I240 暗号理論 (2019:2-1)

導入

令和元年 １０月１１日　講師：藤﨑　英一郎

基本情報: I240 暗号理論

- URL: https://www.jaist.ac.jp/~fujisaki/2019/i240
- 講義日程
  - 講義: 水曜（１限）、金曜（２限）@ I2講義室
  - チュートリアルアワー 水曜 (13:30-15:10) @ I87a
  - 予定 10/11, 10/16, 10/18, 10/25, 10/30 (1), 10/30 (2), 11/1, 11/6, 11/8, 11/13, 11/15, 11/20, 11/22, 11/27, 11/29（期末テスト）

暗号研究とは？

国際暗号学会 (International Association for Cryptologic Research (IACR)) 曰く

https://www.iacr.org/

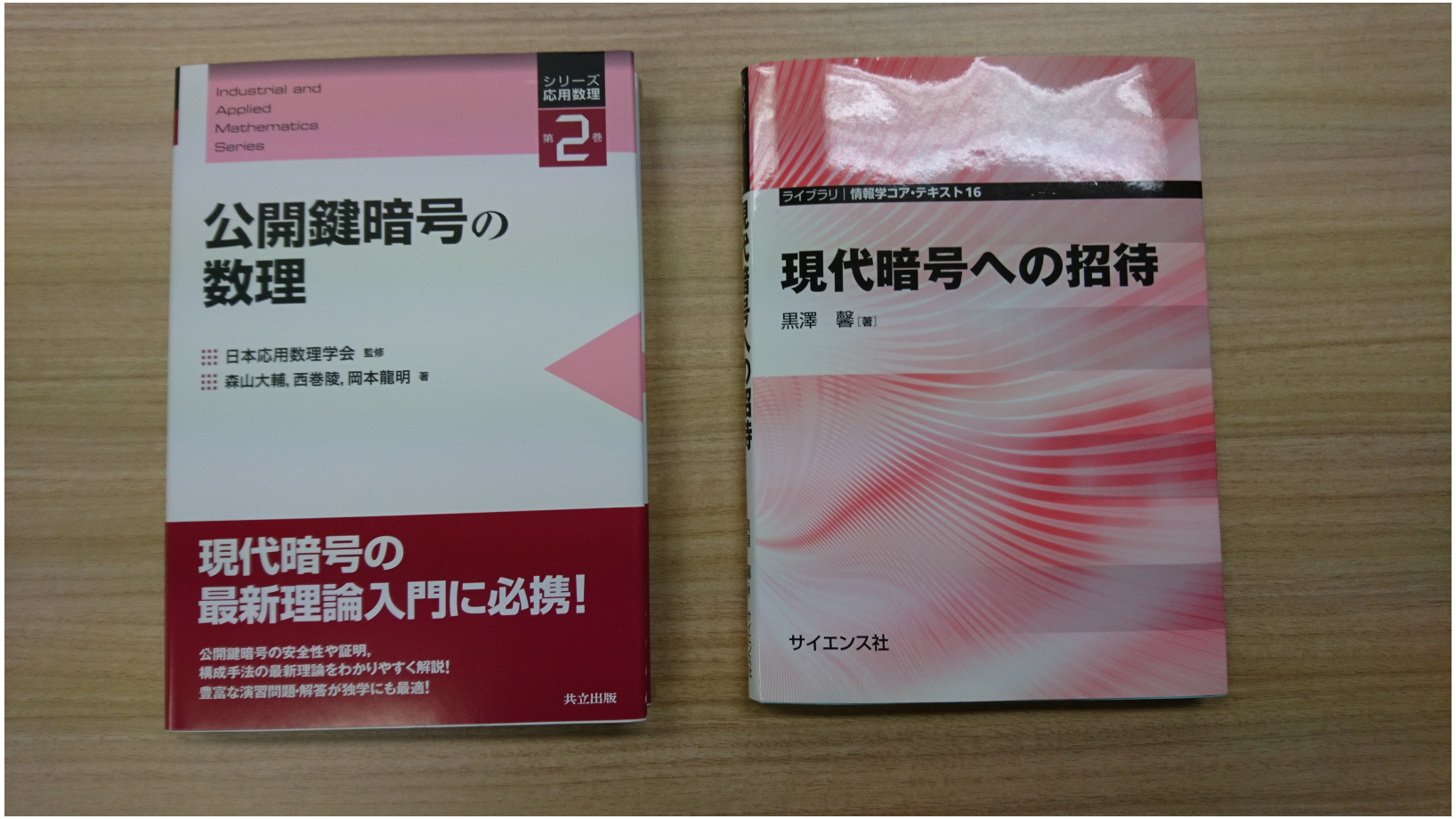
Cryptography is the science and practice of designing computation and communication systems in the presence of adversaries.

I240で学ぶ暗号の要素技術（秘匿と認証）

- 共通鍵暗号 (Symmetric-Key Encryption)
- メッセージ認証コード MAC (Message Authentication Code)
- ハッシュ関数 (Hash Function)
- 公開鍵暗号（≒鍵配送）(Public-Key Encryption/Key-Exchange)
- デジタル署名 (Digital Signatures)

主に概念と安全性モデル、幾つかの構成法
Notions, some security models, and some constructions.

I240の参考図書


Industrial and Applied Mathematics Series
シリーズ 応用数理
第2巻
公開鍵暗号の数理
日本応用数理学会 監修
森山大輔, 西巻陵, 岡本龍明 著
現代暗号の最新理論入門に必携!
公開鍵暗号の安全性や証明,
構成手法の最新理論をわかりやすく解説!
豊富な演習問題・解答が独学にも最適!
共立出版
ライブラリ | 情報学コア・テキスト16
現代暗号への招待
黒澤 馨[著]
サイエンス社

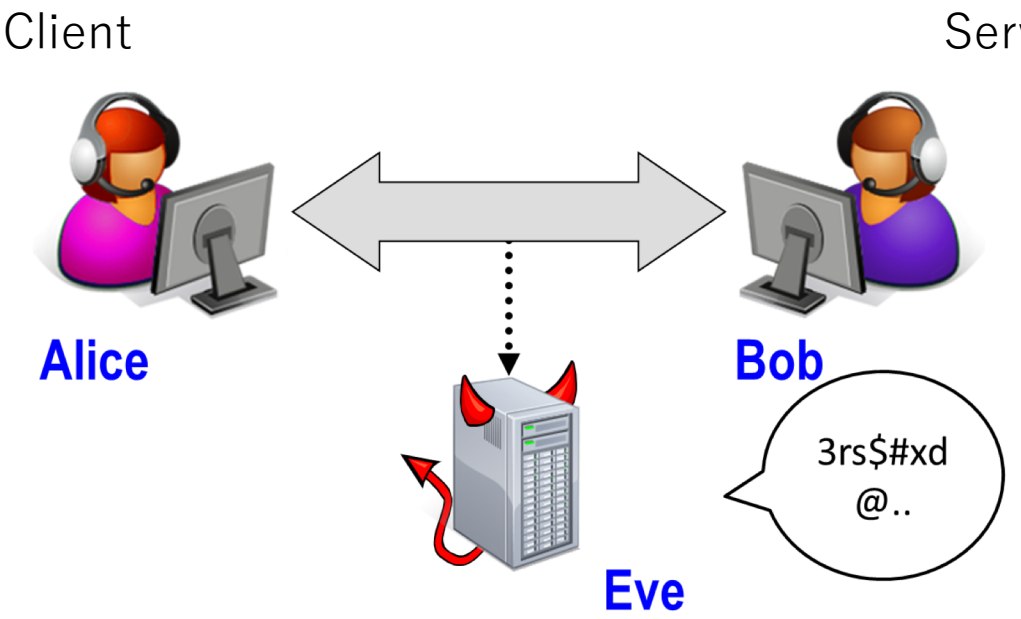
For non-Japanese Speaker

- ``A Graduated Course in Applied Cryptography”
  by Dan Boneh and Victor Shoup
  - https://crypto.stanford.edu/~dabo/cryptobook/
  - Free web version available
- ``Introduction to Modern Cryptography”
  by Jonathan Katz and Yehuda Lindell
  - Covers many topics of I240
- ``Digital Signatures” by Jonathan Katz
  - Concentrate on signature topics
- ``Mathematics of Public Key Cryptography” by Steven Galbraith
  - Strongly math-oriented

実社会で使われている暗号技術の例

事前秘密共有なしで認証付き秘匿通信（例, SSL/TLS）

https://www...



SSL/TLSで使われる暗号技術
- 公開鍵暗号
- ディジタル署名
- メッセージ認証コード (MAC)
- 共通鍵（認証）暗号
- ハッシュ関数

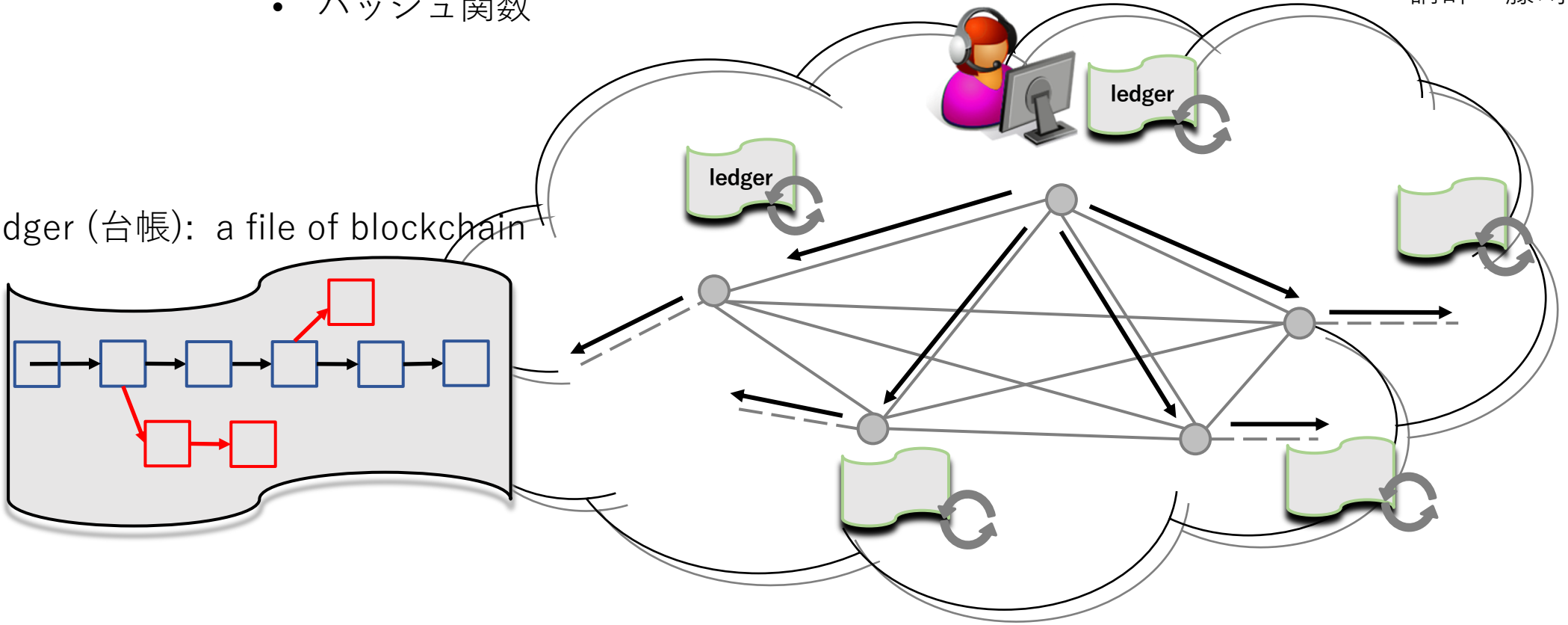
実社会で使われている暗号技術の例（その２）

暗号通貨（仮想通貨）：Bitcoin, Ethereum, etc

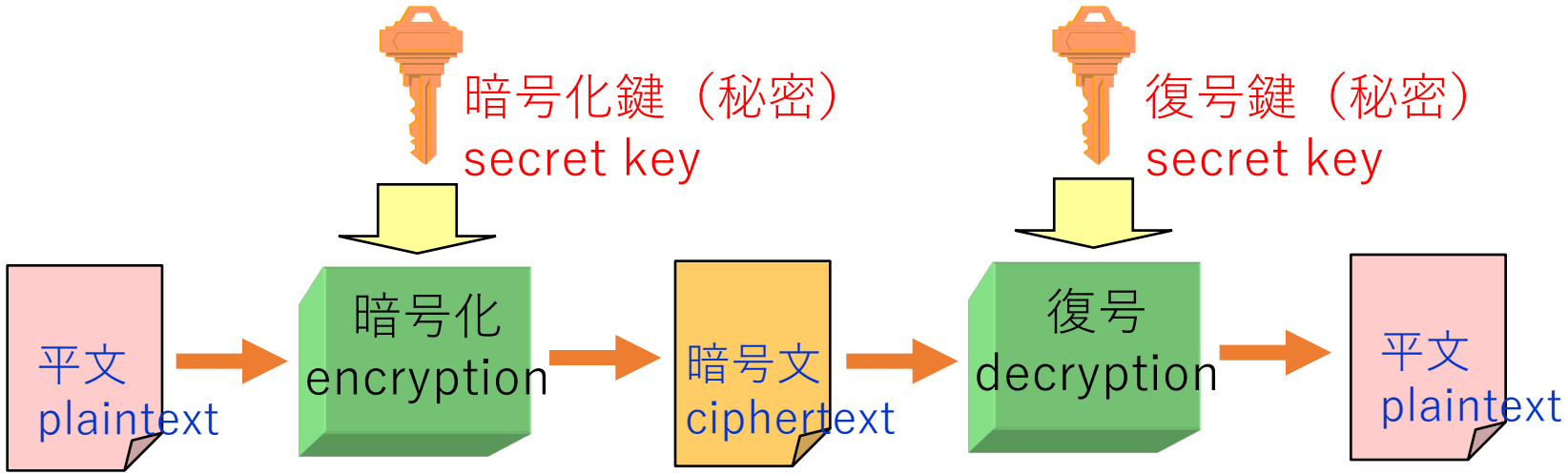
暗号通貨（仮想通貨）で使われている暗号技術
- ディジタル署名
- ハッシュ関数

JAIST J-Beans セミナー
H30.7.19 「暗号通貨入門」
講師：藤崎（ビデオあり）

Ledger (台帳): a file of blockchain

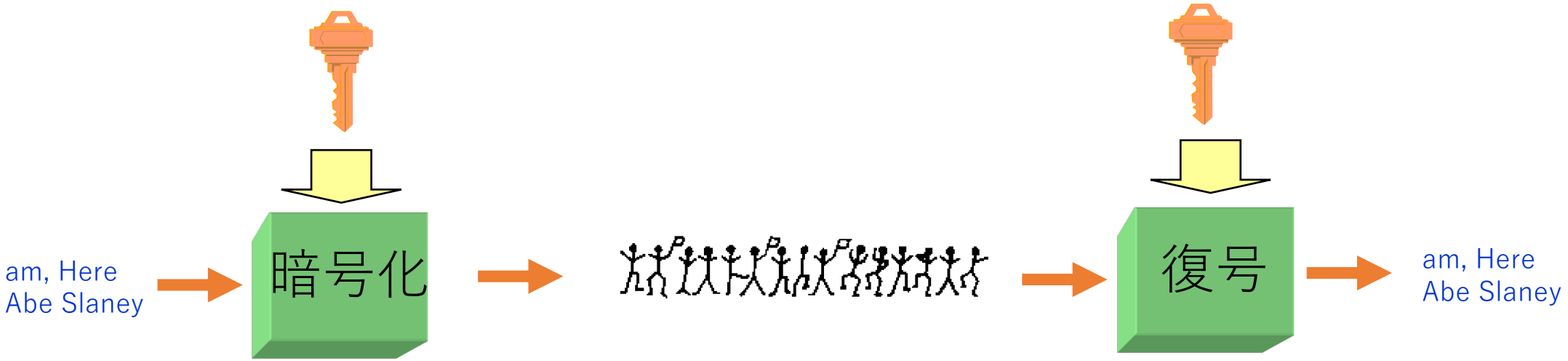


共通鍵暗号 (Symmetric-Key Encryption)

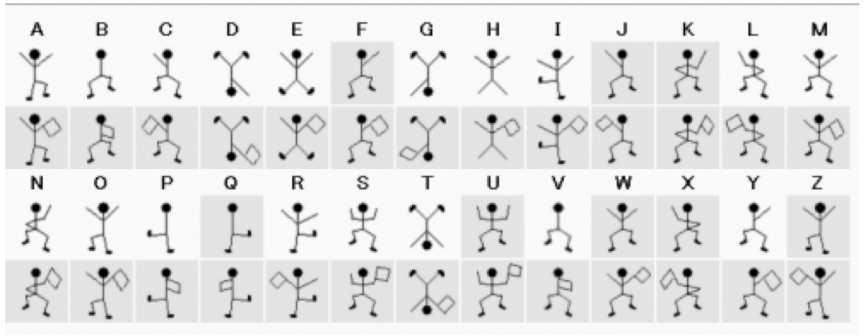


暗号化鍵(秘密鍵)＝復号鍵(秘密鍵)
を秘密裡に送信者と受信者が共有する.

共通鍵暗号の例 (dancing doll)



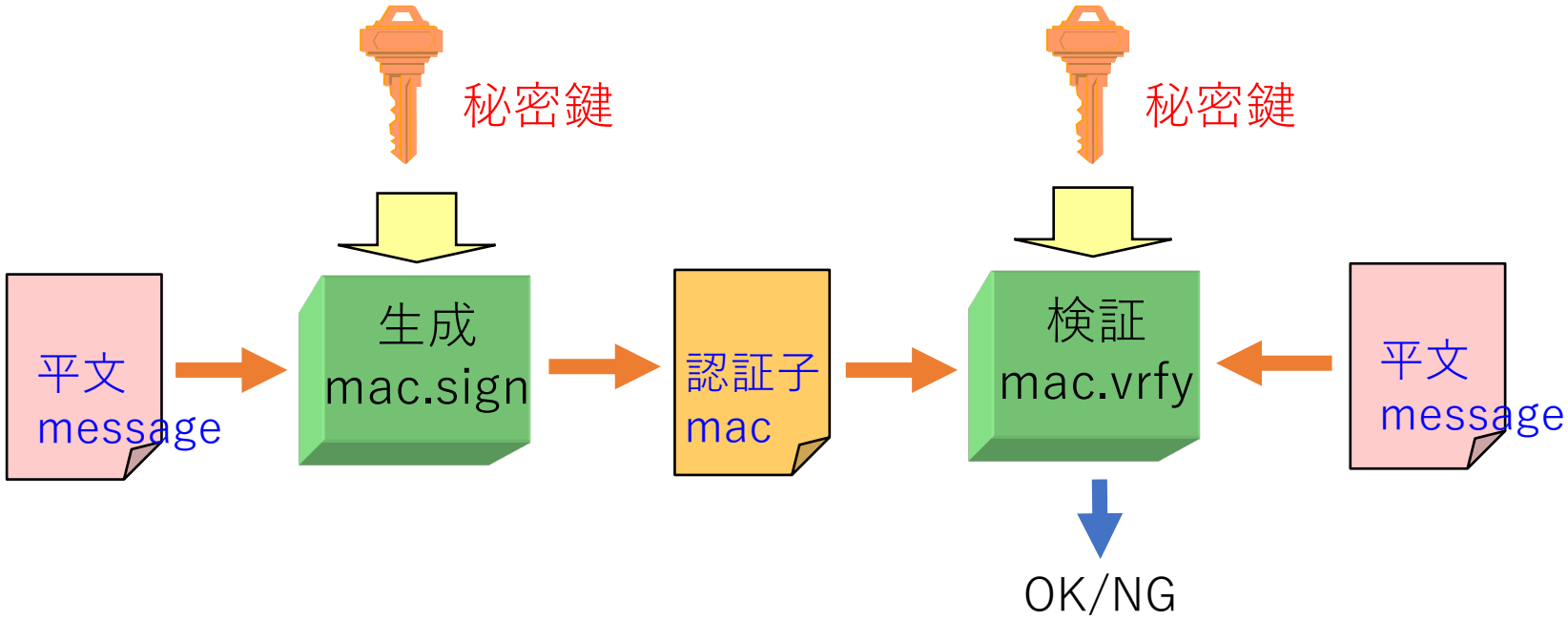
秘密鍵



換字式暗号

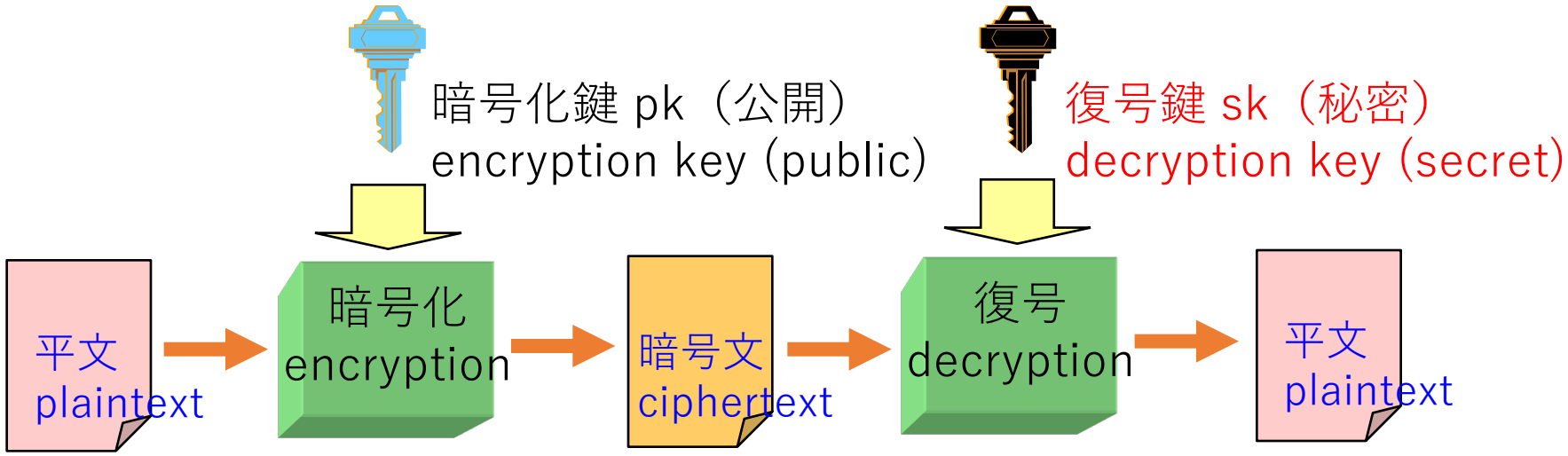
シャーロックホームズ
「踊る人形」から

メッセージ認証コード (MAC)



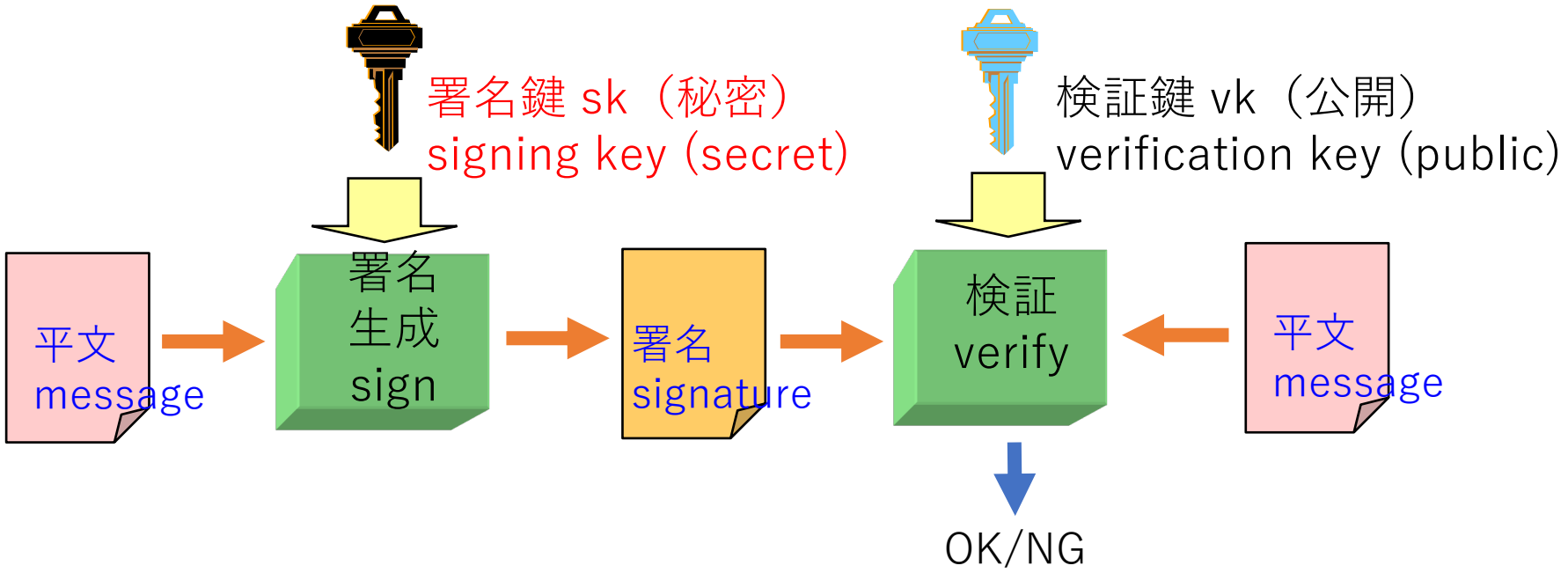
認証子生成鍵(秘密鍵)＝認証子検証鍵(秘密鍵)を秘密裡に送信者と受信者が共有する.

公開鍵暗号 (Public Key Encryption)



暗号化鍵(公開鍵)≠復号鍵(秘密鍵)
だれでも公開鍵を用いて暗号化できる.

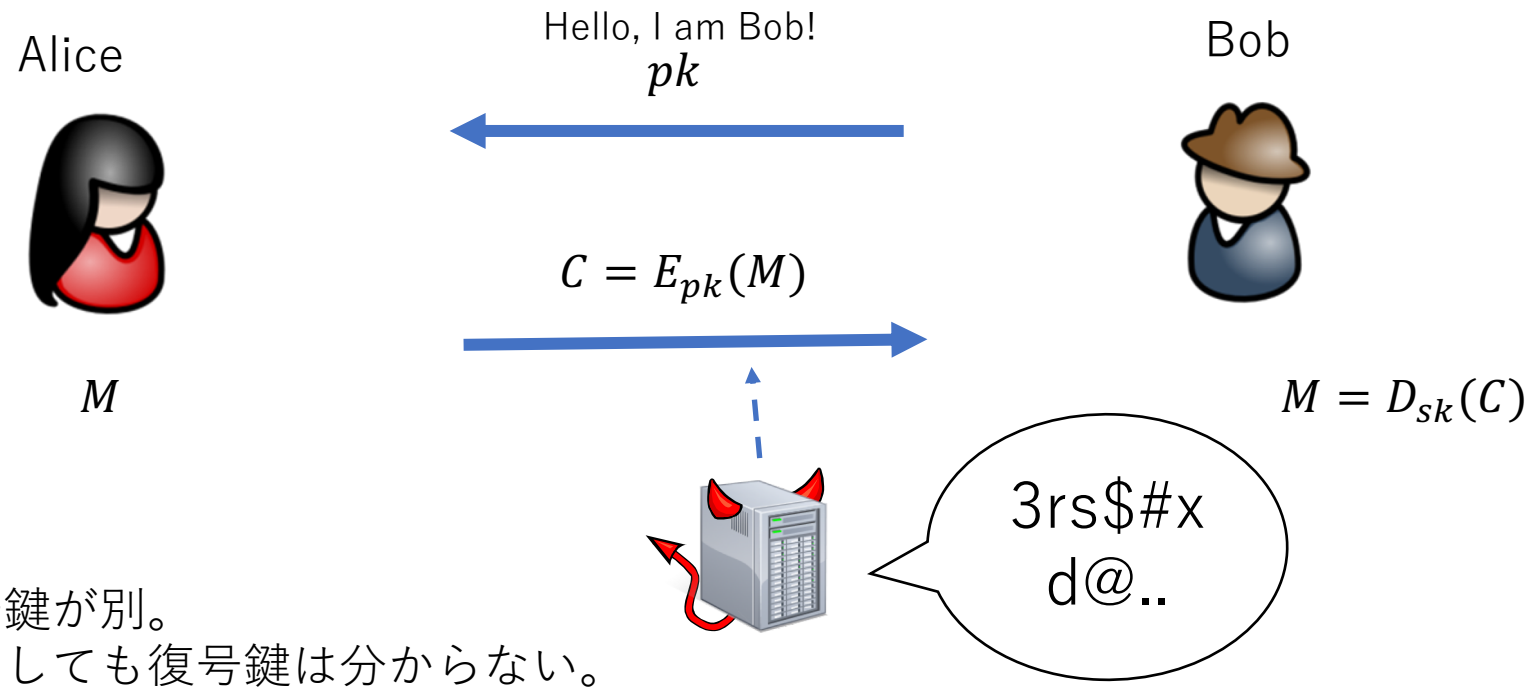
ディジタル署名 (Digital Signature)



検証鍵(公開鍵)≠署名鍵(秘密鍵)
だれでも検証鍵を用いて検証できる.

事前共有なしの秘密通信

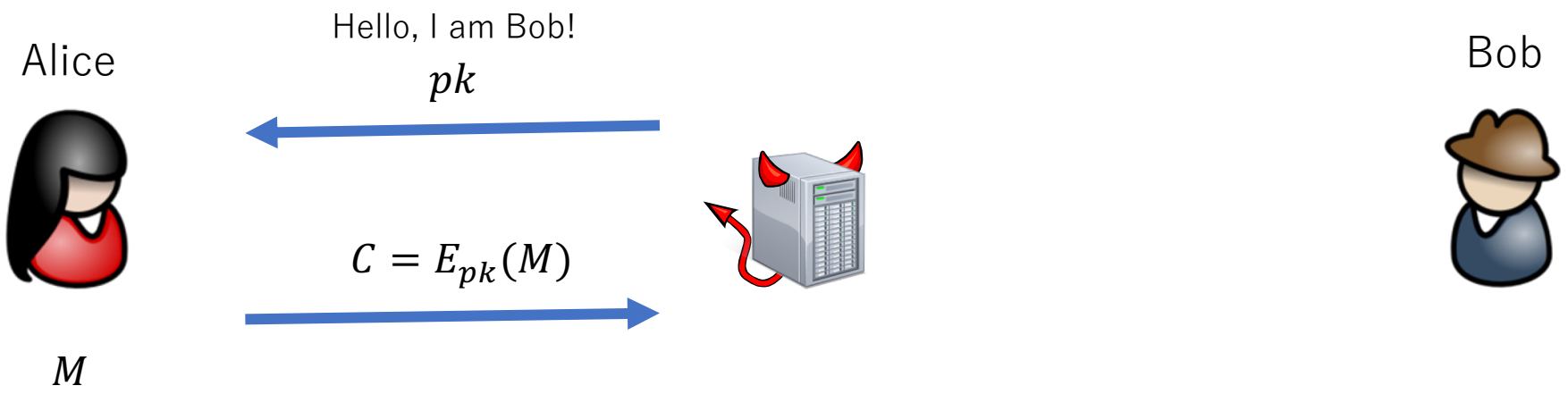
pk: Bobの暗号化鍵（公開鍵）
sk: Bobの復号鍵（秘密鍵）



暗号鍵と復号鍵が別。
暗号鍵を公開しても復号鍵は分からない。

事前の秘密共有不要！

成りすまし攻撃



公開鍵が確かにBobの公開鍵であるかチェックしないと成りすまし攻撃にあってしまう

Certificate Authority (CA)

VK_C: CAの署名検証鍵（公開鍵）
SK_C: CAの署名鍵（秘密鍵）

CAの署名
$\sigma \leftarrow Sign_{SK_C}(pk)$

TLS/SSLの雛形

pk

σ

Alice (Client)

Hello, I am Bob!
pk, σ

Bob (Server)

pk: Bobの暗号化鍵（公開鍵）
sk: Bobの復号鍵（秘密鍵）

$C = E_{pk}(M)$

M

$M = D_{sk}(C)$

3rs$#x
d@..

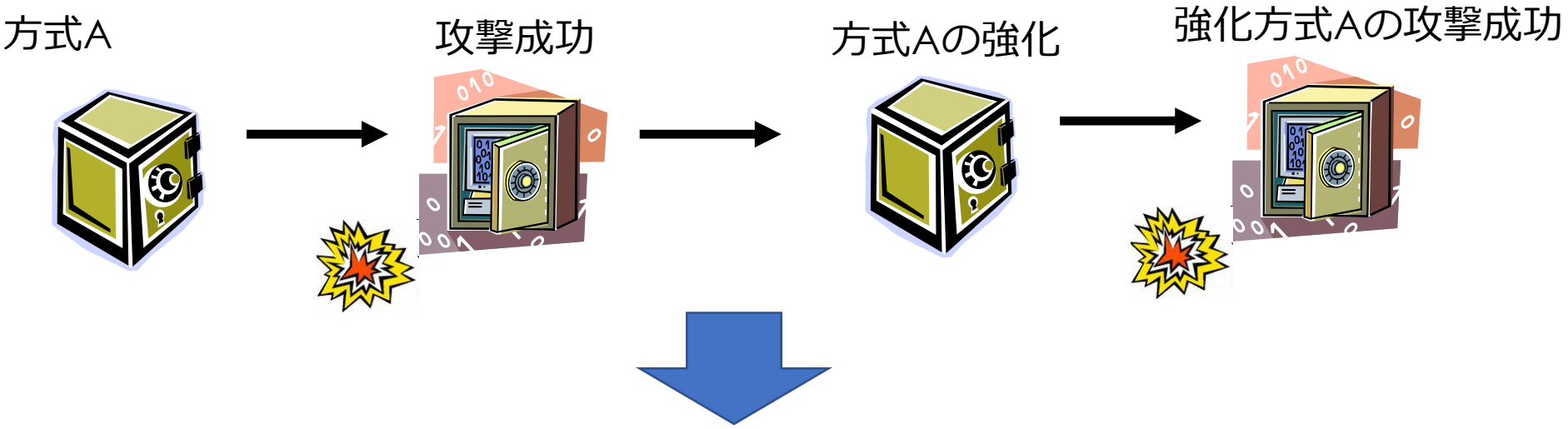
$Vrfy\,(VK_C, pk, \sigma) \overset{?}{=} 1$

公開鍵がBobのものか
チェック後、暗号文
送信

事前の秘密共有不要！

重要

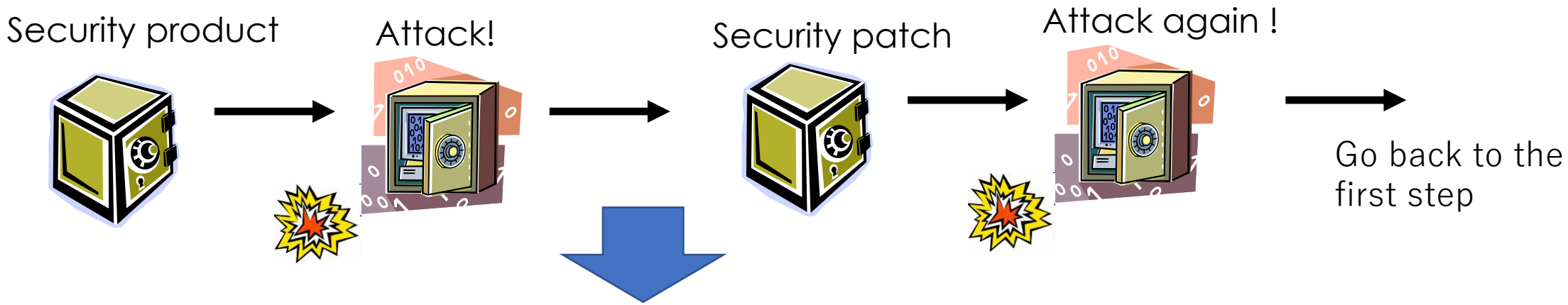
イタチごっこにならない暗号研究



証明可能安全性（という考え方）

1. 安全性証明とは：もし方式Aを敵が攻撃成功するのであれば、ある難しい数学の問題Bが解けることを証明。
2. 対偶：問題Bが難しくて解けないのであれば（仮定）、方式Aの攻撃は成功しない（安全性の帰着）。

Avoid a vicious circle!



Security should be guaranteed against ANY possible (currently unknown) attacks -- Provable Security

1. If there is an adversary that succeeds in breaking Scheme A, then it can also solve an intractable mathematical problem B.
2. (Contraposition) If it is difficult to solve Problem B, then there is no adversary to succeed in breaking Scheme A.

2種類の証明可能安全性

- 計算量的安全性
  - **数学の問題Bが解けなければ、方式Aは安全である（安全性帰着）。**
  - （潜在的リスク１）問題Bを効率良く解く新しいアルゴリズムが発見される
  - （潜在的リスク２）量子計算機などのこれまでのコンピュータを超えるものが出現し問題Bが簡単になってしまう。
    - 例）素因数分解問題、（楕円）離散対数問題
    - 対策：耐量子計算機暗号（例）格子暗号
- 情報理論的（or 統計的）安全性
  - **方式Cはなんの仮定もなく安全である。**
    - (例) One-Time Pad
    - (例)（秘密分散を使った）マルチパーティプロトコル --> I486S 暗号プロトコル理論
  - （デメリット）実現できることが限られている。

両方に共通する潜在的リスク：理論の及ばない領域（安全性モデルの外側、実装ミス等）

I240 暗号理論（講師：藤崎）

2-1期開講

本講義では、計算量仮定に基づく暗号理論の講義を行う。導入では(計算量仮定を使わない)シャノンモデルから入り、メッセー ジ認証、ハッシュ関数、共通鍵暗号について学ぶことで暗号と認証の基本概念を理解する。(計算量的)暗号理論を理解するために は、安全性の帰着という概念を理解する必要がある。このため一方向性関数、擬似乱数生成器、擬似ランダム関数とその等価性に ついて学ぶ。さらに群、環、体の基本性質を学び、その後公開鍵暗号、署名の概念と安全性の定義を学び、次に構成例と安全性証 明を学ぶ。特に、選択暗号文攻撃に強い公開鍵暗号の構成と安全性証明を最終到達点とする。