

# Trust in Distributed Systems

---

- **Information Security**
- **Isolation & Access Control**
- **Authentication & Authorization**
- **Secure Channel**
- **Authentication Protocols**

# 情報セキュリティの三大目標

---

## ■ Confidentiality

- 機密情報が漏洩しない

## ■ Integrity

- 情報やシステムが信用できる
- データやプログラムが改竄されない

## ■ Availability

- (権限のある人は)情報が利用できる

# Isolation & Access Control

---

- Confidentiality & Integrity のためには隔離が有効
  - cf. OS のメモリ保護
  - 物理的な隔離は比較的容易
    - e.g. 複数のコンピュータを物理的に切り離す
  - 論理的な隔離はもう少し複雑
    - e.g. Virtual Machine, Sandbox
- Availability のためには、もっと細かい制御が必要
  - 隔離だけでは、情報の共有ができない
- アクセス制御にはポリシーが必要
  - 典型的には「誰が何にどんな方法でアクセス可能か」を規定
  - 隔離のポリシーなら単純
    - i.e. 共有を一切許さない

# Authentication/Authorization

---

- アクセス制御には、主体と対象の把握が必要
  - アクセス対象は、OS やアプリケーションが把握
    - e.g. OS のファイル, プログラミング言語のオブジェクト
  - 外部からのリクエストでは、アクセス主体の把握が必要
    - e.g. ログイン時のパスワード認証
    - e.g. SSL のサーバ認証とクライアント認証
- Authentication と authorization に分けて考える
  - Authentication でアクセス主体を確認する
  - Authorization でアクセス主体に権限を付与
  - システム構成上も両者を分離したいことがある
    - e.g. 認証は OS, リソース保護は Web サーバが行う
    - e.g. Kerberos サーバが認証し, ユーザはシングルサインオンで各種アプリケーションを利用

# Secure Channel

---

- 以下の性質を持った通信経路
  - 不正に改竄できない
  - 不正に盗聴できない
  - 成りすましができない
    - i.e. 送信者がわかる
- 暗号技術を用いれば原理的には実現可能
  - 暗号が破れないという前提が必要
  - Availability には必ずしも寄与しないが
    - e.g. ケーブルの切断に耐えるわけではない

# Cryptography

---

## ■ 記号の定義

- $K$ : key,  $T$ : text

- $\{T\}_K$ :  $T$  を  $K$  で暗号化した結果

## ■ 鍵の対 $K, K^{-1}$ を使う

- $K^{-1}$  があれば  $\{T\}_K$  を復号可能

## ■ $K = K^{-1}$ なら対称, そうでなければ非対称

## ■ 次の性質が求められる

- $K^{-1}$  を知らずに,  $\{T\}_K$  から  $T$  を知るのが困難

- i.e. 復号鍵なしでは暗号文を読むのが困難

- $\{T\}_K$  と  $T$  から  $K$  を知るのが困難

- i.e. 署名用の鍵を推測するのも困難

- 非対称暗号系では,  $K$  から  $K^{-1}$  を知るのが困難

# Asymmetric Cryptosystem

---

- 公開鍵(public key)暗号系が実現可能
  - $A$  は, 秘密鍵  $K_A^{-1}$  を秘匿, 公開鍵  $K_A$  を公開
    - 秘密の共有が避けられる
- 盗聴・改竄の防止のほか, 署名にも使える
- 通常, 次の性質が成り立つものを利用
  - $K^{-1}$  があれば  $\{T\}_K$  を復号可能
  - $K$  があれば  $\{T\}_{K^{-1}}$  を復号可能

# 公開鍵暗号系による署名

- $\{T\}_{K_A^{-1}}$ は  $A$  が  $T$  に署名したものとみなせる
  - $K_A$  を使い,  $T$  が  $K_A^{-1}$  で暗号化されたことを確認できる
  - 改竄防止, 否認防止に利用できる
- しかし, 疑問が残る
  - $K_A^{-1}$  が  $A$  以外に漏れている可能性はないか?
    - 鍵無効化の社会的インフラが必要
  - 任意の  $X$  に対し,  $\{X\}_{K_A^{-1}}$  を  $A$  の署名つきとは考えにくい
    - $X$  の内容や構造は任意ではありえない



# 公開鍵暗号系による盗聴防止

- $\{T\}_{K_B}$  は,  $B$  にしか復号できない
  - 復号には  $K_B^{-1}$  が必要
  - ただし, これだけでは送信者を確認できない
- $\{\{T\}_{K_A^{-1}}\}_{K_B}$  により,  $A$  が  $B$  に  $T$  を署名つきで送信可
  - 盗聴の防止と発信者の確認が同時に可能
  - cf.  $\{\{T\}_{K_B}\}_{K_A^{-1}}$  では, 読めないものに署名することになる



# 改竄の防止

- 通常, セキュアハッシュ値に秘密鍵で署名する
  - $\{T\}_{K^{-1}}$ の代わりに  $\{T, \{hash(T)\}_{K^{-1}}\}$  を用いる
  - $\{hash(T)\}_{K^{-1}}$  の偽造は困難
    - ただし, MD5 などが最近では怪しくなりつつある
  - ブロック単位の置換を検出できない方式との併用も有効
- $\{T\}_{K^{-1}}$  の偽造が困難でも, replay なら容易
  - 同じ  $T$  が2度送られないプロトコルが必要
    - タイムスタンプなどをメッセージに含める



# 公開鍵を一方だけが持つ場合

- $B$  だけが公開鍵を持つと仮定
  - e.g. サーバだけが公開鍵を持つ
  - $B$  による署名,  $B$  への秘密通信は可能
- $A$  が一時的秘密鍵  $K$  を生成し,  $K_B$  で暗号化して  $B$  へ送る
  - 以降の通信は  $K$  で暗号化
  - 認証は一方向, 暗号化通信は双方向



# Symmetric Cryptosystem

---

- 秘密の共有が必要
  - 送受信者間のみで鍵を共有
    - 信頼できる第三者まで共有を許す場合もある
  - 共有秘密に基づき暗号化や認証が可能
  - 鍵の安全な配信が必要
- 一对の送受信者に一つの鍵が必要
- 公開鍵方式より, 暗号化・復号が高速
  - 公開鍵暗号を用いて, 一時的秘密鍵(セッション鍵)を交換する方法がよく用いられる

# 社会的インフラの必要性

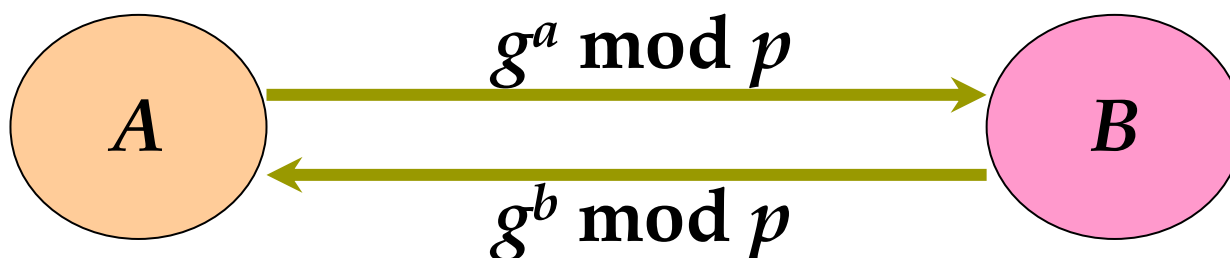
---

- Secure Channel の実現には、認証局などのインフラが必要
  - 盗聴と改竄の防止だけでは不十分
  - 「信用」の実現が必要
  - cf. 盗難と偽造が不可能な紙幣が仮に実現できても、発行国(機関)の信用がなければ紙屑同然

# Diffie-Hellman Protocol

---

- セッション鍵について合意をとる
  - $p, g$  は公開情報
  - $A, B$  が  $a, b$  を生成
  - 共有鍵として  $g^{ab} \bmod p$  を使う
    - $g^{ab} \bmod p = (g^a \bmod p)^b \bmod p = (g^b \bmod p)^a \bmod p$
- 両者の寄与は同等
- これだけでは認証はできない

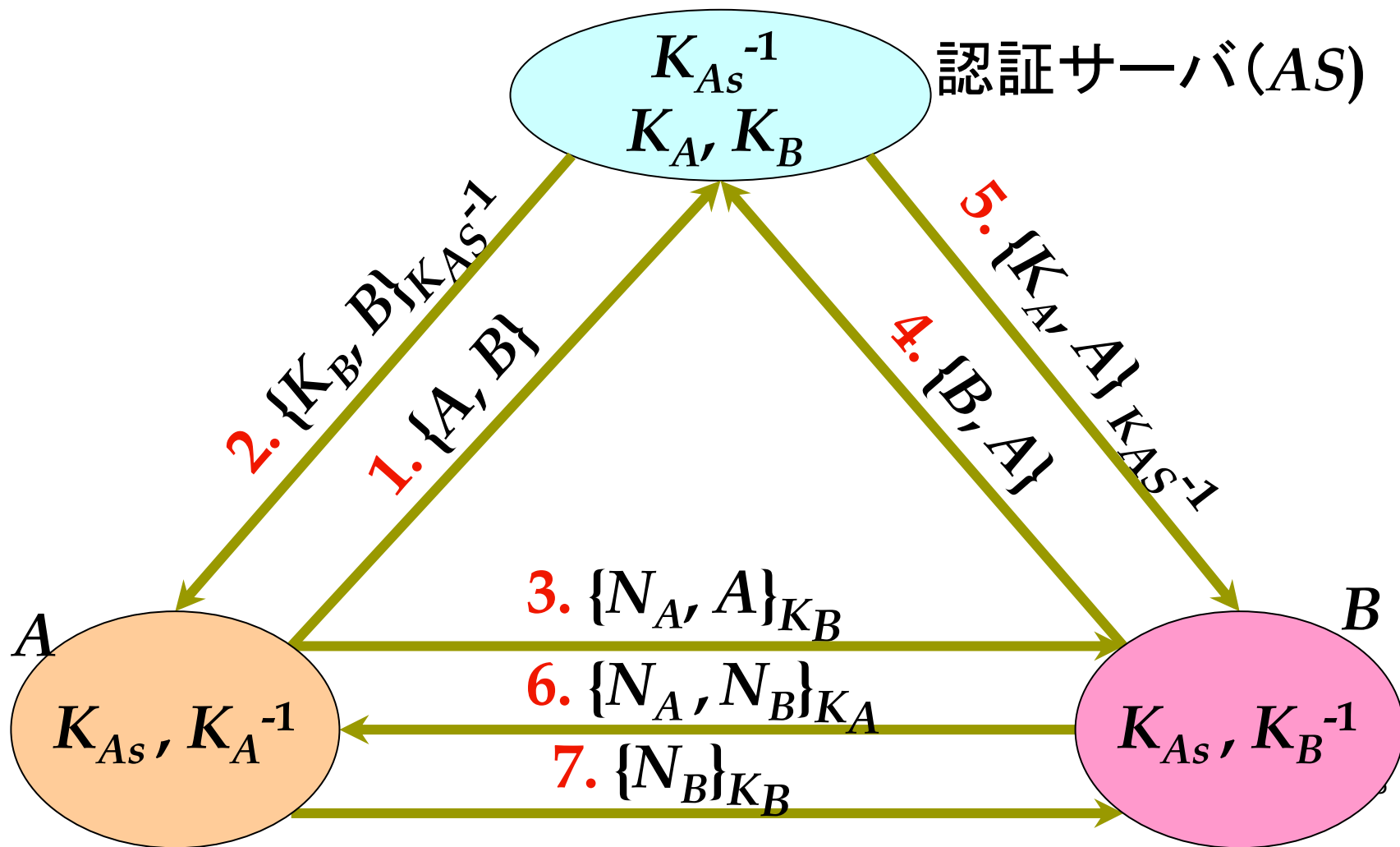


# Needham-Schroeder Protocol

---

- 2者間通信で、相手が本物であることを保証する認証プロトコル
- 公開鍵版と秘密鍵版がある
  - 今回は公開鍵版だけを紹介する
- 認証サーバの存在を仮定
  - 公開鍵版では、認証サーバの公開鍵が必要
  - 秘密鍵版では、各参加者と認証サーバが秘密鍵を共有

# 公開鍵を用いた方式 (1/2)



# 公開鍵を用いた方式 (2/2)

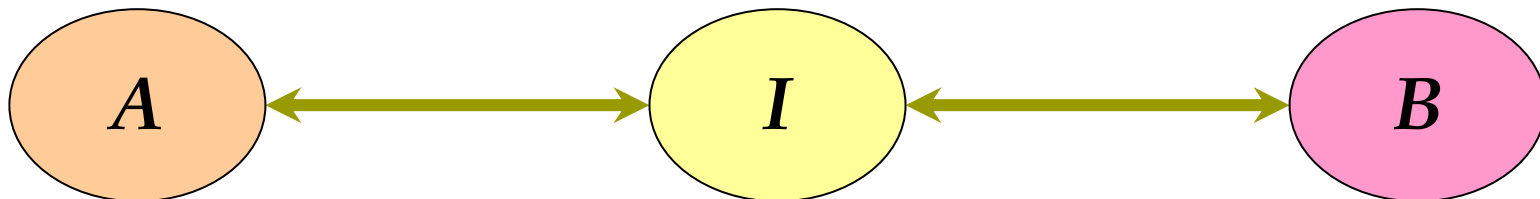
---

- 7ステップは多すぎないか？
  - 公開鍵の配送に4ステップ(1, 2, 4, 5), 相互信頼の確立に3ステップ(3, 6, 7)
  - 2種類のプロトコルが混ざっている
- $N_A, N_B$  は何故必要？
  - セッション中だけ有効な秘密を共有し, replay攻撃に耐える
- 認証サーバからの返事は  $\{K_B\}_{K_{AS}^{-1}}, \{K_A\}_{K_{AS}^{-1}}$  で十分では？
  - 要求の改竄に対抗するため  $B, A$  が含まれる

# Needham-Schroeder Protocol の 問題点 (1/2)

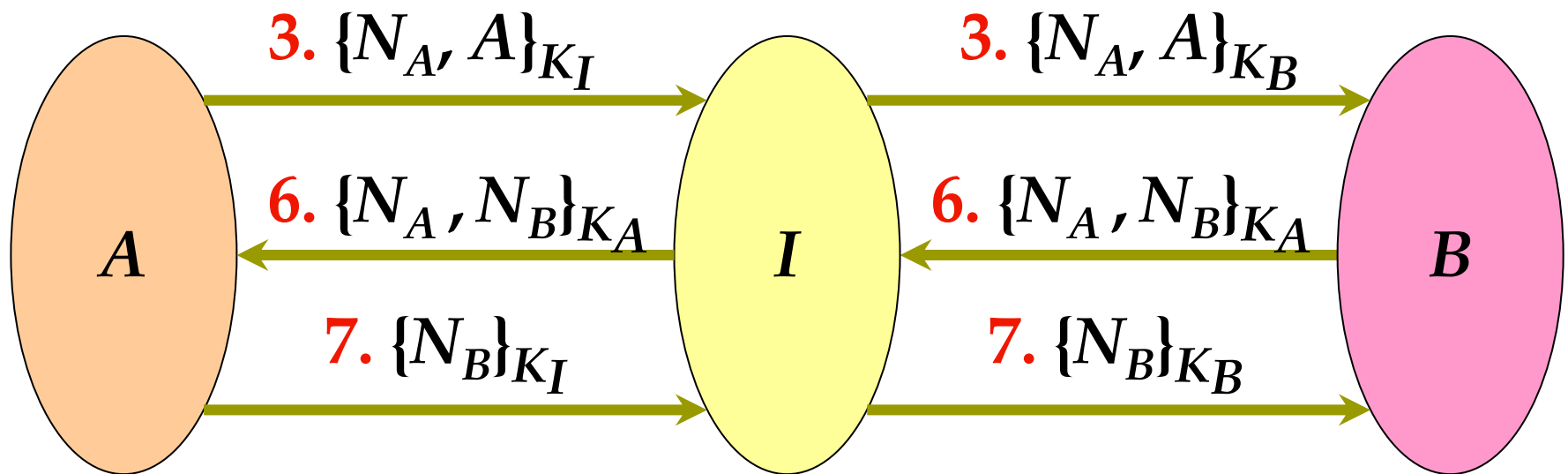
---

- 公開鍵の配信部分で replay 攻撃が可能
  - 最新の鍵が得られる保証がない
- 以下のような攻撃が可能
  - $I$  が攻撃者
  - $A$  は  $I$  が攻撃者とは知らず, セッションを開始
  - 並行して,  $I$  は  $B$  に対して  $A$  になりすましてセッションを開始



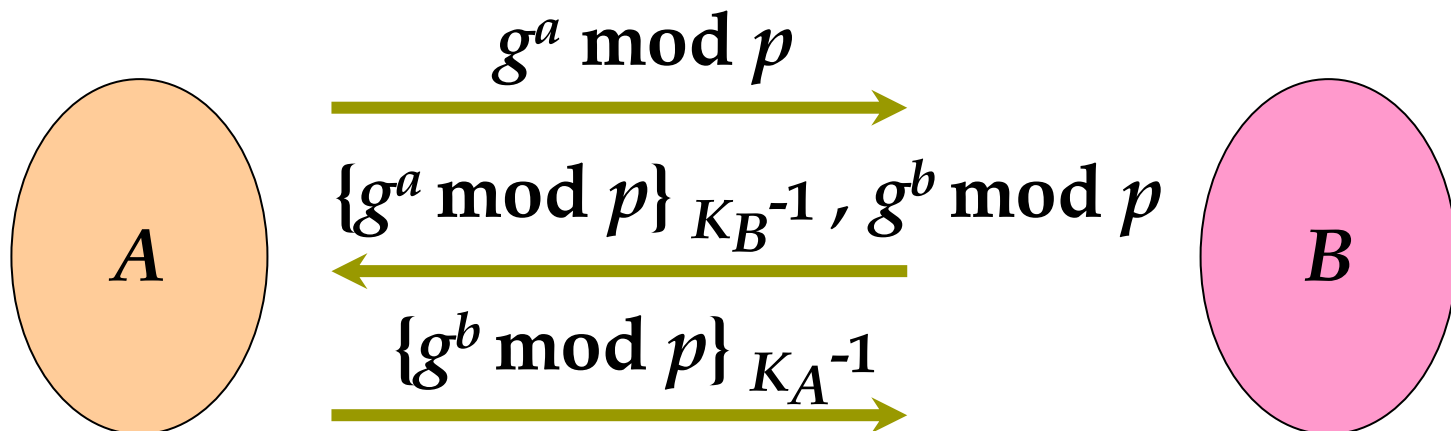
# Needham-Schroeder Protocol の 問題点 (2/2)

---



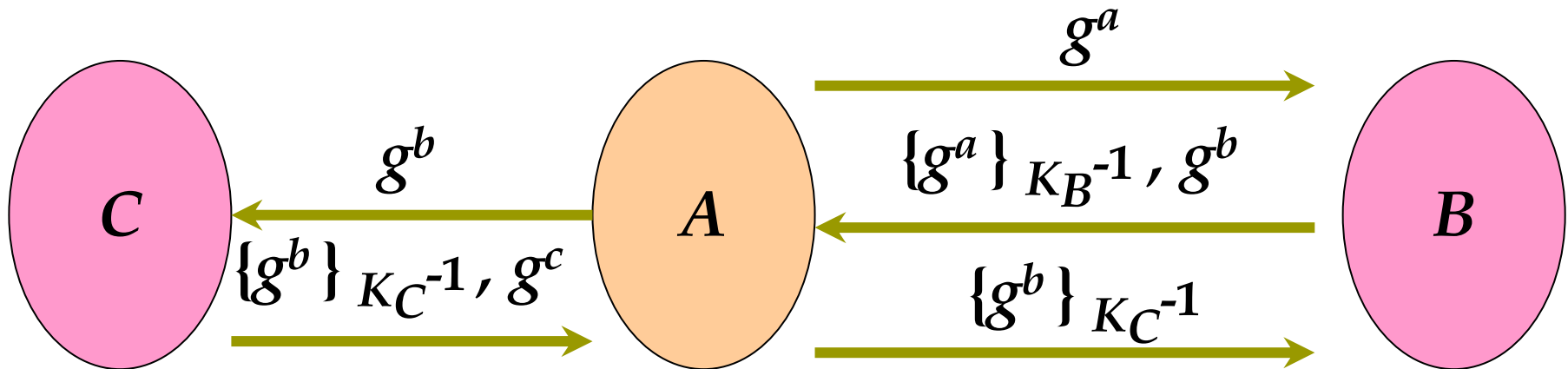
# Authenticated Diffie-Hellman Protocol (1/3)

- セッション鍵の合意と認証を同時に行いたい
  - 認証しないと成りすまし攻撃等が可能
  - 一度認証すると, 相手確認にセッション鍵が使える
- 署名を確認すれば認証できるわけではない



# Authenticated Diffie-Hellman Protocol (2/3)

- 一般には、送信者と署名者は別人
  - 他人が作ったデータに安易に署名するのは危険
- 以降、「 $\text{mod } p$ 」は省略する



# Authenticated Diffie-Hellman Protocol (3/3)

---

- $A, B$  は, それぞれ, 秘密の値  $\alpha, \beta$  を持ち,  $g^\alpha, g^\beta$  を公開
- $g^{\alpha\beta} (=K_{AB})$  を知りうるのは  $A, B$  のみ
  - この性質を利用して認証を行なう
- $g^a, g^b$  の代わりに  $g^{a K_{AB}}, g^{b K_{AB}}$  を使って Diffie-Hellman protocol を実行
  - (注)  $K_{AB}$  の値がわかれば  $g^{a K_{AB}}, g^{b K_{AB}}$  から  $g^a, g^b$  を求めることが可能

# 参考文献 (1/2)

---

## ■ RSA 暗号

- Ronald Rivest, Adi Shamir, and Leonard Adleman: A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, *Comm. of the ACM*, Vol. 21, pp. 120-126, 1978

## ■ ハッシュ関数の脆弱性

- Xiaoyun Wang and Hongbo Yu: How to Break MD5 and Other Hash Functions, *Proc. of Eurocrypt, LNCS 3494*, Springer-Verlag, 2005
- Vlastimil Klima: Tunnels in Hash Functions: MD5 Collisions Within a Minute, *Cryptology ePrint Archive, Report 2006/105*, 2006 <http://eprint.iacr.org/2006/105>
- Stefan Lucks and Magnus Daum: The Story of Alice and Her Boss: Hash Functions and the Blind Passenger Attack, *Eurocrypt Rump Session*, 2005 <http://www.cits.rub.de/MD5Collisions/><sub>23</sub>

# 参考文献 (2/2)

---

## ■ Diffie-Hellman

- Whitfield Diffie and Martin Hellman: New Directions in Cryptography, *IEEE Trans. on Information Theory*, Vol. 22, No. 6, pp. 644-654, 1976
- Whitfield Diffie et al.: Authentication and Authenticated Key Exchanges, *Designs, Codes and Cryptography*, vol. 2, pp. 107-125, 1992.

## ■ Needham-Schroeder

- Roger Needham and Michael Schroeder: Using Encryption for Authentication in Large Networks of computers, *Comm. of the ACM*, Vol. 21, No. 12, pp. 993-999, 1978
- Gavin Lowe: An attack on the Needham-Schroeder public-key authentication protocol, *Information Processing Letter*, Vol. 56, pp. 131-133, 1995