

情報通信工学実験 A・B

1. 情報通信 (情報・セキュリティ)

栗原正純 kuri @ ice.uec.ac.jp
電気通信大学大学院情報理工学研究所
〒 182-8585 東京都調布市調布ヶ丘 1-5-1
<http://www.code.ice.uec.ac.jp/kuri/C3/>

(11x3: /doc/tex/uec/jikken/2010/, time:2010/11/16/15:45)

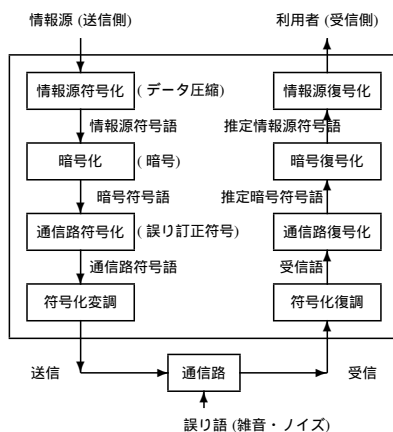
情報通信工学実験 A・B 実験項目 1. 情報通信 — 情報・セキュリティ —

1. 「データ圧縮の理解と実装」
— ハフマン符号の理解と実装 (プログラミング) —
2. 「暗号化の理解と実装」
— RSA 暗号の理解と実装 (プログラミング) —
3. 「誤り訂正符号の理解と実装」
— リード・ソロモン符号と最小距離復号の
理解と実装 (プログラミング) —

キーワード: 『符号化』

1/ 36

デジタル通信システム



3/ 36

「暗号化の理解と実装」 — RSA 暗号の理解と実装 (プログラミング) —

目的

提出レポートの内容

1. はじめに
2. 暗号化
 - 2.1 暗号の具体例 (シフト暗号)
 - 2.2 暗号化システムの形式的記述
 - 2.3 二つの暗号システム 公開鍵暗号 と 秘密鍵暗号
3. 数学的準備 (整数の諸性質)
4. RSA 暗号 (公開鍵暗号)
5. 課題
6. プログラミング

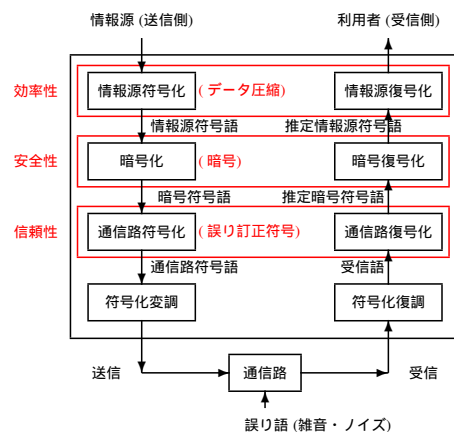
5/ 36

提出レポートの内容

1. 「RSA 暗号」をキーワードにして「暗号」と「認証」について調べたことを 1 ページ以内 (A4 サイズ) に簡潔にまとめ、記述する。
2. プログラミングで工夫した点を記述する。
3. 印刷したプログラムのソースをレポートに添付する。
4. 参考文献 を明記する。
自分のアイデアと他人のアイデアを明確に区別すること。
5. 紙のレポートとは別に、ソースプログラムをメールにて担当教員宛に送る。
kuri@ice.uec.ac.jp
その際、そのファイルのコンパイル方法、実行方法を明記する。
 1. Subject: 3jikken(name)
 2. 「氏名」と「学籍番号」を書くこと。

7/ 36

デジタル通信システム



4/ 36

目的 (課題)

1. 暗号の一つである **RSA 暗号** の具体的な **暗号化** と **復号化** の方法について **理解する**。
2. 次に、RSA 暗号の暗号化と復号化の **プログラムを作成し**、計算機上で **実装する**。

6/ 36

1. はじめに

テキストの目的:

本実験課題で扱う RSA 暗号とよばれる暗号化アルゴリズムの説明、および、その実装のための諸注意などを説明することにある。

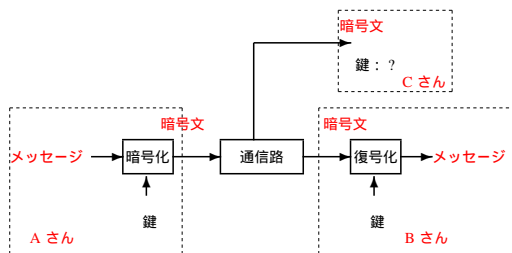
R.L.Rivest, A. Shamir and L. Adleman,
“A Method for Obtaining Digital Signatures and Public-Key
Cryptosystems,”
Communications of the ACM, 21(1978), pp.120–126, 1978.

一般的な暗号については、
暗号に関連する講義や暗号の専門書にゆずる。

8/ 36

2. 暗号化

A さんから B さんへ伝えたいメッセージを第三者の C さんに見られても分からないように、メッセージを暗号化することを考える。



9/ 36

2.1 暗号の具体例 (シフト暗号)

定義 (シフト暗号)

メッセージおよびメッセージを暗号化した暗号文 はいずれも 26 文字のアルファベット:

ABCDEFGHIJKLMNOPQRSTUVWXYZ

により構成されているものとする。

1. 暗号化 (鍵 k): メッセージ $\rightarrow$ 暗号文
辞書順に従って 右へ k だけ (循環) シフト させる変換
2. 復元 (復号化) (鍵 k): 暗号文 $\rightarrow$ もとのメッセージ
辞書順に従って 左へ k だけ (循環) シフト させる変換

10/ 36

「シフト」の例 (鍵の値を $k = 5$ とする)

1. “I” を右へ 5 だけシフト変換すると “N”

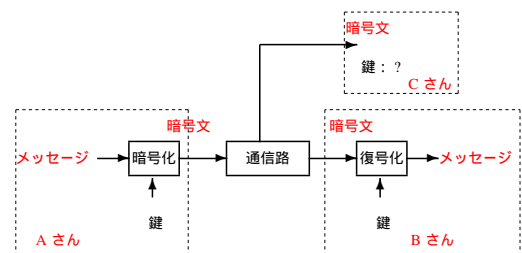
...	I	J	K	L	M	N	...
	$\rightarrow$	$\rightarrow$	$\rightarrow$	$\rightarrow$	$\rightarrow$		
	1	2	3	4	5		

2. “W” を右へ 5 だけ (循環) シフト変換すると “B”

...	W	X	Y	Z	A	B	...
	$\rightarrow$	$\rightarrow$	$\rightarrow$	$\rightarrow$	$\rightarrow$		
	1	2	3	4	5		

11/ 36

暗号システムの概念図



A さんから B さんへ暗号文を送信する前に、鍵情報 k を共有しておく必要がある。

しかも、鍵情報は、第三者の C さんには知られていないものとする。

12/ 36

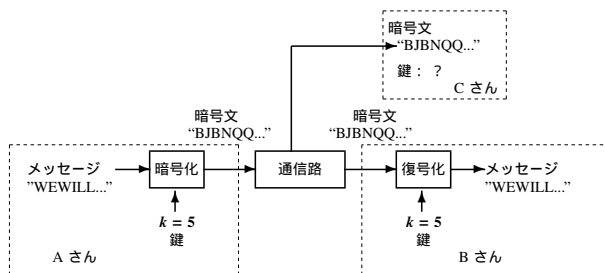
例えば、鍵を $k = 5$ とし、A さんが B さんに伝えたいメッセージ

WEWILLMEETATCHOFUSTATION

を暗号化するとその暗号文は、

BJBNQQRJJYFYHMTKZXIFYNTS

となる。これを B さんに送信すればよい。



13/ 36

「文字」から「整数」へ

すなわち、

「シフト処理」から「算術演算処理」へ

を考える。そこで、

「ASCII」

を復習しよう。

14/ 36

大文字 “A” の 2 進数表現、10 進数表現

ASCII の表より、

上位: 4 $\Leftrightarrow$ 0100

下位: 1 $\Leftrightarrow$ 0001

これより、

$A \Leftrightarrow 01000001 \Leftrightarrow 65$

なぜなら、

$$01000001 \Leftrightarrow 2^6 + 2^0 = 64 + 1 = 65$$

15/ 36

「文字」 「整数」

$$\{A, B, \dots, Z\} \Leftrightarrow Z_{26} := \{65, 66, \dots, 90\}$$

A	B	C	D	E	F	G	H	I	J	K	L	M
65	66	67	68	69	70	71	72	73	74	75	76	77
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
78	79	80	81	82	83	84	85	86	87	88	89	90

16/ 36

「シフト処理」 「算術演算処理」

1. “I” を右へ5だけシフト変換すると“N”

...	I	J	K	L	M	N	...
	73					78	

$$73 + 5 = 78$$

2. “W” を右へ5だけ(循環)シフト変換すると“B”

...	W	X	Y	Z	A	B	...
	87					66	

$$87 + 5 = 92,$$

$$92 \equiv 66 \pmod{26}.$$

(「文字」から「整数」へ)

メッセージ:

WEWILLMEETATCHOFUSTATION

を ASCII に従って整数に変換すると

87 69 87 73 76 76 77 69 69 84 65 84 67 72 79 70 85 83 84 65 84 73 79 78

となる。

鍵 $k = 5$ の場合、その暗号文は、

66 74 66 78 81 81 82 74 74 89 70 89 72 77 84 75 90 88 89 70 89 78 84 83

となる。

注意: 各文字を数字で表現した場合に「区切り文字」として、空白を挿入していることに注意する。

区切り文字がないと次のようになってしまう。

8769877376776969846584677279708583846584737978

667466788181827474897089727784759088897089788483

17/ 36

18/ 36

2.3 二つの暗号システム

暗号システムを

「秘密鍵暗号システム」
(または、「共通鍵暗号システム」ともよぶ)

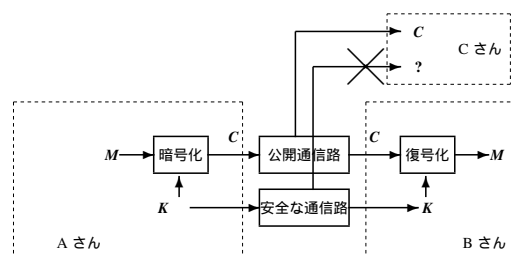
と

「公開鍵暗号システム」

の2種類に分類する。

2.3.1 秘密鍵暗号システム (共通鍵暗号システム)

1. 暗号化鍵 K を第三者には秘密にする



秘密鍵暗号システムの問題点

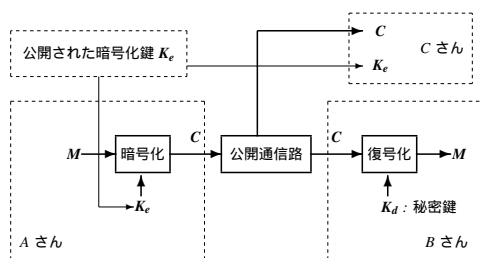
第三者には知られないように暗号化鍵 K を共有する必要がある。
すなわち、安全な通信路を利用して送信する必要がある

19/ 36

20/ 36

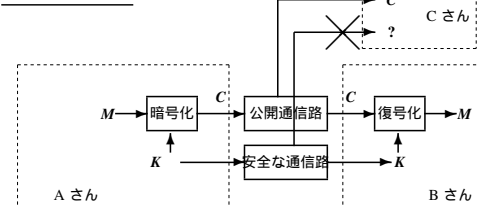
2.3.2 公開鍵暗号システム

- 暗号化鍵 K を第三者にも公開することができる
- ゆえに、安全な通信路を利用して通信する必要がない
- 公開された暗号化鍵 K_e とは異なる秘密鍵(復号化鍵) K_d により暗号文を復号化することができる
- RSA 暗号は、公開鍵暗号システム的一种である

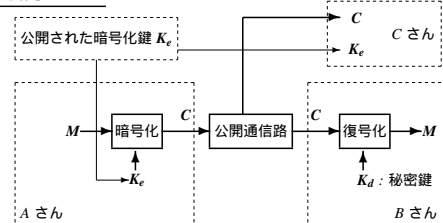


21/ 36

秘密鍵暗号システム



公開鍵暗号システム



22/ 36

○ 秘密鍵暗号システムと公開鍵暗号システムの違い

- 秘密鍵暗号システム: 「暗号化鍵 K_e 」 = 「復号化鍵 K_d 」
その結果、鍵 $K_e = K_d$ を第三者に分からないように通信し、共有する必要がある
- 公開鍵暗号システム: 「暗号化鍵 K_e 」 $\neq$ 「復号化鍵 K_d 」
その結果、暗号化鍵を共有する必要はない

○ 誰が鍵を作成するのか?

- 秘密鍵暗号システム:
送信者(Aさん)、または受信者(Bさん)のどちらか一方が鍵を作成する。そして、鍵の情報が第三者に分からないように、相手に鍵を渡す。
- 公開鍵暗号システム:
受信者(Bさん)が、公開鍵と秘密鍵の両方を作成する。
そして、公開鍵を公開する一方、秘密鍵は秘密に保管する。

4. RSA 暗号

暗号化鍵(公開鍵)と復号化鍵(秘密鍵)を作成するために、いくつかの整数を選択し、計算をする。

1. 任意の互いに異なる素数 p と q を選び、その積 $p \times q$ を計算する。

$$n := p \times q$$

2. $(p-1)$ と $(q-1)$ の最小公倍数 (least common multiple) L を計算し、 L と互いに素で L より小さな任意の整数 e を選ぶ。

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

$$e \text{ such that } \text{gcd}(e, L) = 1 \text{ and } 1 < e < L$$

ここで、 $\text{gcd}(e, L)$ は、 e と L の最大公約数 (greatest common divisor) を表す。

3. 次式を満たす整数 d_e を計算する。(拡張 Euclid 法を利用する)

$$d_e \text{ such that } e \times d_e \equiv 1 \pmod{L}$$

23/ 36

24/ 36

1. 暗号化鍵 (公開鍵): (e, n)
2. 復号化鍵 (秘密鍵): (d_e, n)
3. 秘密にする情報: p, q, d_e

25/ 36

1. Select (p, q)
2. $n := p \times q$
3. $L := \text{lcm}(p-1, q-1)$
4. e such that $\text{gcd}(e, L) = 1$ and $1 < e < L$
5. d_e such that $e \times d_e \equiv 1 \pmod{L}$

たとえば、

1. $(p, q) = (17, 19)$
2. $n = p \times q = 17 \times 19 = 323$
3. $L = \text{lcm}(17-1, 19-1) = \text{lcm}(16, 18) = 2 \times 2 \times 2 \times 2 \times 3 \times 3 = 144$
4. $e = 5$ such that $\text{gcd}(e, 144) = 1$ and $1 < e < 144$
 $e \in \{5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35, \dots, 139, 143\}$
5. $d_e = 29$ such that $5 \times d_e \equiv 1 \pmod{144}$

26/ 36

暗号化と復号化について

メッセージも暗号文も「文字」から「整数」に変換されているものとする。

1. 暗号化:
公開鍵 (e, n) を用いて メッセージ (整数) M を暗号化する。

$$C \equiv M^e \pmod{n}$$

C が M の暗号文になる。ただし、 $0 \leq C \leq n-1$ とする。

2. 復号化:
復号化鍵 (d_e, n) を用いて 暗号文 (整数) C を復号する。

$$\hat{M} \equiv C^{d_e} \pmod{n}$$

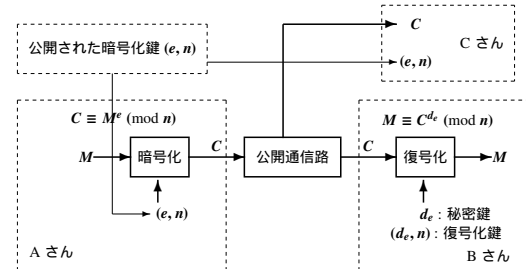
$\hat{M}$ が C を復号したメッセージになる。ただし、 $0 \leq \hat{M} \leq n-1$ とする。

3. 復号したのであるから $\hat{M} = M$ であって欲しい。
実際に、次式が成り立つ事より、 $\hat{M} = M$ が保証される。

$$\hat{M} \equiv C^{d_e} = (M^e)^{d_e} = M^{e \times d_e} \equiv M \pmod{n}$$

27/ 36

RSA 暗号を用いた公開鍵暗号システム



28/ 36

26 文字のアルファベットで記述されたメッセージ (ひら文) を RSA 暗号で暗号化することを考える。

1. 二つの素数 p, q を、 $n = pq \geq 26$ を満たす $(p, q) = (17, 19)$ とする
 $n = 17 \times 19 = 323$
2. $(p-1)$ と $(q-1)$ の最小公倍数 L を計算する $L = 144$
3. $1 < e < 144 = L$ を満たし、 L と互いに素な整数 e を求める
 $e = 5$
4. 秘密鍵 d_e を計算する $d_e = 29$

以上より、

1. 公開鍵 (暗号化鍵) : $K = (e, n) = (5, 323)$
2. 秘密鍵 : $d_e = 29$
3. 復号化鍵 : $(d_e, n) = (29, 323)$

29/ 36

文字 “C” 数字 “67” : これを 暗号化/復号化 してみよう。

1. メッセージ $M = 67$,
2. 暗号化: $K = (e, n) = (5, 323)$
 $C \equiv M^e = (67)^5 \equiv 288 \pmod{323}$
3. 復号化: $(d_e, n) = (29, 323)$.
復号化 : $\hat{M} \equiv C^{d_e} = (288)^{29} \equiv 67 \pmod{323}$

上記の計算は、電卓でもできる:

- 1) $(67)^2 \equiv 67 \times 67 = 4489 \equiv 290 \pmod{323}$,
- 2) $(67)^3 \equiv 290 \times 67 = 19430 \equiv 50 \pmod{323}$,
- 3) $(67)^4 \equiv 50 \times 67 = 3350 \equiv 120 \pmod{323}$,
- 4) $(67)^5 \equiv 120 \times 67 = 8040 \equiv 288 \pmod{323}$.

各結果は、0 から $322 \times 322 = 103684$ の間の数字であることに注意

30/ 36

数式処理システム Mathematica (マセマティカ) による計算例

```

IED: hostname
ied1
IED: math
Mathematica 5.2 for Sun Solaris (UltraSPARC)
Copyright 1988-2005 Wolfram Research, Inc.
-- Terminal graphics initialized --

In[1]:= (67)^(5)
Out[1]= 1350125107
In[2]:= Mod[(67)^(5), 323]
Out[2]= 288
In[3]:= (288)^(29)
Out[3]=
210078759859150987224561197336654397674351288252695054617776181894709
> 248
In[4]:= Mod[(288)^(29), 323]
Out[4]= 67
In[5]:= Quit
IED:

```

31/ 36

○暗号化: 暗号化鍵 $(e, n) = (5, 323)$ を用いてメッセージ:

WEWILLMEETATCHOFUSTATION

を暗号化しよう。

まず、各文字を ASCII に従って整数に変換:

87 69 87 73 76 76 77 69 69 84 65 84 67 72 79 70 85 83 84 65 84 73 79 78

暗号化鍵 $(e, n) = (5, 323)$ を用いて暗号化すると、
暗号文は以下のように計算される:

83 103 83 99 247 247 229 103 103 50 12 50 288 21 129 185 187 87 50 12 50 99 129 108

○復号化: 秘密鍵を含む復号化鍵 $(d_e, n) = (29, 323)$ を用いて暗号文 (各数字) を復号すればよい。

注意: 暗号文に区切り記号の空白がないと...

831038399247229103103501250288211291851878750125099129108

32/ 36

5. 課題

RSA 暗号の理解と実装に関連する実験テーマとして以下の 5 個の課題を必修とする。

1. RSA 暗号の暗号化および復号化のプログラムを作成し、実装せよ。
具体的には、以下のような暗号化および復号化の仕様を満たすこと。

暗号化:

入力: 暗号化鍵 (e, n) とメッセージ (ひら文) のファイル。

出力: 暗号化されたファイル。

復号化:

入力: 復号化鍵 (d, n) と暗号化されたファイル。

出力: 元のメッセージ (ひら文) のファイル。

このとき、メッセージ (ひら文) のファイルと暗号化されたファイルのサイズを比較せよ。

33/ 36

課題 1 の RSA 暗号の暗号化・復号化プログラムを作成した後に、以下の課題 2 ~ 5 を行なうことが望ましい。

2. 1 から 10000 までの間に存在する素数をすべて求めるプログラムを作成し、実装せよ。
3. 異なる素数 p と q に対し、 $p-1$ と $q-1$ の最小公倍数 $L = \text{lcm}(p-1, q-1)$ を求めるプログラムを作成し、実装せよ。
4. 整数 L に対し、 $\text{gcd}(e, L) = 1$ かつ $1 < e < L$ を満たす正整数 e を求めるプログラムを作成し、実装せよ。
5. 整数 L と e に対し、 $ed \equiv 1 \pmod{L}$ を満たす正整数 d を求めるプログラムを作成し、実装せよ。

34/ 36

6. プログラミング

6.1 プログラミングの準備

6.2 参考プログラム <http://www.code.ice.uec.ac.jp/kuri/C3>

1. RSA 暗号の暗号化 (符号化) と復号化プログラム (rsa.c)
2. ファイルをコピーするプログラム (fcopy.c)
3. ファイルデータの表示プログラム (fdisp.c)
4. 文字の変換プログラム (fchg.c)
5. 拡張 Euclid 法のプログラム (euclid2.c)
6. シフト暗号の暗号化・復号化プログラム (shift.c)

35/ 36

C 言語のプログラミングについて

1. 下記の WEB に「C 言語入門プログラムソース」という資料を置いてあります。
<http://www.code.ice.uec.ac.jp/kuri/C3/indexprog.html>
2. 初めて C 言語を扱う者は、上記 WEB の資料を参考に、実際に動作するプログラムを作成することで、C 言語の初歩を学習して下さい。
3. また、参考書籍: 梶田賢 (むくだみのる) 著「はじめての C」を IED 計算機室後方の本棚に用意してあります。
この参考書は、本実験課題用にリクエストして購入設置したものです。

36/ 36