平成１０年度プロジェクト研究構想発表

「ファイル暗号化セキュリティボックスの開発」

担当教官　：大岩幸太郎教官
担当者　：　　０７１０２９４
佐藤利明

目　次

１　情報セキュリティーと暗号

通信

インターネットの電子メールは普通、相手に届くまでにいくつかのサーバーに仲介される

・途中で誰かに読まれてしまう
・匿名や、他人の名をかたったメール
（なりすまし）

ソフトウェア

保存しているファイルの中身を第三者から盗み見される

確実性の高い解決策→暗号化

暗号（encrypt）

「通信の内容が、当事者以外には解読できないように普通の文字・記号を一定の約束（アルゴリズム）で他の記号に置き換えたもの」

２　暗号とその歴史

a）シーザー暗号　　（換字暗号）

ABCDEFGHIJKLMNOPQRSTUVWXYZ

↓

BCDEFGHIJKLMNOPQRSTUVWXYZA

例）　ENCRYPT　→　FODSZQU

b）拡張シーザー暗号　　（換字鍵暗号）

鍵を二個用意　　**A　B**

奇数番目の文字→**A**の鍵
偶数番目の文字→**B**の鍵

例）鍵がＢＣの場合

AA　→　BC　　OA　→　PC

ENCRYPT　→　FPDTZRU

c）多表式暗号

変換規則表を複数用意しそれぞれの表の規則に従って暗号化・復号化をする

暗号表の例）

ABCDEFGHIJKLMNOPQRSTUVWXYZ

↓

JDGKOSALFNQVZRTIWMHUBCEPYX

d）エニグマ暗号（enigma：謎）

周期の異なる輪を組み合わせて長い周期の鍵を作り出す

素数の周期：11, 13, 17, 19, 23, 29, 31

$$11\times13\times17\times19\times23\times29\times31=955049953\ \ 10^{9}$$

３　慣用暗号

３．１　ブロック暗号

ブロック暗号：「十数ビット以上の比較的長いデータブロックごとに暗号化・復号化する」

例）ＤＥＳ暗号（ＤＥＳ：Ｄａｔａ　Ｅｎｃｒｙｐｔｉｏｎ Ｓｔａｎｄａｒｄ）

使用例）ＵＮＩＸのパスワード

暗号化：Ｃ＝ＥＫ（Ｍ）
復号化：Ｍ＝ＤＫ（Ｃ）

Ｍ：平文ブロック　Ｃ：暗号文ブロック
Ｋ：鍵を表すブロック
Ｅ：暗号化　Ｄ：復号化

特徴
- 平文ブロックと暗号文ブロックの長さ（ビット長）が同じ
- 暗号化手順と復号化手順の大部分が同じ

３．２　ストリーム暗号

ストリーム暗号：「1ビット～数ビットの小データブロックごとに暗号化する」

例）バーナム暗号

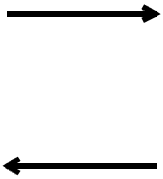
暗号化：C＝M Å K
復号化：M＝C Å K

M：平文を表すシンボル系列
C：暗号文を表すシンボル系列
K：乱数シンボル系列
Å：一ビット対応の排他的論理和

排他的論理和を使った暗号化計算

排他的論理和		
変数p	変数q	演算結果
0	0	0
0	1	1
1	0	1
1	1	0

暗号化		
元の文章	鍵	復号化の結果
1	1	0
1	1	0
0	1	1
0	1	1
1	1	0
0	1	1
1	1	1



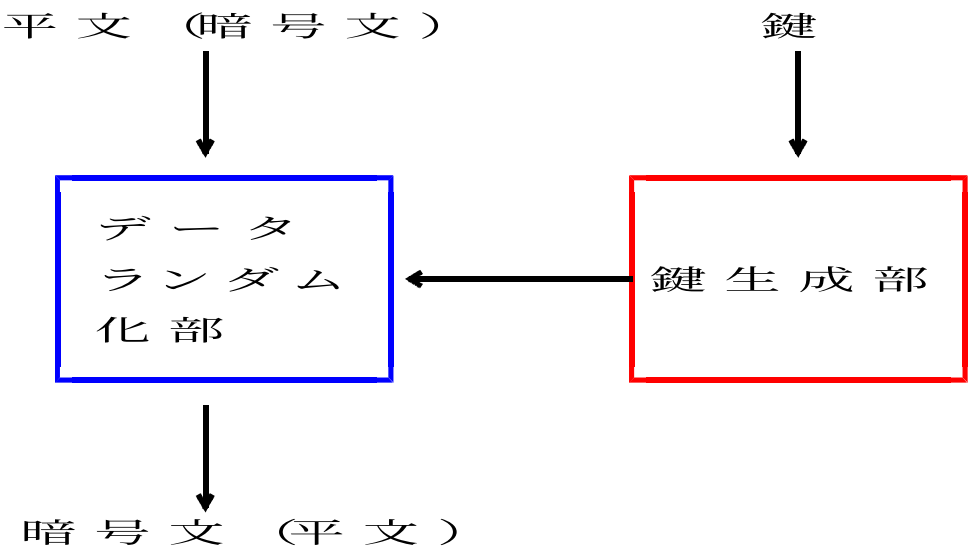
復号化		
暗号文	鍵	復号化の結果
0	1	1
0	1	1
1	1	0
1	1	0
0	1	1
1	1	0
0	1	1

４　新しい暗号アルゴリズム

４．１　アルゴリズム公開型慣用鍵暗号

特徴　・アルゴリズムを公開
・集積回路（ＬＳＩ）技術に応用

ＤＥＳ暗号・ＦＥＡＬ暗号
（ＦＥＡＬ：Ｆａｓｔ　Ｄａｔａ
Ｅｎｃｉｐｈｅｒｍｅｎｔ　Ａｌｇｏｒｉｔｈｍ）



４．２　公開鍵暗号

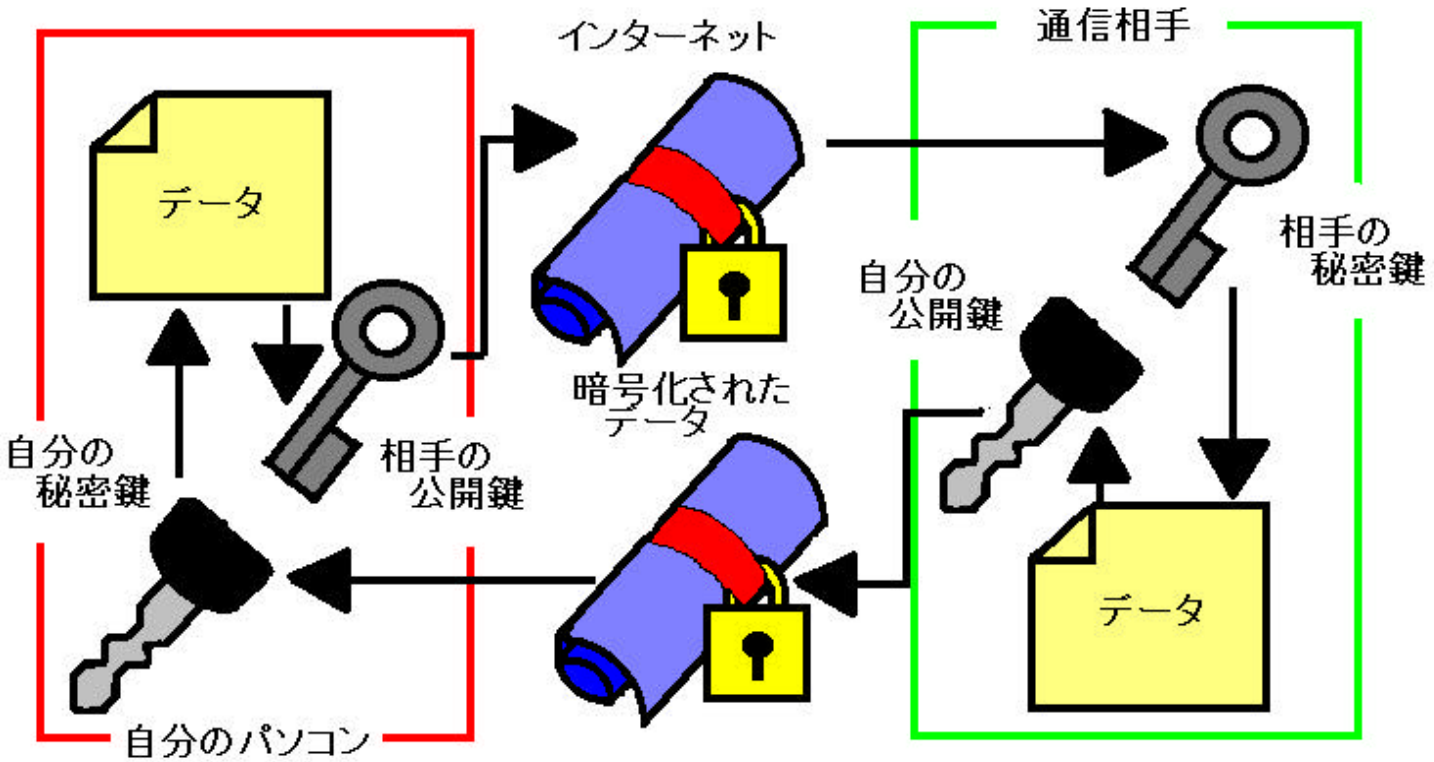
公開鍵暗号

①各人が暗号化鍵と復号化鍵を一対づつ作成
②暗号化鍵を公開
③復号化鍵を秘密に保持

特徴
- 鍵を配送する必要がない
- 鍵の数が少なくて済む
- ディジタル署名が可能である

ＲＳＡ暗号（R. L. Rivest　A. Shamir　L. Adleman）

１５０桁以上の素因数分解が困難な特性を利用
↓
片方向性の鍵が作成できる



電子署名

電子署名：

データを送ったのが本当に本人かを確認

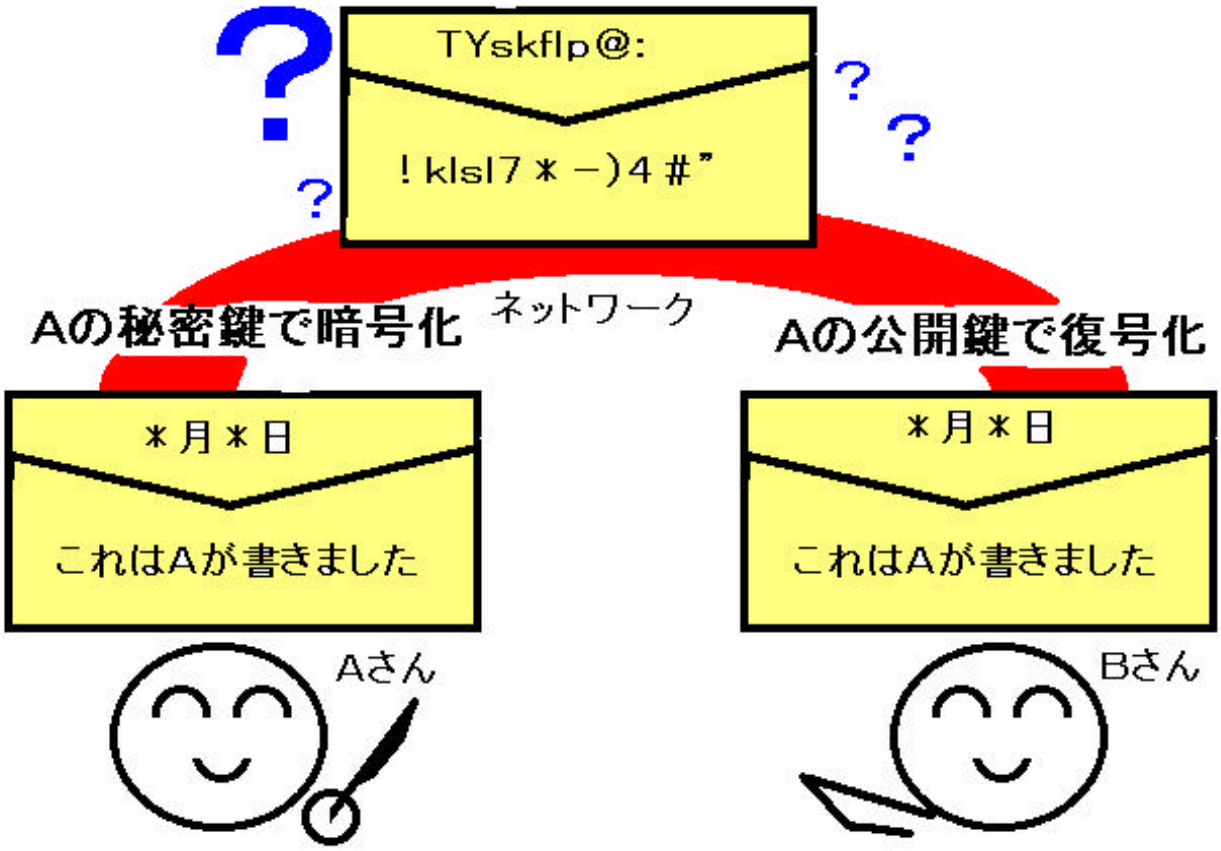
ポイント：

・書いた本人以外の者による
署名文の偽造が出来ない

・書いた本人が後で署名文を否定できない

使用例）

インターネットでの商取引　等



５　今後の展開

・ファイルセキュリティーボックスの開発

・暗号アルゴリズム学習ＣＡＩの開発

６　参考文献・参考サイト

「暗号と情報セキュリティー」
辻井重男・笠原正雄編著　昭晃堂
（序章・二章・三章・九章・十章）

「暗号」
辻井重男　講談社
（一章・二章・四章・五章）

「セキュリティハンドブックII」
セキュリティ・マネジメント学会編日科技連
（一章・三章・四章）

「日本ＲＳＡ株式会社」
http://www.rsa-japan.co.jp/

「かつきのページ」
http://www2m.biglobe.ne.jp/~katuki/rsa/

「Ｙｏのホームページ」
http://www.geocities.co.jp/SiliconValley/2008

「ＥＬＮＩＳ　ｈｏｍｅ ｐａｇｅ」
http://www.elnis.com/MISC/angou7.html