情報処理システム論 (17)

暗号技術の利用

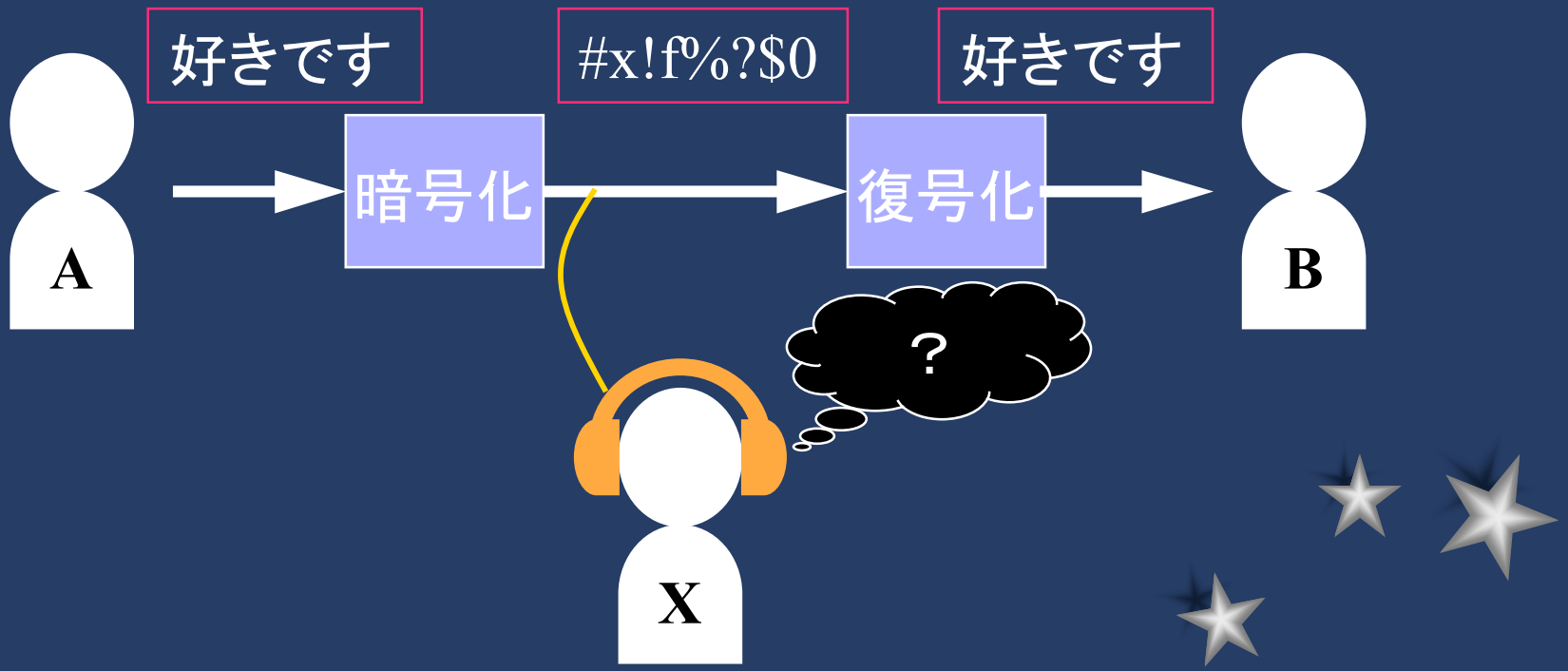
- 通信の安全の確保
  - 盗聴の防止
  - 改竄（かいざん）の防止
  - なりすましの防止

盗聴

- 暗号化していないと…

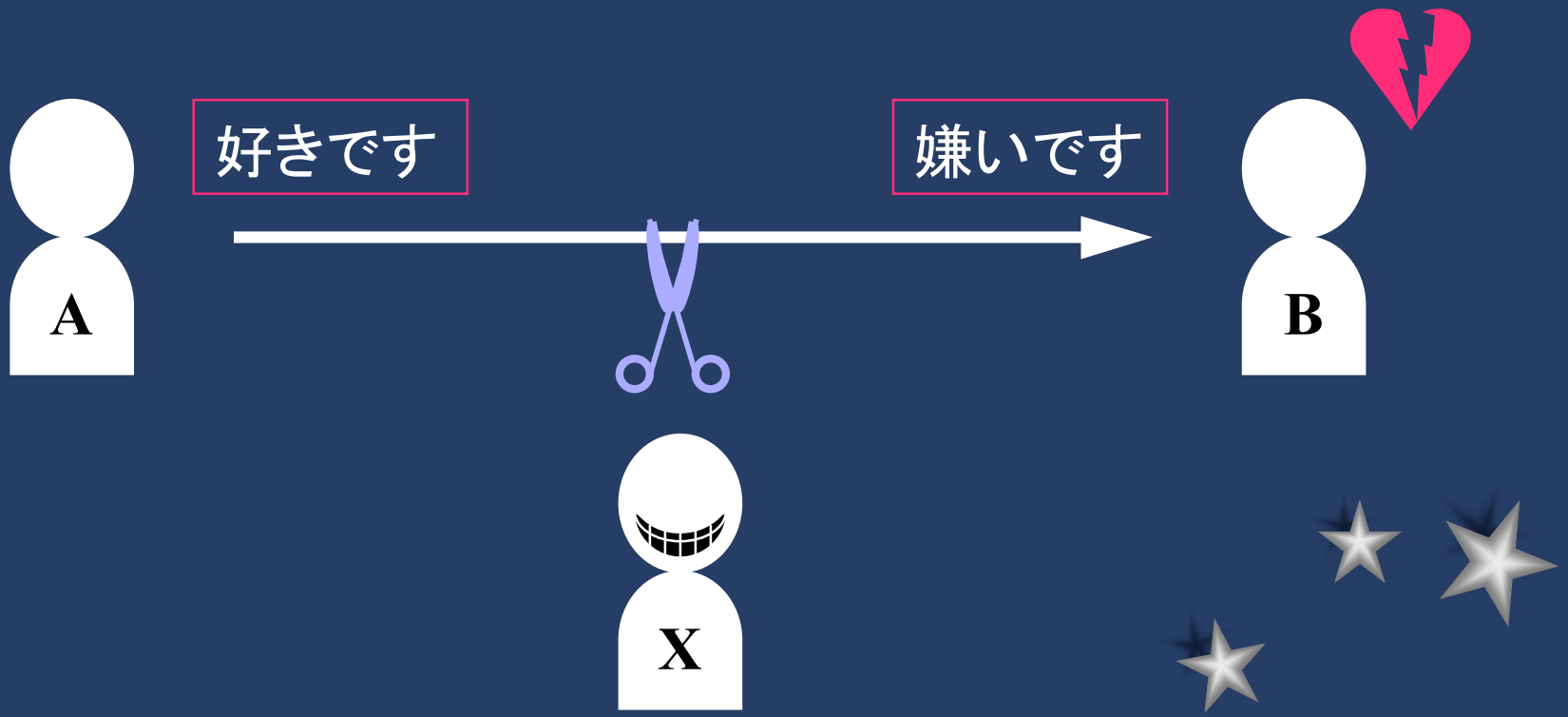
盗聴の防止

- 暗号化によって盗聴を防ぐ



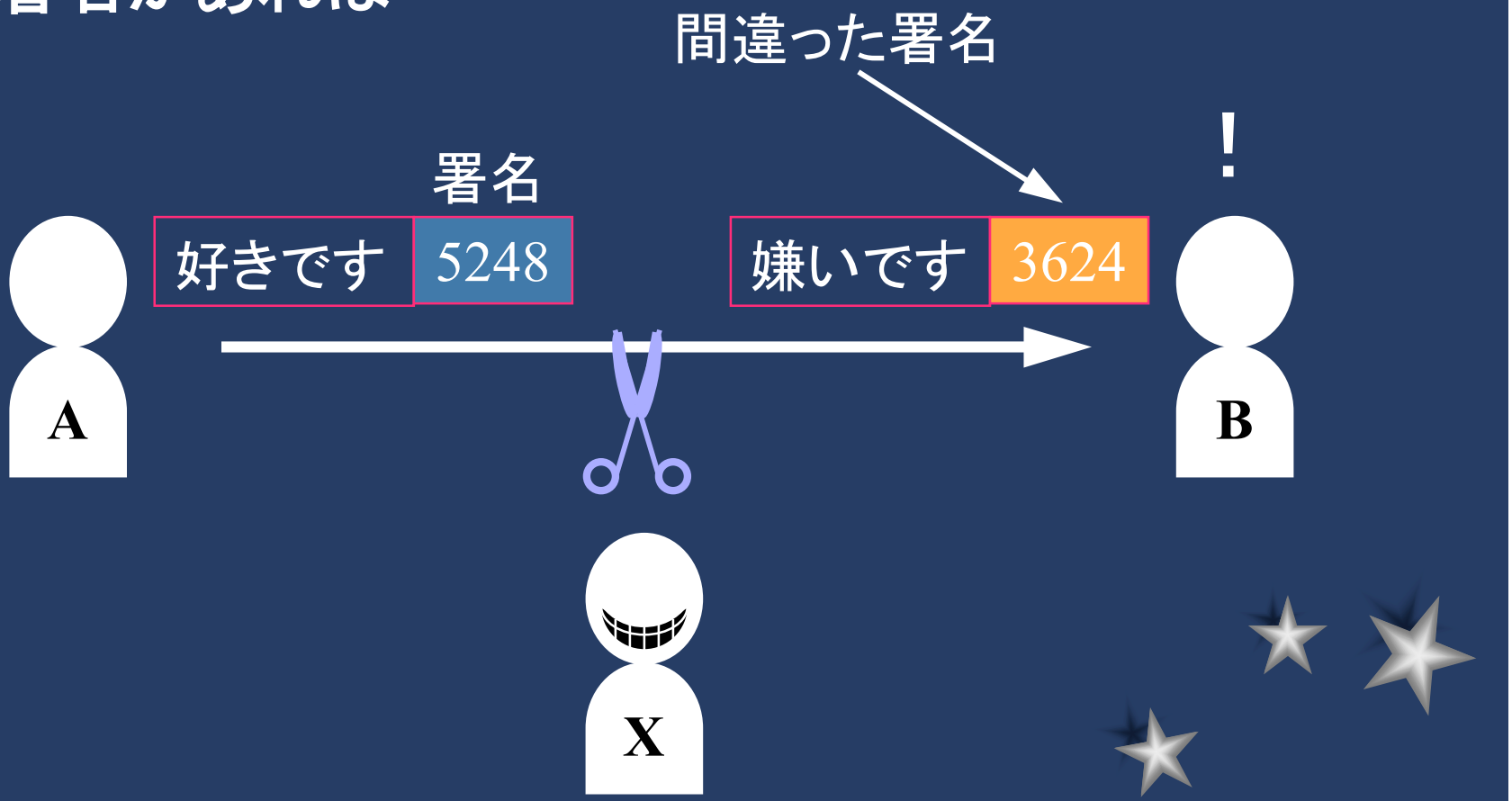
改竄

- 署名していないと…



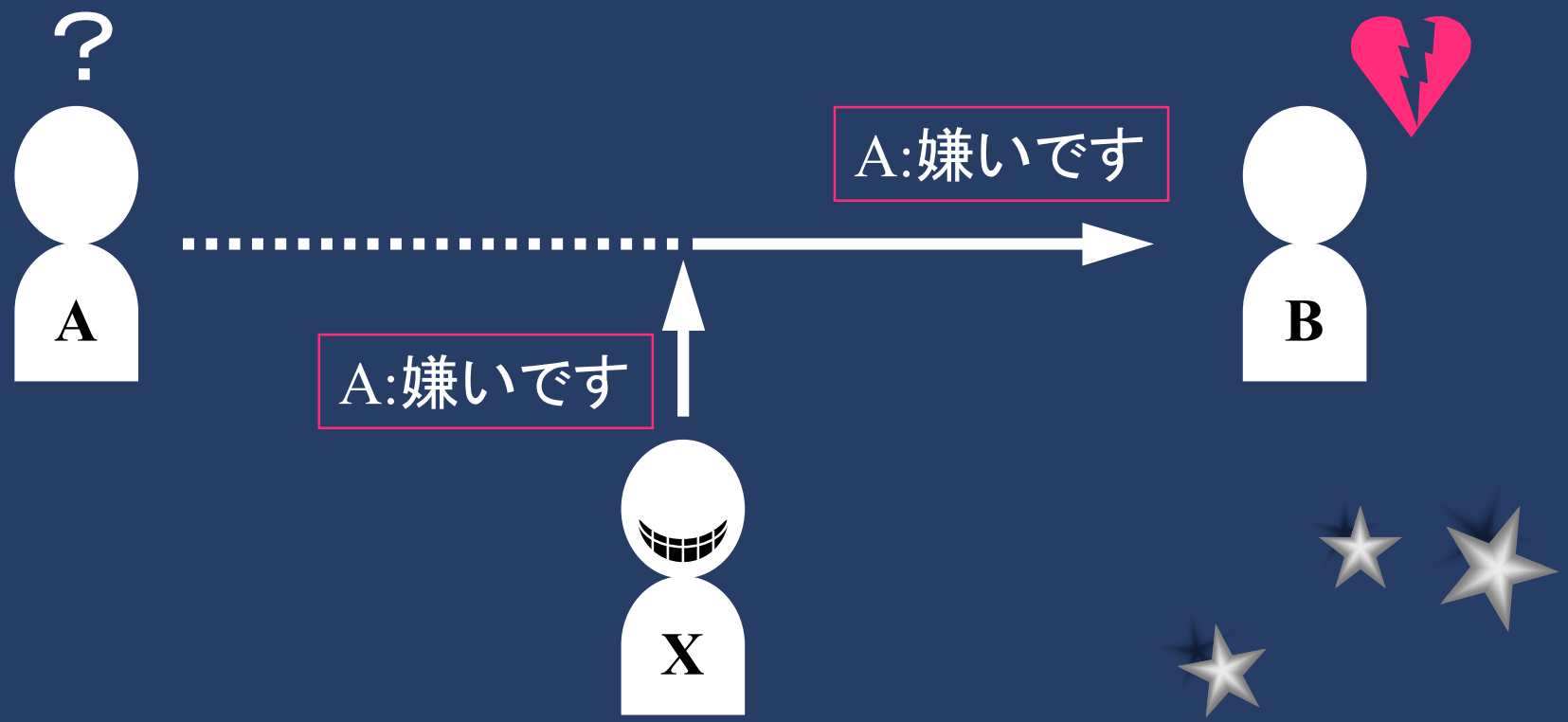
改竄の防止

- 署名があれば



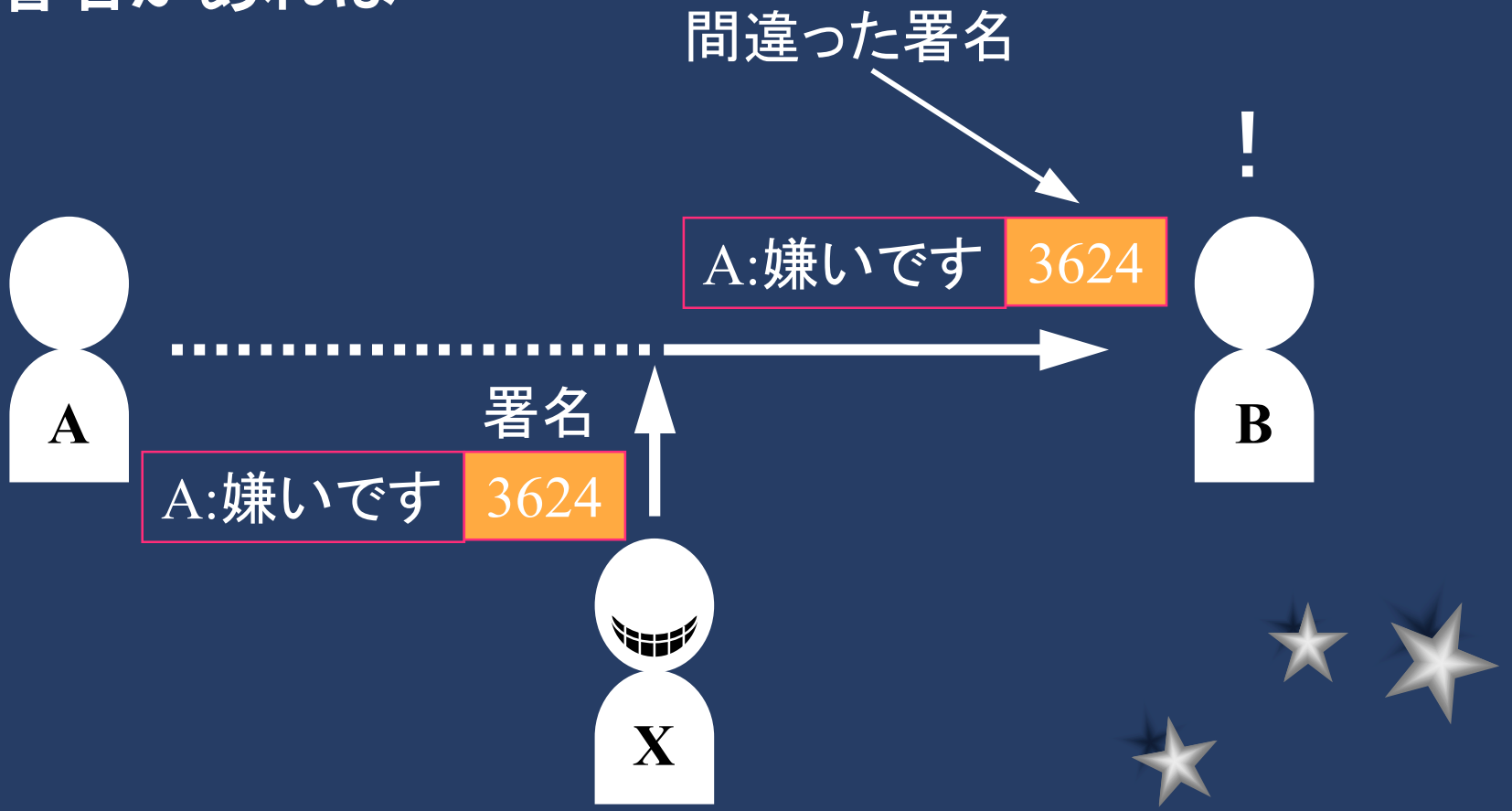
なりすまし

- 署名していないと…



なりすましの防止

- 署名があれば



暗号方式 の大分類

- 慣用系
  - 共有鍵方式
- 公開系
  - 公開鍵方式

共有鍵暗合

- 通信の両側で同じ鍵を共有する
  - コード方式（合い言葉風）
    - 「やま」…好きです
    - 「かわ」…嫌いです
  - スクランブル方式
    - 換字暗合
      - 適当に文字をずらす
      - IBM → HAL
    - 使い捨てパッド
      - ずらす度合いを辞書に頼る
      - 一度使ったページは再利用しない

共有鍵暗合アルゴリズム

- **DES**
  - Data Encryption Standard (1977:アメリカ)
- **トリプル DES**
  - DES の寿命を延ばす
- **RC2, RC4**
- **IDEA**
- スキップジャック

共有鍵方式の問題

- 通信前に両側で鍵の情報を交換
  - 秘密情報（鍵）をどうやって安全に教えあう？
- 鍵の管理
  - 新しい相手ごとに共有鍵を用意
  - n 人だと全体で n(n-1)/2 個の鍵が必要

DES の強さ

- 56ビットの暗合は何年で破れるか
  - 総当たりによる方法

Macintosh Quadra	98,488 年
Power Macintosh	22,659 年
1000 台の Power Mac	22.7 年

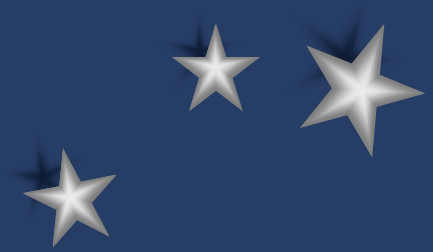
- 方式を工夫すればもっと速く破れる
  - 辞書探索
  - 既知平文攻撃、差分暗合攻撃

公開鍵暗合

- 2種類の鍵
  - 秘密鍵
    - 本人だけが持つ秘密
    - 署名用、暗合解読用
  - 公開鍵
    - すべての人に公開する
    - 暗号化用、署名確認用
- 電子署名ができる
  - 共有鍵暗合方式が持たない性質

公開鍵暗合アルゴリズム

- **Diffie-Hellman**
  - 公開鍵システムの考案者による方式
- **RSA (1976, MIT)**
  - Ronald Rivest, Adi Shamir, Len Adleman
- **Merkle-Hellman**
  - ナップサック問題に基づく
  - 欠陥が発見された

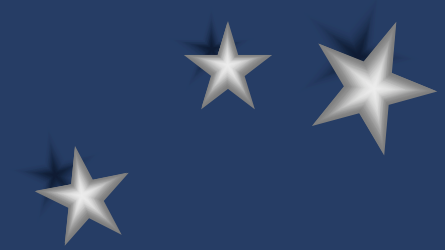


公開鍵暗合のしくみ

- 大きな素数の合成数が簡単に因数分解できないことを利用
  - 2つの大きな素数（秘密）
    - P: 47
    - Q: 71
  - 積 N = P × Q = 47 × 71 = 3337

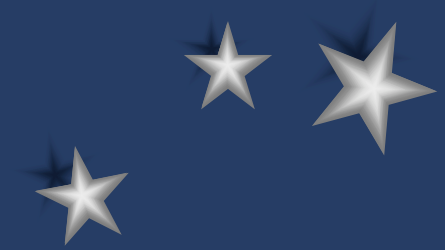
公開鍵となる2つの数

- 積 N = P × Q = 47 × 71 = 3337
- 任意の整数 e = 79
  - (P-1)(Q-1) = 3220 と互いに素



秘密鍵となる数

- P, Q, e とユークリッドの互除法から計算
  - $d = 79^{-1} \pmod{3220} = 1019$
    - $79 \times d \pmod{3220} = 1$ となる d

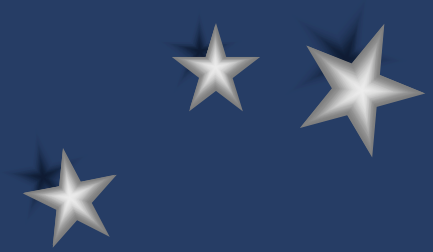


暗号化と復号化

- 暗号化
  - $b = a^{e} \pmod{N}$
  - 668 を送る場合
    - $668^{79} \pmod{3337} = 1570$
- 復号化
  - $a' = b^{d} \pmod{N}$
  - 受け取った 1570 を復号化
    - $1570^{1019} \pmod{3337} = 688$
- 逆方向の計算は非常に時間がかかる

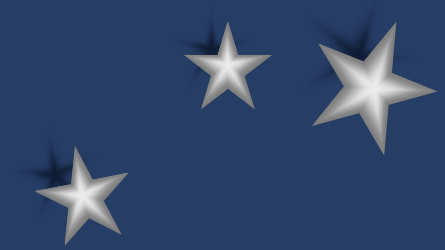
暗号化と署名

- 暗号化
  - 公開鍵でひねって、秘密鍵で戻す
    - 秘密鍵を持っている人しか解読できない
    - だれでも暗号化することができる
- 署名
  - 秘密鍵でひねって、公開鍵で戻す
    - 秘密鍵を持っている人しか署名できない
    - だれでも確認できる



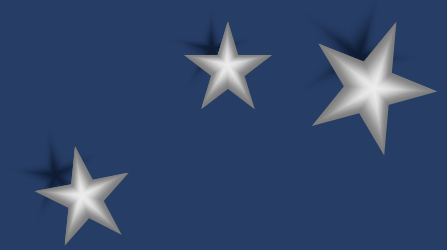
双方向通信

- 2組の鍵を用意する
  - A さんの公開鍵、秘密鍵
  - B さんの公開鍵、秘密鍵
- 署名と暗号化の組み合わせ
  - 盗聴の防止
  - なりすましの防止



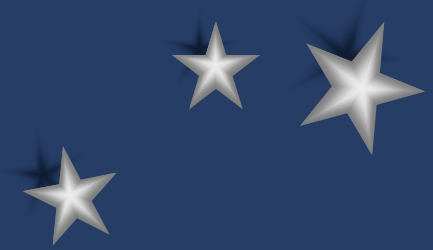
共有鍵と公開鍵の組み合わせ

- 公開鍵暗合は計算に時間がかかる
  - 共有鍵を公開鍵暗合で送る
  - 暗号化自体は共有鍵で行う
  - 頻繁に共有鍵を更新する
    - 解読の危険を避けるため



暗合にできないこと

- 通信の存在の隠匿
  - さらに他の技術と組み合わせる
- 盗まれた暗合への対抗
  - 古い暗合文書がすべて解読されてしまう
- 破壊的攻撃への対抗
- 裏切り者への対抗
  - 暗合以前の問題



暗合利用の制限

- 特許
  - 特許料の支払い
  - 万人に広く普及させるべきものには特許はそぐわない
- 輸出規制
  - ビット数で規制
  - 電子的、機器的輸出の規制
    - 本に印刷したプログラムの輸出はOK（アメリカ）

    → アメリカへ逆輸入

参考文献

- **PGP - 暗号メールと電子署名**
  - Simson Garfinkel
  - 山本和彦監訳
  - オライリージャパン
  - ISBN 4-900900-02-8