

授業アンケート (数学科「応用数学Ⅰ」)

「教員独自の設問」:

- (1) 数学科の他の情報系科目との連携は適切だったと思いますか
(独立し過ぎ ← 適切 → 重複し過ぎ)
- (2) 数学科の教職課程 (教科「情報」) の情報通信ネットワーク区分の科目として適切な内容だったと思いますか
(専門的過ぎ ← 適切 → 概論的過ぎ)
- (3) 数学科の4年配当の科目として適切な内容だったと思いますか
(専門的過ぎ ← 適切 → 概論的過ぎ)

期末試験のお知らせ

7月24日(木) 9:15 ~ 10:45

9-252教室 (ここじゃない)

- 今日(7/17)の講義内容まで
- 学生証必携

レポート提出について

期日: **8月4日(月)20時頃まで**

内容:

配布プリントのレポート問題の例のような内容、及び授業に関連する内容で、授業内容の理解または発展的な取組みをアピールできるようなもの(詳細はプリント参照のこと)

提出方法:

- 4-574 室扉のレポートポスト
- 電子メール

情報通信を行なう際の要請

- 効率的に → 情報理論
- 確実に → 符号理論
- 安全に → 暗号理論

暗号通信

公開された情報伝達路 (盗聴可能 と仮定) で、

暗号方式を公開 して通信

- 秘密鍵暗号 (共通鍵暗号)
- 公開鍵暗号

秘密鍵 (共通鍵) 暗号

暗号化鍵・復号鍵が同じ

- 換字暗号・Caesar 暗号
- 線型ブロック暗号
- Vernam 暗号
- DES (Data Encryption Standard)
- AES (Advances Encryption Standard)

秘密鍵 (共通鍵) 暗号の特徴

暗号化鍵・復号鍵が同じ

- 一般に原理は簡単で高速
- 事前の鍵共有の必要
- 通信相手毎に別の鍵が必要

公開鍵暗号

暗号化鍵 (公開鍵) ・ 復号鍵 (秘密鍵) が別

- 事前の鍵共有の必要無し

→

見ず知らずの人からも送ってもらえる

- **署名機能**がある

→ 改竄・なり済ましの対策

→ 否認防止の機能も持つ

公開鍵暗号

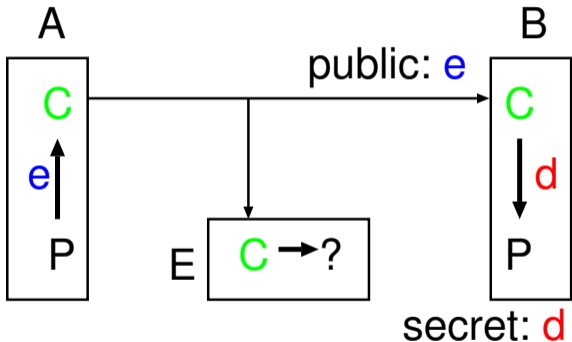
一般には、
暗号化・復号が共通鍵暗号に比べて低速

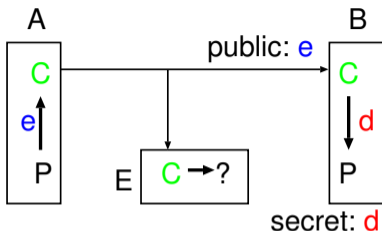
そこで、

- 始めに公開鍵暗号方式で鍵を送付・共有
- その鍵を用いて秘密鍵暗号方式で通信

というように、組合わせて用いることが多い。

公開鍵暗号による暗号通信

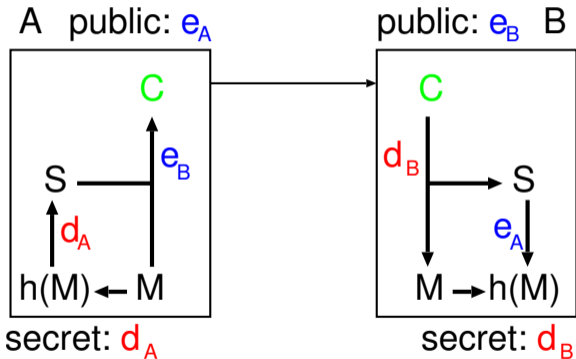




しかし、これだと誰でも暗号化できるので、
A 氏が送った保証がない。

→ 署名の必要性

公開鍵暗号を用いた署名



公開鍵暗号の特徴

- 暗号化は誰でも出来る
- 復号は秘密鍵を知らないと出来ない
(もの凄く時間が掛かる)

そんな都合の良い仕組みが本当にあるのか？

→ ある!! (多分大丈夫)

計算困難な問題 を利用

(素因数分解・離散対数問題)

代表的な公開鍵暗号方式

- **RSA 暗号 (Rivest-Shamir-Adleman)**
- **Diffie-Hellman 鍵共有**
- **ElGamal 暗号**

RSA 暗号 (Rivest-Shamir-Adleman)

p, q : 相異なる大きい素数
(実際には現在は 512 bit 程度)

$N := pq$: RSA 方式の法 (modulus)

$m := \text{lcm}(p - 1, q - 1)$

$$\begin{aligned}(\mathbf{Z}/N\mathbf{Z})^\times &\simeq (\mathbf{Z}/p\mathbf{Z})^\times \times (\mathbf{Z}/q\mathbf{Z})^\times \\ &\simeq \mathbf{Z}/(p-1)\mathbf{Z} \times \mathbf{Z}/(q-1)\mathbf{Z}\end{aligned}$$

: 指数 m の有限アーベル群

RSA 暗号 (Rivest-Shamir-Adleman)

p, q : 相異なる大きい素数

$$N = pq, m = \text{lcm}(p - 1, q - 1)$$

e を $\text{gcd}(e, m) = 1$ となるように選ぶ

d を $ed \equiv 1 \pmod{m}$ となるように求める

- (N, e) : 公開鍵 (暗号化鍵)
- d : 秘密鍵 (復号鍵)

RSA 暗号 (Rivest-Shamir-Adleman)

p, q : 相異なる大きい素数

$$N = pq, m = \text{lcm}(p - 1, q - 1)$$

$$ed \equiv 1 \pmod{m}$$

- (N, e) : 公開鍵 (暗号化鍵)
- d : 秘密鍵 (復号鍵)

平文 $M \pmod{N}$ の 暗号化: $C = M^e \pmod{N}$

暗号文 $C \pmod{N}$ の 復号: $M = C^d \pmod{N}$

公開鍵 (N, e) から秘密鍵 d が計算できるか？

- N の素因数分解 $N = pq$ を知っていれば容易
- 事実上 N の素因数分解と同程度の困難さ

「困難さ」… 計算時間が掛かる

RSA 暗号の安全性 \iff 素因数分解の困難さ

“計算量的安全性”

公開鍵 (N, e) から秘密鍵 d が計算できるか？

- N の素因数分解 $N = pq$ を知っていれば容易
- 事実上 N の素因数分解と同程度の困難さ

「困難さ」… 計算時間が掛かる

RSA 暗号の安全性 \iff 素因数分解の困難さ

“計算量的安全性”

公開鍵 (N, e) から秘密鍵 d が計算できるか？

- N の素因数分解 $N = pq$ を知っていれば容易
- 事実上 N の素因数分解と同程度の困難さ

「困難さ」・・・ 計算時間が掛かる

RSA 暗号の安全性 \iff 素因数分解の困難さ

“計算量的安全性”

計算量

入力データの大きさ (**bit 長**) に対する
計算の回数の オーダー で表す
(定数倍の違いは気にしない)

N **bit** の入力に対し

- $O(N^v)$: 多項式時間
- $O(e^{vN})$: 指数時間

計算量

素因数分解アルゴリズム等の計算量を表すのに

$$L_n[u, v] := \exp(v(\log n)^u (\log \log n)^{1-u})$$

が良く用いられる。

$N = \log n$ (n の桁数) とおくと、

- $L_n[0, v] = e^{v \log \log n} = N^v$: 多項式時間
- $L_n[1, v] = e^{v \log n} = e^{vN}$: 指数時間

素因数分解問題

現状では“準指数時間”のアルゴリズムしか
知られていない

- 楕円曲線法 (Elliptic Curve Method)
- 二次篩法 (Quadratic Sieve)
- 数体篩法 (Number Field Sieve)

素因数分解問題の高速なアルゴリズムの発見



RSA 暗号の解読

しかし、逆は真とは限らない。

(解読には色々な方法があり得る)

「何で負けても負けは負け」

素因数分解問題の高速なアルゴリズムの発見



RSA 暗号の解読

しかし、逆は真とは限らない。

(解読には色々な方法があり得る)

「何で負けても負けは負け」

離散対数問題 (Discrete Logarithm Problem)

p : 素数

$G := (\mathbf{Z}/p\mathbf{Z})^\times$: 位数 $p - 1$ の巡回群

$g \bmod p \in G$: $\bmod p$ の原始根 ($G = \langle g \rangle$)

とすると、

$x \bmod p \in G$ に対し、

$$g^a \equiv x \pmod{p}$$

となる a を求めよ。

Diffie-Hellman 鍵共有

離散対数問題の困難さを利用して、

公開通信路で秘密裡に鍵共有を行なう方式

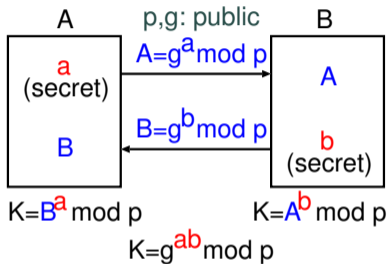
p : 素数

$G = (\mathbf{Z}/p\mathbf{Z})^\times = \langle g \rangle$: 位数 $p - 1$ の巡回群

A・B 両氏がそれぞれランダムに a, b を選ぶ



Diffie-Hellman 鍵共有



(p, g, A, B) が判っても a, b が判らない (DLP)

→ 秘密鍵 K の共有が可能

ElGamal 暗号

離散対数問題を利用し、乱数を用いた暗号方式

p : 素数

$G = (\mathbf{Z}/p\mathbf{Z})^\times = \langle g \rangle$: 位数 $p - 1$ の巡回群

受信者 **B** 氏がランダム (秘密) に b を選び、
 $B := g^b \bmod p$ を公開

送信者 **A** 氏がランダム (秘密) に a を選び、
 $A := g^a \bmod p, C := B^a M \bmod p$ を送信

ElGamal 暗号

受信者 **B** 氏がランダム (秘密) に b を選び、
 $B := g^b \bmod p$ を公開

送信者 **A** 氏がランダム (秘密) に a を選び、
 $A := g^a \bmod p$, $C := B^a M \bmod p$ を送信

受信者 **B** 氏は、 $M = (A^b)^{-1} C \bmod p$ を計算

ElGamal 暗号

平文 $M \longrightarrow$ 暗号文 (A, C)

- 送信データ長が 2 倍 (メッセージ膨張)
- 乱数により、同じ文書が毎回異なる暗号化

離散対数問題を利用した方式は
他の有限アーベル群でも可能

- 有限体上の楕円曲線の有理点の群
(楕円曲線暗号)
- 有限体上の超楕円曲線の
Jacobian の有理点の群
(超楕円曲線暗号)
- 代数体の ideal 類群

疑似乱数

充分ランダムに見える 長い周期の数列を
発生させるアルゴリズム

“**Mersenne Twister**”

… 現在、事実上最強のアルゴリズム