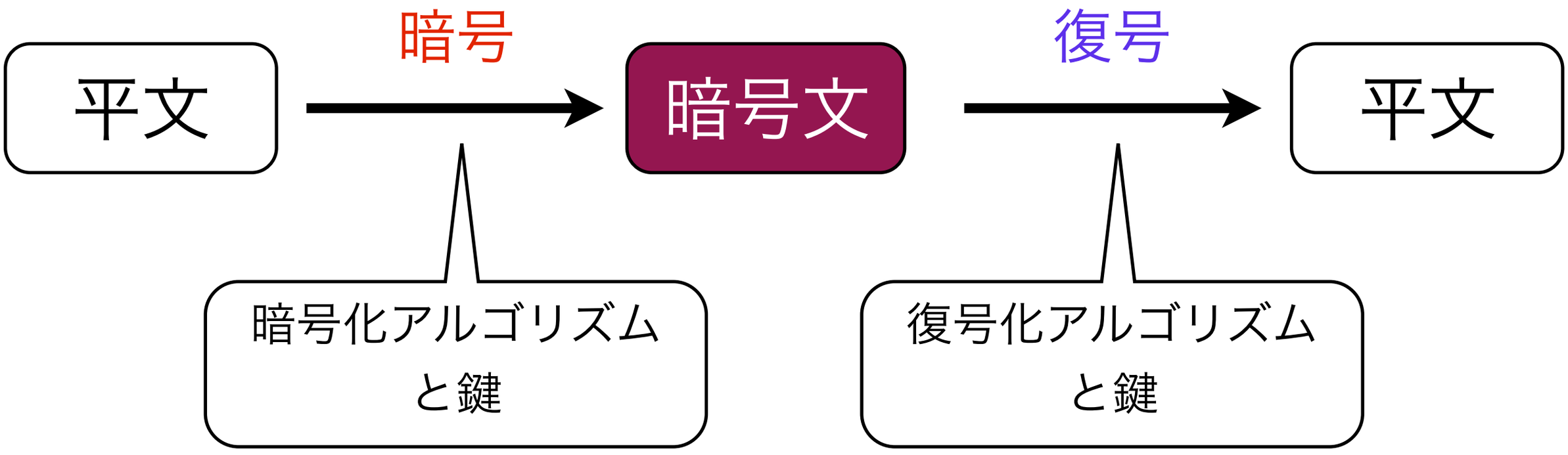
利用されている要素技術

- 通信路の暗号化
  - 公開鍵暗号、共通鍵暗号
- 認証 (Server認証、Client認証)
  - 公開鍵(電子)証明書、Public Key Infrastructure (PKI): 公開鍵基盤
- 通信データの改ざん検出
  - ハッシュ関数、電子署名

TLSと暗号処理

- 共通鍵暗号と公開鍵暗号
- Public Key Infrastructure (PKI)
- ハッシュ関数 (一方向関数)

暗号化



対称鍵暗号方式

- 暗号化鍵と復号鍵が同一、または片方の鍵から
  他方の鍵が容易に求められることを特徴とする暗号方式
  - 「暗号化した鍵」で暗号文の復号が可能
    - 鍵の呼称はいろいろ
    - 秘密鍵 (secret key), 共通鍵 (common key), 共有鍵 (shared key)
- 「共通鍵暗号方式」とも呼ばれる

非対称鍵暗号方式

- 暗号化鍵から復号鍵を求めることが困難なことを特徴とする暗号方式
  - 「暗号化鍵」で暗号文を復号することは不可能
  - 「一対の鍵 (paired keys)」で処理を行う
    ⇒ 公開鍵 (public key) と 秘密鍵 (secret key)
    - 別の呼称：私有鍵、プライベート鍵 (private key,)
- 「公開鍵暗号方式」と呼ばれる

公開鍵暗号方式の利点

鍵管理の手間が異なる

共通鍵

- 通信相手毎に生成
- 通信相手毎に交換
- 鍵は秘密裏に管理

４名で相互通信
各利用者は 3つの鍵が必要

公開鍵

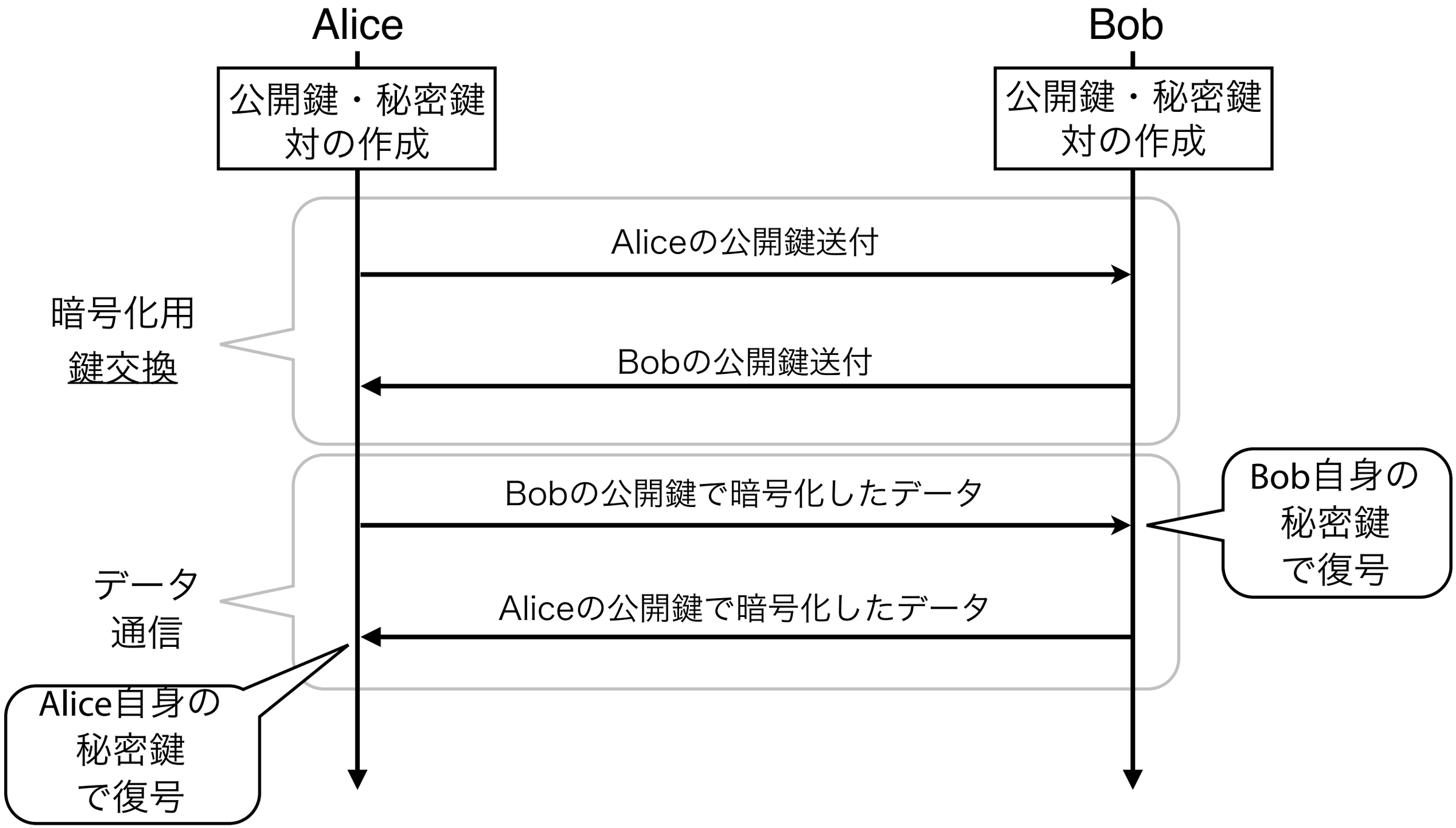
- 鍵対を一回生成
- 公開鍵の公開だけ
- 秘密鍵1つのみ
  秘密裏に管理

４名で相互通信
各利用者は1ペアの鍵が必要

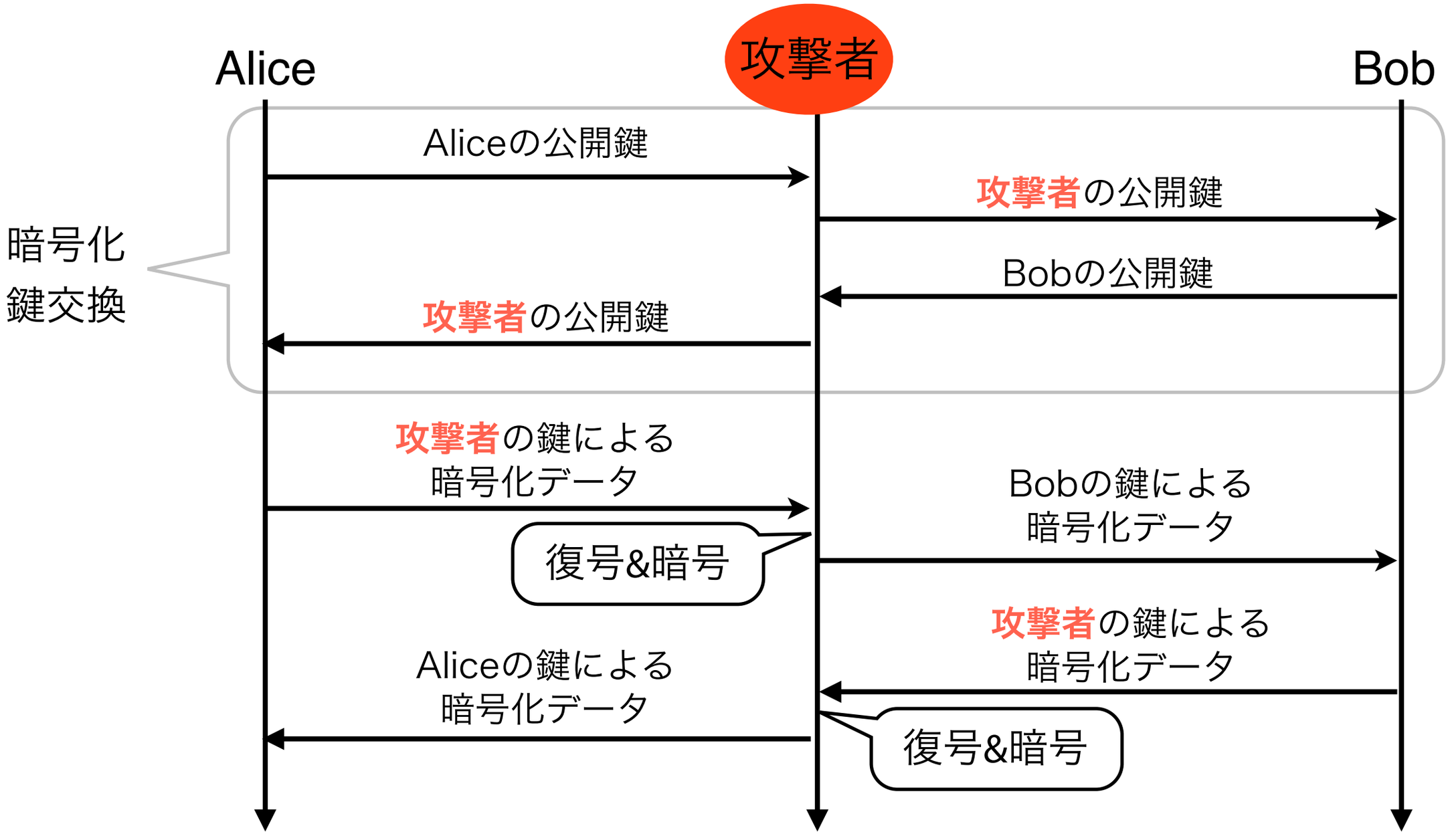
公開鍵暗号での代表的な処理

- **暗号通信** (他者⇒自分への秘匿通信)
  - 相手(送信者): 受信者の「公開鍵」で暗号化
  - 自分(受信者): 自身の「秘密鍵」で復号
- **電子署名** (処理主体を他者に証明)
  - 自分(証明者): 自身の「秘密鍵」で署名
  - 他人(検証者): 署名者の「公開鍵」で検証

公開鍵による通信

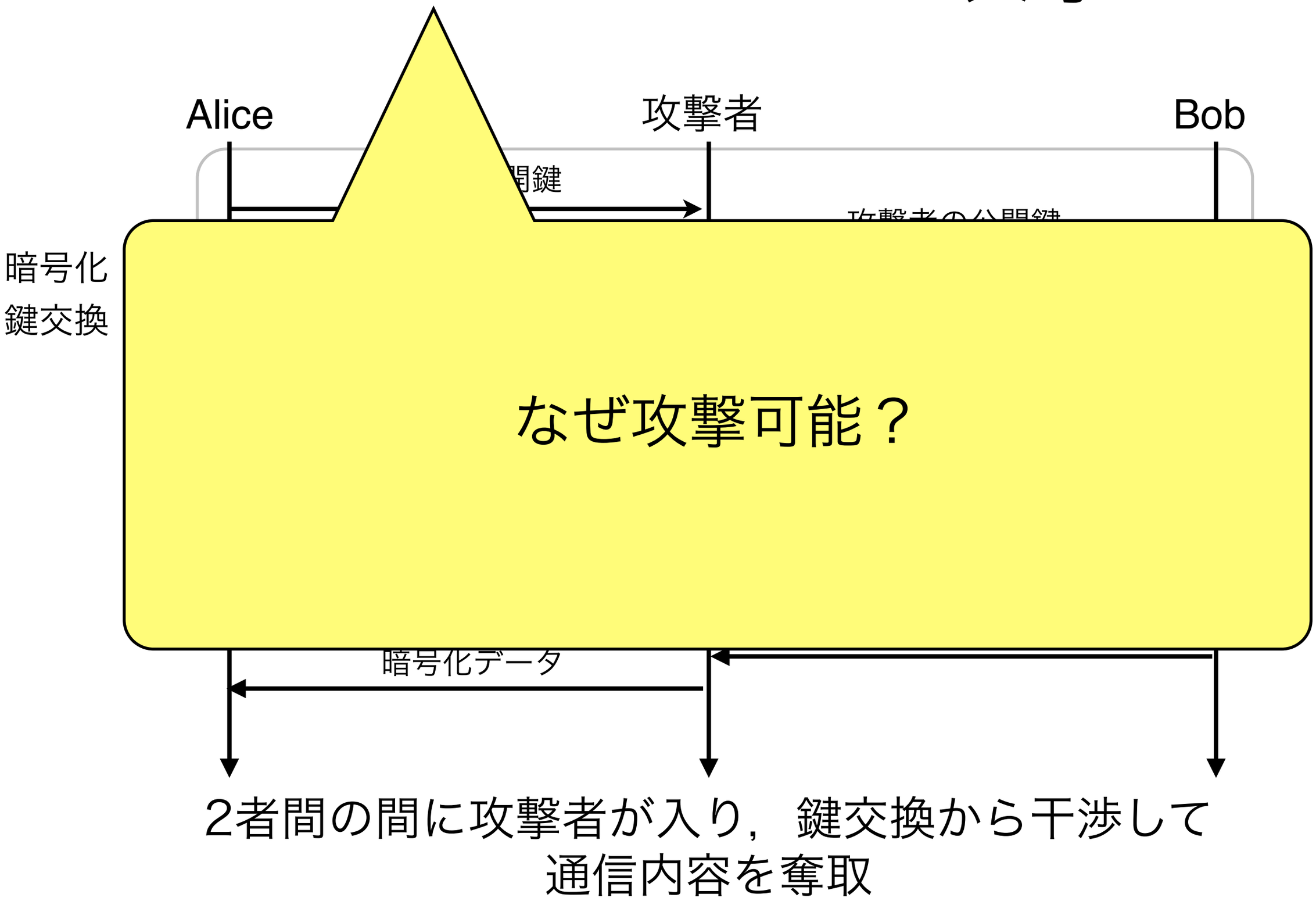

Alice
Bob
公開鍵・秘密鍵
対の作成
公開鍵・秘密鍵
対の作成
Aliceの公開鍵送付
Bobの公開鍵送付
暗号化用
鍵交換
Bobの公開鍵で暗号化したデータ
Aliceの公開鍵で暗号化したデータ
データ
通信
Bob自身の
秘密鍵
で復号
Alice自身の
秘密鍵
で復号

man-in-the-middle攻撃



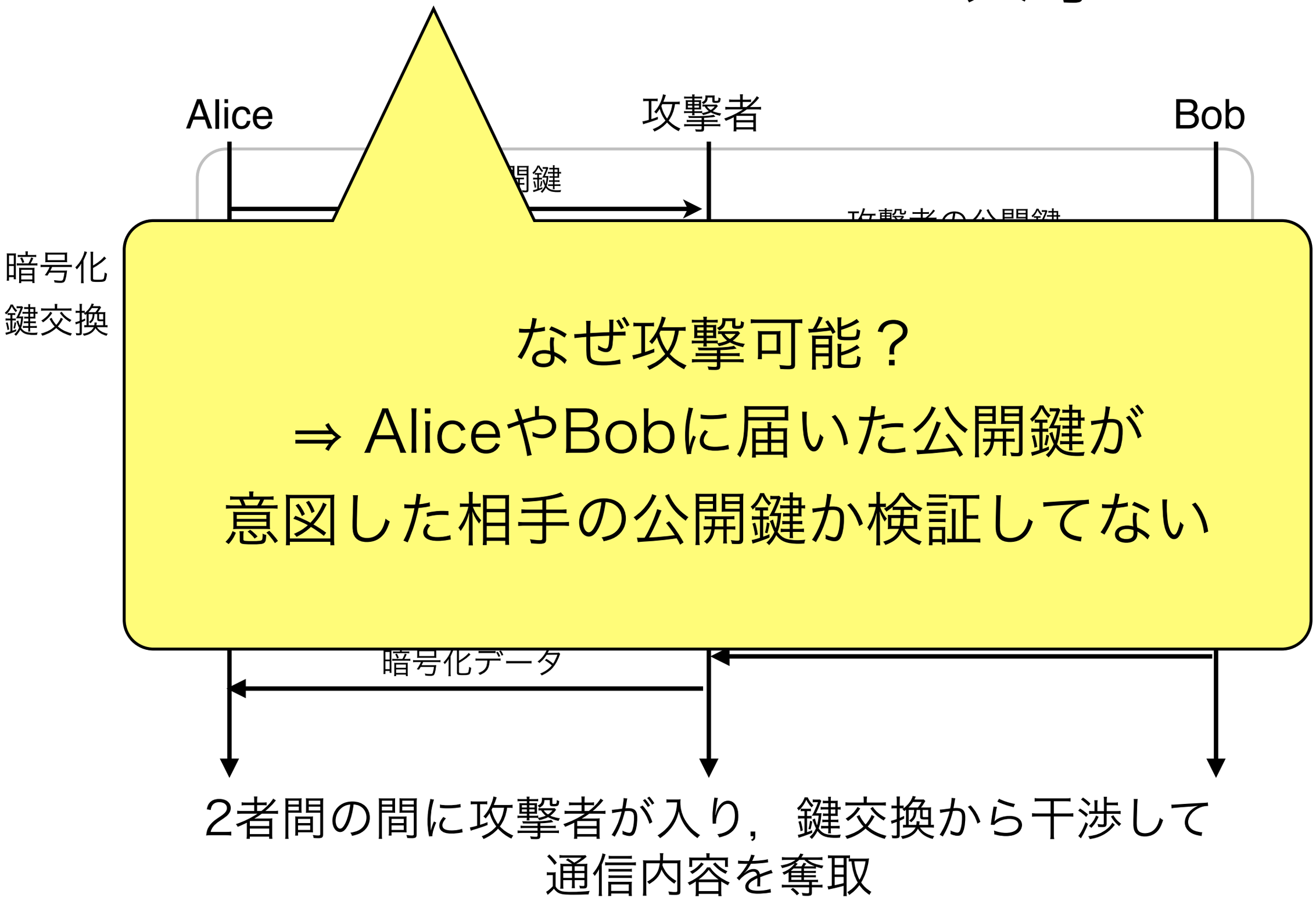
通信する2者間の間に攻撃者が入り(*man-in-the-middle*),
鍵交換から干渉して通信内容を奪取

man-in-the-middle攻撃



2者間の間に攻撃者が入り，鍵交換から干渉して
通信内容を奪取

man-in-the-middle攻撃



なぜ攻撃可能？

⇒ AliceやBobに届いた公開鍵が
意図した相手の公開鍵か検証してない

2者間の間に攻撃者が入り，鍵交換から干渉して
通信内容を奪取

公開鍵とその認証

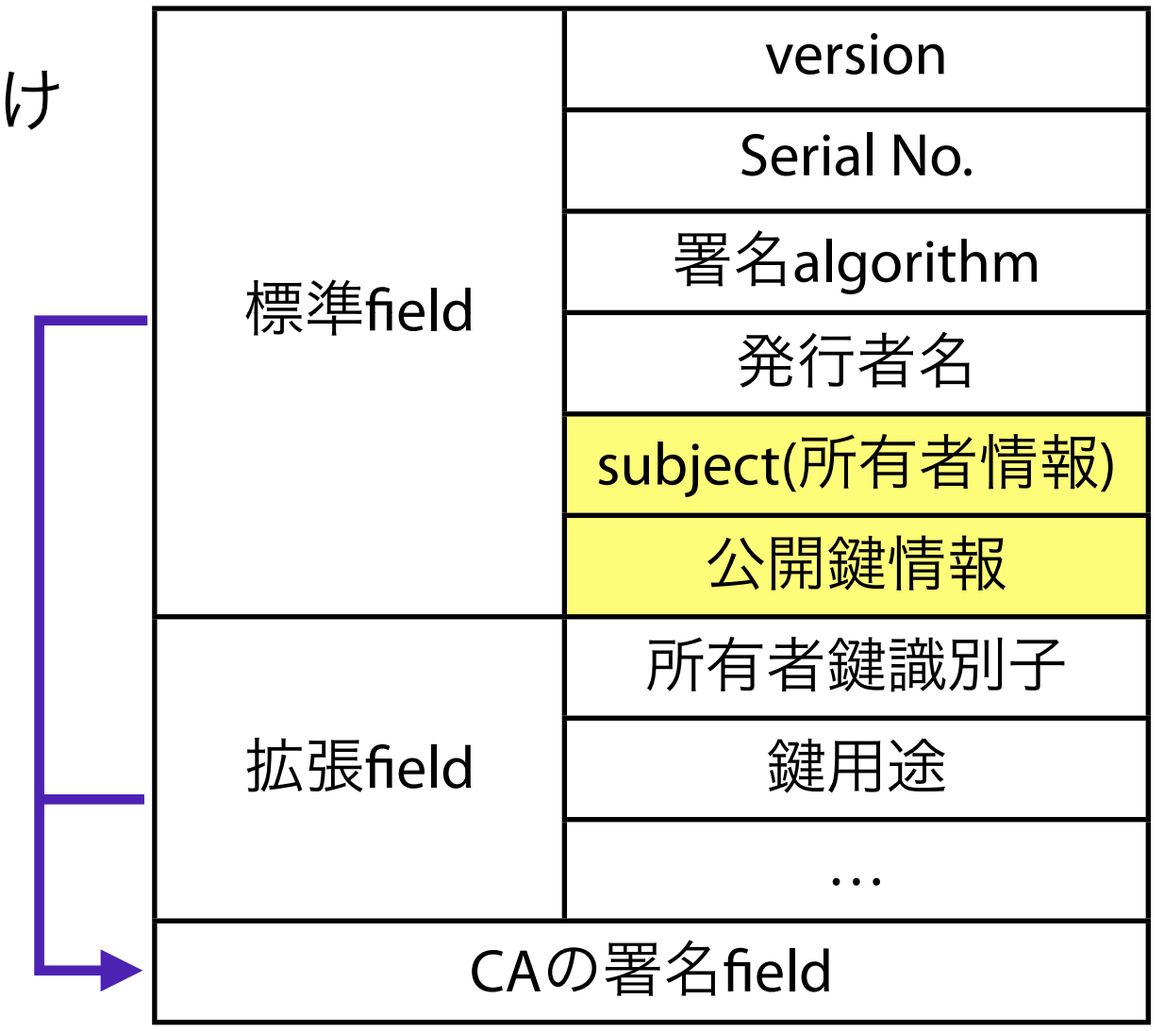
- 問題: 公開鍵と所有者の「関連付け（結びつき）」をどう担保するか？
  - 中間者攻撃：第三者が「偽の公開鍵」を「A君の公開鍵」として公開し、A君宛の通信を仲介 (中身を知ることが可能)
- 公開鍵を公開する際、その鍵の所有者が誰かを保証する(検証可能にする)枠組みが必要
  ⇒ Public Key Infrastructure (PKI)
  - “Infrastructure” が意味する通り、公開鍵暗号技術の利用における「社会基盤システム」

Public Key Infrastructure
(公開鍵基盤)

- 信頼できる第三者機関が審査し、保証する枠組み
- 信頼できる第三者 (Trusted Third Party)
  ⇒ 認証局 (Certification Authority：CA)と呼ぶ
- CAは、審査を通過した公開鍵に対し
  「公開鍵証明書」(電子証明書)を発行
  ⇒ 公開鍵とその所有者の「結びつき」を証明
  - たとえ)「Aさんの運転免許証」：私はAさん本人であり、普通自動車 運転資格を持つ人物であることを証明する証明書.
    この例で、CAに該当するのは都道府県公安委員会

公開鍵証明書
(a.k.a. 電子証明書)

- CAが公開鍵とその所有者の関連付けを証明
- フォーマット: X.509 v3 (RFC 2459)
  - 所有者情報と公開鍵情報を保持
  - CAの秘密鍵で両fieldのデータに対し署名(電子署名)



参考：電子証明書には何が書いてあるの?: https://www.verisign.co.jp/basic/pki/content/

所有者情報

C (=Country)	2文字の国コード
ST (=State or Province)	州名または都道府県名
L (=Locality Name)	都市名または地方名
O (=Organization name)	組織名
OU (=Organization Unit Name)	部門・部署名
CN (=Common Name/E-mail)	姓名/ホスト名/E-mail

実際に見てみよう

https://www.cc.uec.ac.jp/　https://www.jibunbank.co.jp/　https://www.boy.co.jp/