

# 電子署名 (PGP)

森田 互昭



# 電子署名とは

手書きサインや実印に相当する機能を電子的に代用する技術  
インターネット上でのメールを通じた商取引などに活用

インターネット上では、見ず知らずの人を相手にした取引  
他人による「成りすまし」の危険性

「成りすまし」を防止して、相手方の本人性を認証する必要

秘密鍵を世界にただ一つの「自分のサイン」とする

# PGP (Pretty Good Privacy)

- ◆ Philip R. Zimmermann

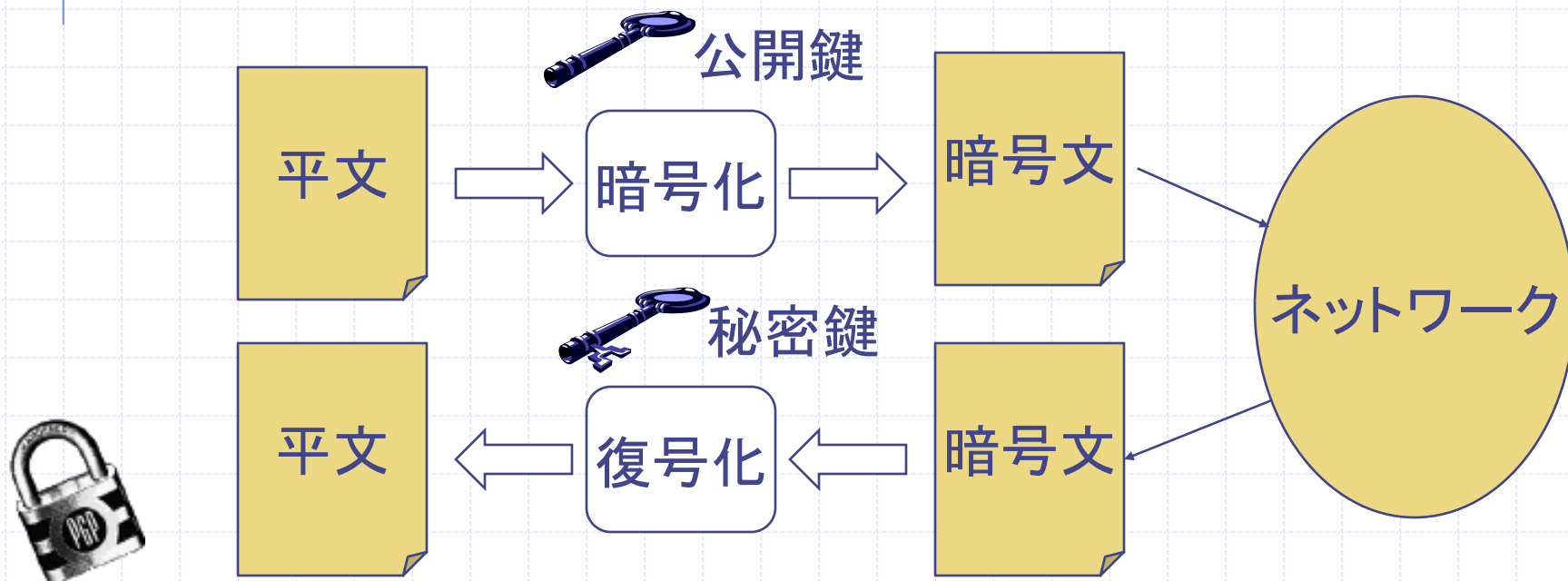
- ◆ 公開鍵暗号方式

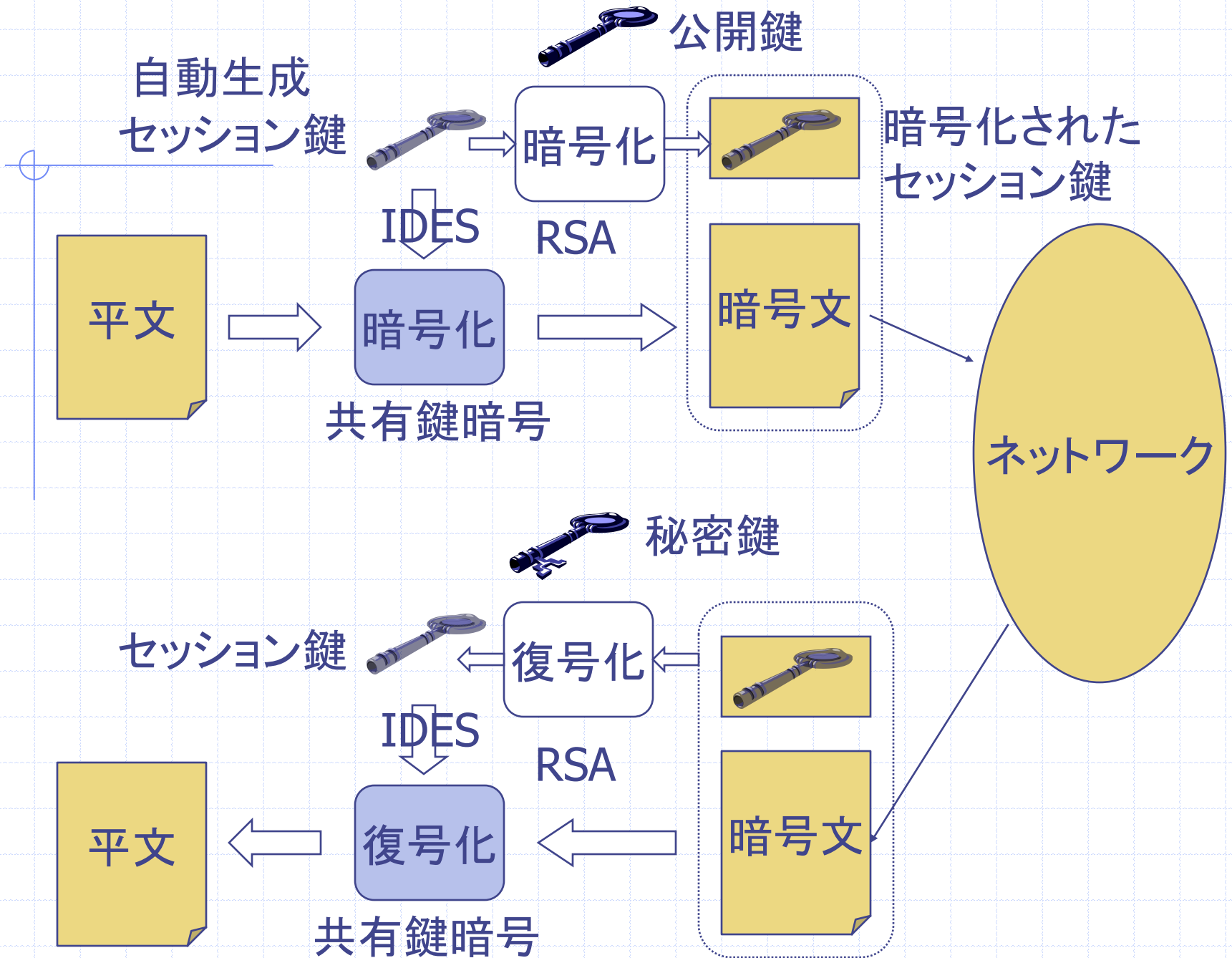
  - RSAアルゴリズム (version 2.x以前)



# 公開鍵暗号方式

- ◆ Diffie, Martin Hellman (1975)
- ◆ 暗号化と復号化を別々の鍵で行う
  - 「公開鍵」で暗号化された文書は、「秘密鍵」でしか復号化できない





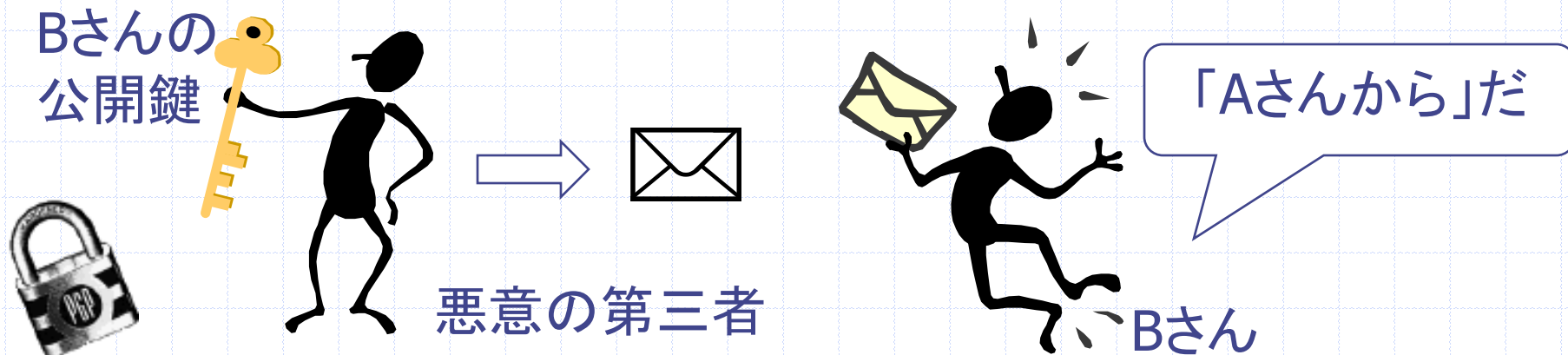
# 公開鍵？

## ◆「電子メールで送る」「Webに公開」

- **本物であるという保証**がない
- 途中で**改竄**されるかも

## ◆公開鍵で送られてきた暗号文

- **本当に本人から送られてきたのか？**

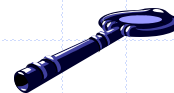


# 鍵の証明

- ◆ 直接会って公開鍵をもらう
- ◆ 信用の輪
  - 友達の友達は友達だ
- ◆ 鍵の指紋

Bさんのサインがある  
ので信用していいかな

Cさんの公開鍵



Bさんのサイン

Aさん ↔ Bさん ↔ Cさん

信頼している

お互いの「公開鍵」も完全に信頼できる

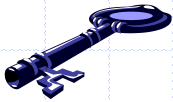


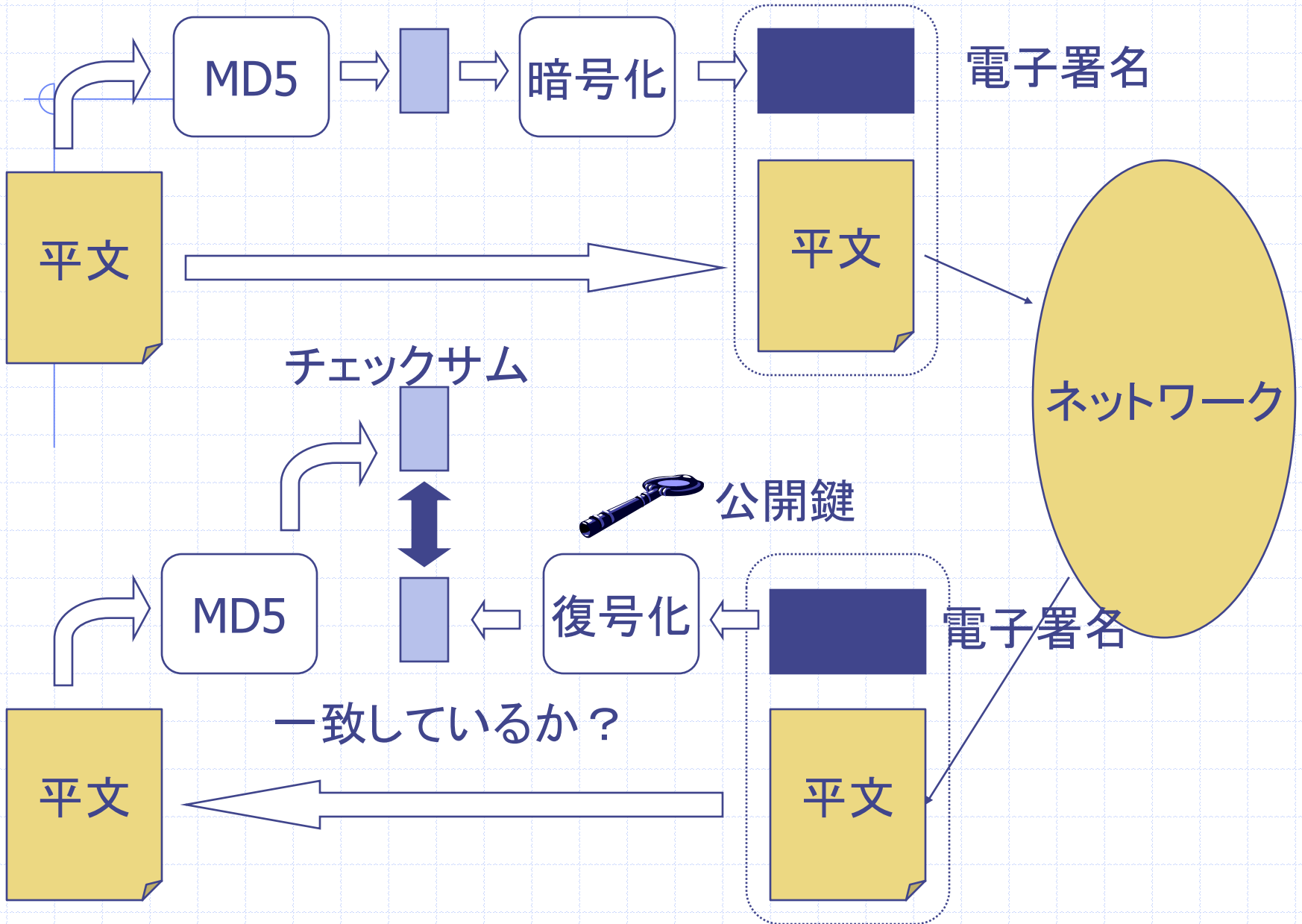
# 電子署名

- ◆ 公開鍵を使用して本人であることを確認
  - 「秘密鍵」で暗号化された文書は、「公開鍵」でしか復号化できない





チェックサム  秘密鍵



# 実習

## ◆ MewでPGPを使おう

- PGP2.6.3iをインストール
- PGPの設定
- PGPで暗号化したメールをMewで送信
- PGPで暗号化されたメールをMewで受信
- Mewで電子署名

「研究室のメールサーバのホスト名」は？の答えを  
自分のメールアドレス宛てにpgp暗号化したメールで送信し、  
受信したメールを複合化してみてください



<http://www.db.is.kyushu-u.ac.jp/~morita/pgp/morita.asc>

# PGP2.6.3iのインストール

- ◆ % su root
- ◆ % cd /usr/ports/security/pgp
- ◆ % make
- ◆ % make install



# 設定(pgp2.x)

## ◆ 鍵の生成

■ % pgp -kg

Pretty Good Privacy(tm) 2.6.3ia - Public-key encryption for the masses.  
(c) 1990-96 Philip Zimmermann, Phil's Pretty Good Software. 1996-03-04  
International version - not for use in the USA. Does not use RSAREF.  
Current time: 2001/07/09 09:30 GMT

Pick your RSA key size:

- 1) 512 bits- Low commercial grade, fast but less secure
- 2) 768 bits- High commercial grade, medium speed, good security
- 3) 1024 bits- "Military" grade, slow, highest security

Choose 1, 2, or 3, or enter desired number of bits:

**3を選ぶ**



You need a user ID for your public key. The desired form for this user ID is your name, followed by your E-mail address enclosed in <angle brackets>, if you have an E-mail address.

For example: John Q. Smith <12345.6789@compuserve.com>

Enter a user ID for your public key:

## ユーザIDを決める

例 Nobuaki Morita <morita@db.is.kyushu-u.ac.jp>

- パスフレーズを聞かれるので入力
- 確認のためもう一度
- 乱数を入力: キーボードを適当にたたきだけ

\$HOME/.pgp/にファイルが作成

pubring.pgp 公開鍵ホルダー

secring.pgp 秘密鍵ホルダー

(Errorが出たら、\$homeに自分で.pgpディレクトリを作ってもう一回)

# PGPのコマンド(1)

## ◆ 公開鍵を取り出す

- % `pgp -kx ユーザ名 ファイル名`
  - ◆ ファイル名.pgpというファイルが作成される
  - ◆ **バイナリファイル**
  - ◆ 例 ユーザ”morita”の公開鍵を取り出す  
`%pgp -kx morita morita`
- % `pgp -kxa ユーザ名 ファイル名`
  - ◆ ファイル名.ascというファイルが作成される
  - ◆ **テキストファイル(メール等でやりとりができる)**



# PGPのコマンド(2)

## ◆ 公開鍵を登録

- % `pgp -ka ユーザ名 ファイル名{.pgp or asc}`

鍵の信用について質問があるので下記のホームページ等を参考に

<http://www.cc.u-ryukyu.ac.jp/~k008367/lab/pgp/pgp263ka.htm>



# PGPのコマンド(3)

## ◆ その他

- %pgp -kc
  - ◆ 鍵に付いている署名をチェック
- %pgp -kvc
  - ◆ 公開鍵の指紋を表示
- %pgp -h
  - ◆ ヘルプ





# Mewで暗号メール

## ◆ メールを暗号化

draftモードで**C-c C-e**

## ◆ 暗号化されたメールを読む

- SummaryモードでEのマーク = 暗号化されたメッセージ
- **スペース**でメールを読もうとするとパスフレーズを要求される
- 正しくパスフレーズを打つと自動的に復号



# Mewで電子署名(1)

◆ メールに電子署名

Draftモードで**C-c C-s**

◆ メールに電子署名をしかつ暗号化

Draftモードで**C-c C-b**



# Mewで電子署名(2)

## ◆ 電子署名されたメールを読む

- Summaryモードで**S**というマーク = 電子署名が付いているメール
- 普通にメールを読むようにSマークが付いたメールで**スペース**を押す
- 相手の公開鍵を持っていてかつ電子署名の検証に成功するとメッセージのヘッダに  
**X-Mew:Good PGP sign “ID..”**



# Mewで電子署名(3)

- ◆ 相手の公開鍵を持っていないと、  
**X-Mew: No his/her public key. ID = (key ID)**  
とヘッダ部に表示される -- **C-c C-f** で公開鍵サーバ  
から公開鍵を **get** して追加できる
- ◆ 自分の公開鍵を送信
  - **draft** モードで **C-c C-a** 打って **multipart** 作  
成モードに入った後、**p**



# PGPのバージョン

Version 2.x	Version 5.x	Version 6.x
RSA	RSA ElGamal/DSS	ElGamal/DSS
IDEA	3DES	3DES
MD5	MD5 SHA-1	SHA-1



# PGP5.xとの共存

- ◆ MewでPGP2.xと5.xを共存させたい方は下記のホームページを参考に
  - <http://minerva.jaist.ac.jp/pgp.html>

