情報通信工学実験 $A \cdot B$

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 情報通信工学科
〒182-8585 東京都調布市調布ヶ丘1-5-1
www.code.ice.uec.ac.jp/kuri/C3/

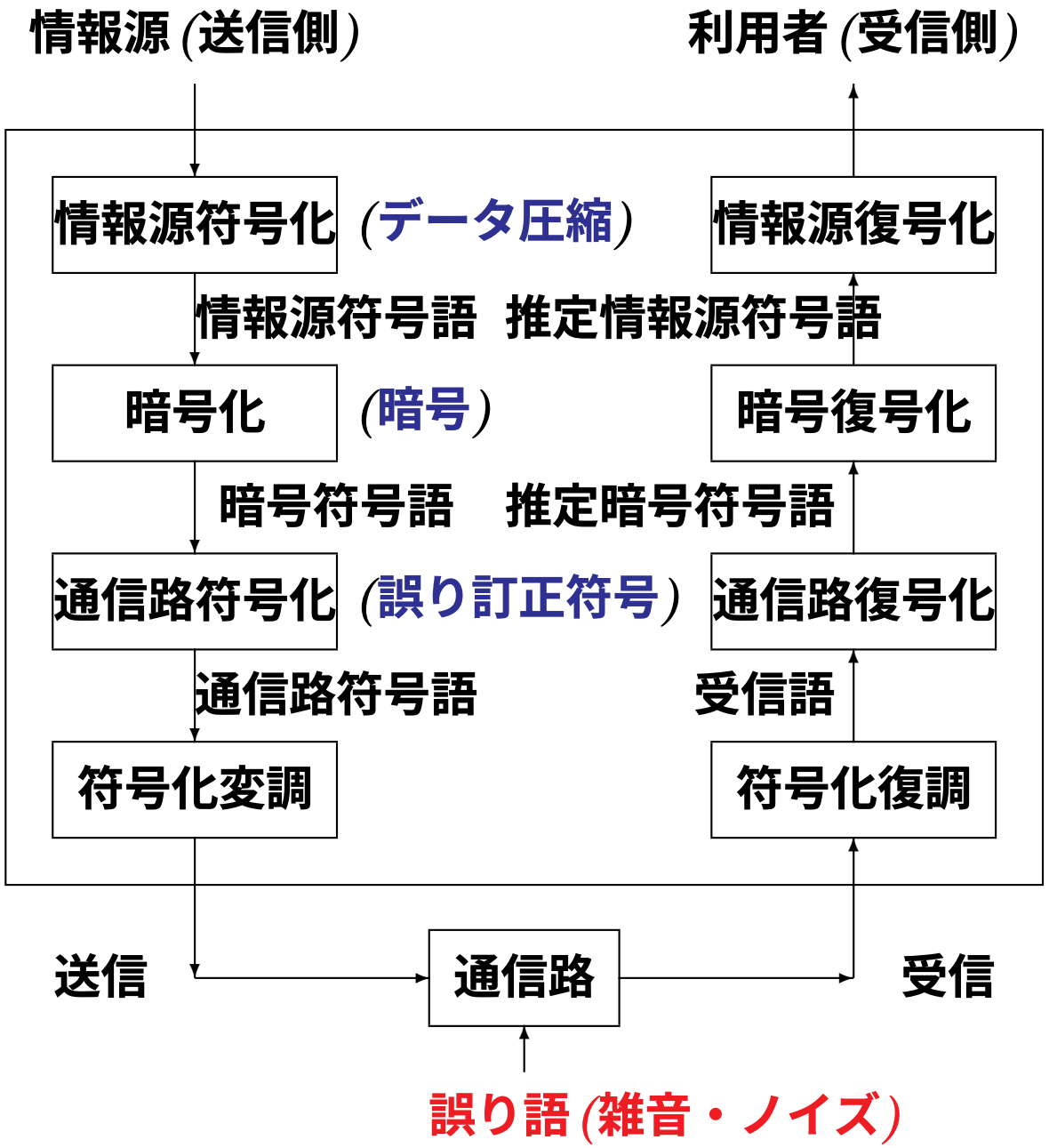
11× 3 : /doc/tex/uec/jikken/2009text/presenrsa2009(2009/6/11/14:27)

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

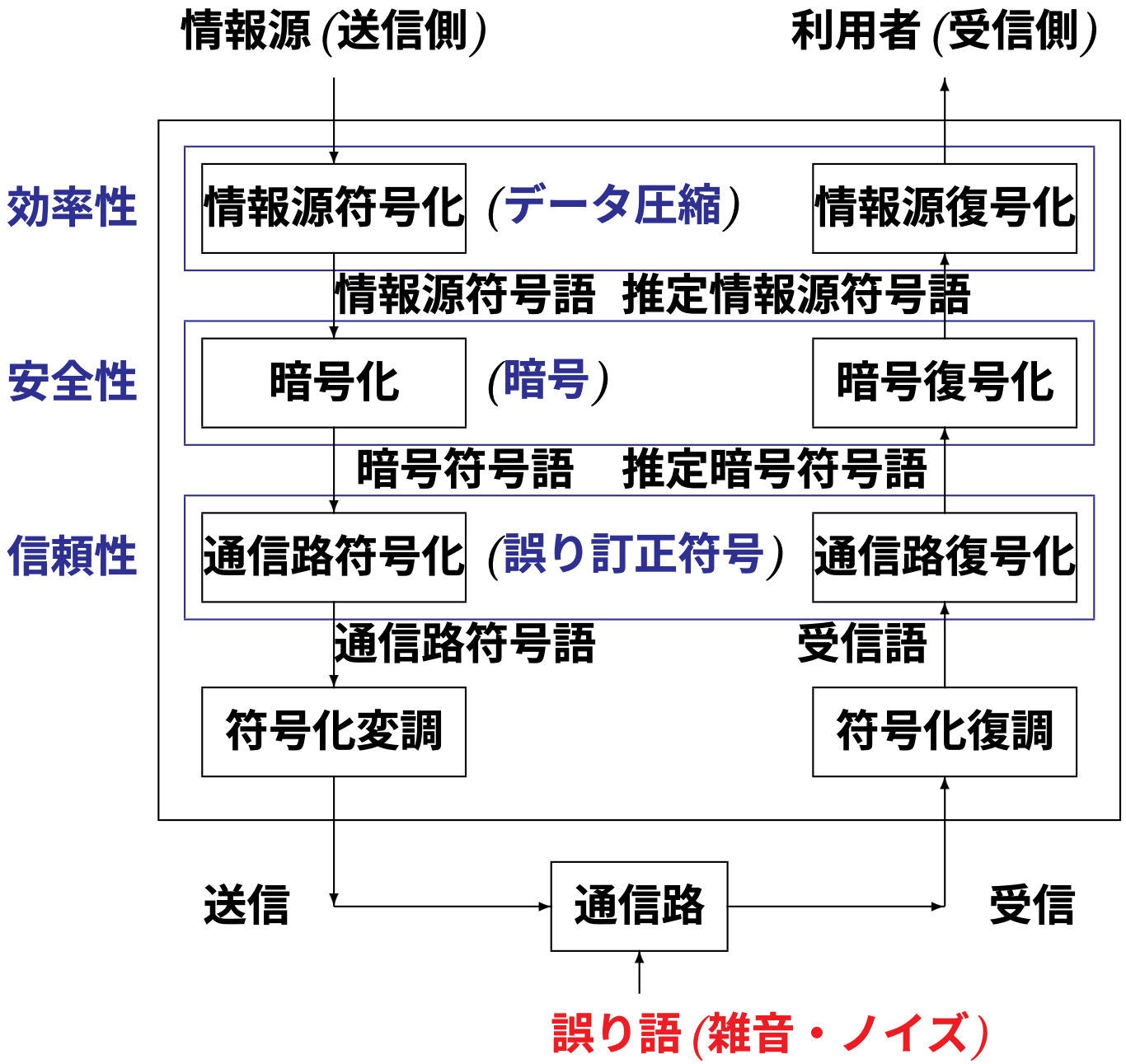
1. 「データ圧縮の理解と実装」
   — ハフマン符号の理解と実装 (プログラミング) —
2. 「暗号化の理解と実装」
   — RSA 暗号の理解と実装 (プログラミング) —
3. 「誤り訂正符号の理解と実装」
   — リード・ソロモン符号と最小距離復号の
   理解と実装 (プログラミング) —

キーワード：『符号化』

ディジタル通信システム



ディジタル通信システム



「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

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．
   具体的には、5 節の課題を解く。

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イ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．

1. はじめに

本テキストの目的：

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 Publick-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譲る。

2. 暗号化

2.1 暗号の具体例（シフト暗号）

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。

定義 1. *[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文字からなるアルファベット，“A,B,...,Z ,” により構成されているものとする。アルファベットの各文字を辞書式順序に並べる。

$$A\ B\ C\ D\ E\ F\ G\ H\ I\ J\ K\ L\ M\ N\ O\ P\ Q\ R\ S\ T\ U\ V\ W\ X\ Y\ Z$$

1. 暗号化 (鍵k): メッセージ $\to$ 暗号文

   各文字を順序に従って 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 $\to$ もとのメッセージ

   各文字を順序に従って 左へ k だけ循環シフト させる変換

暗号化： 鍵 $k = 5$ とする。

右へ 5 だけシフト

“ I ” $\rightarrow$ ... H I J K L M N O P ... $\rightarrow$ “ N ”

右へ 5 だけ循環(巡回)シフト

“ W ” $\rightarrow$ ... V W X Y Z A B C D ... $\rightarrow$ “ B ”

暗号システムの概念図

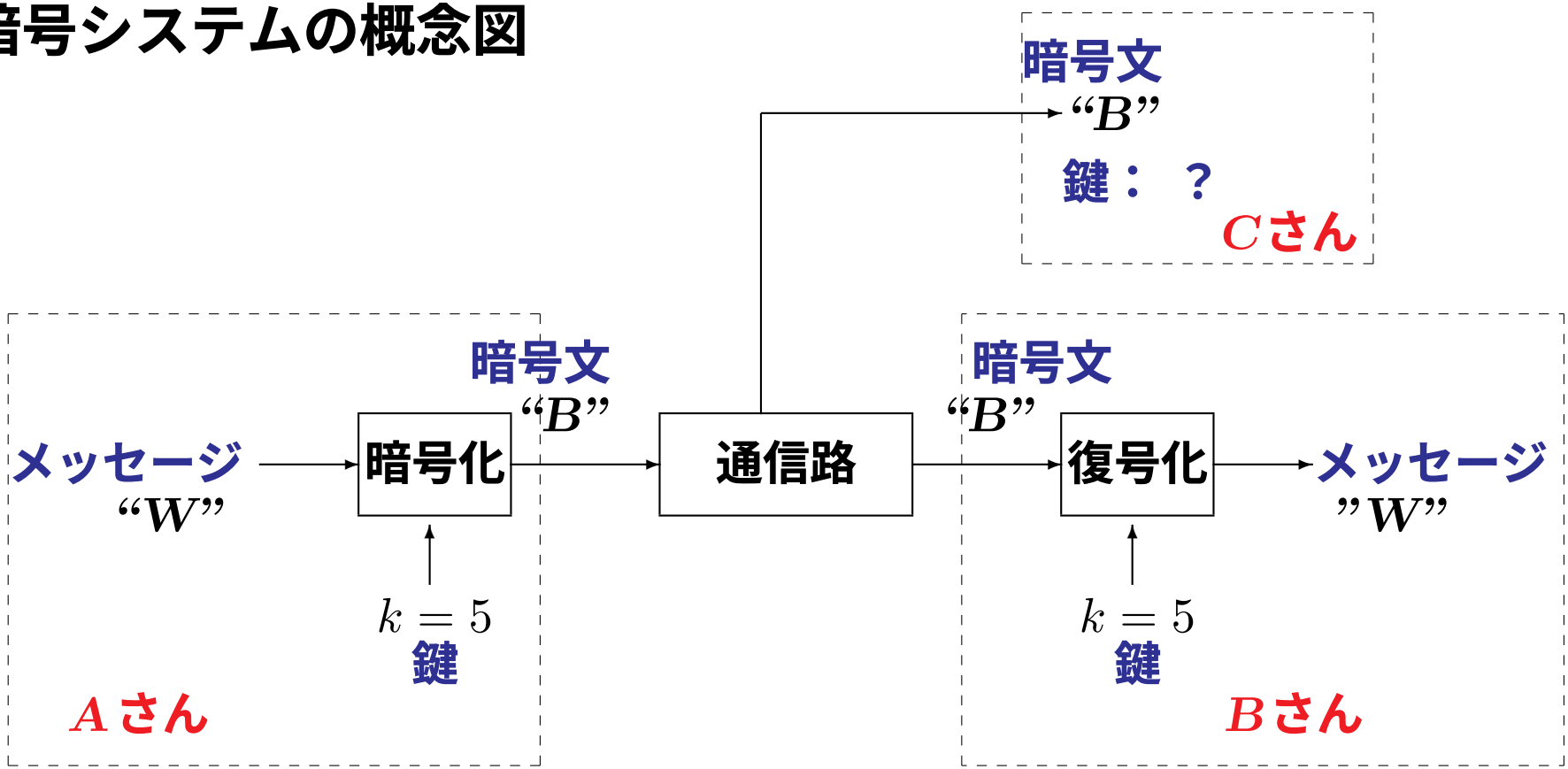


Figure 1: シフト暗号を用いたデータ伝送の様子

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。

例 2. 例えば、$k = 5$ として、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、

$$BJBNQQRJJYFYHMTKZXYFYNTS$$

となる。 これを Bさんに送信すればよい。

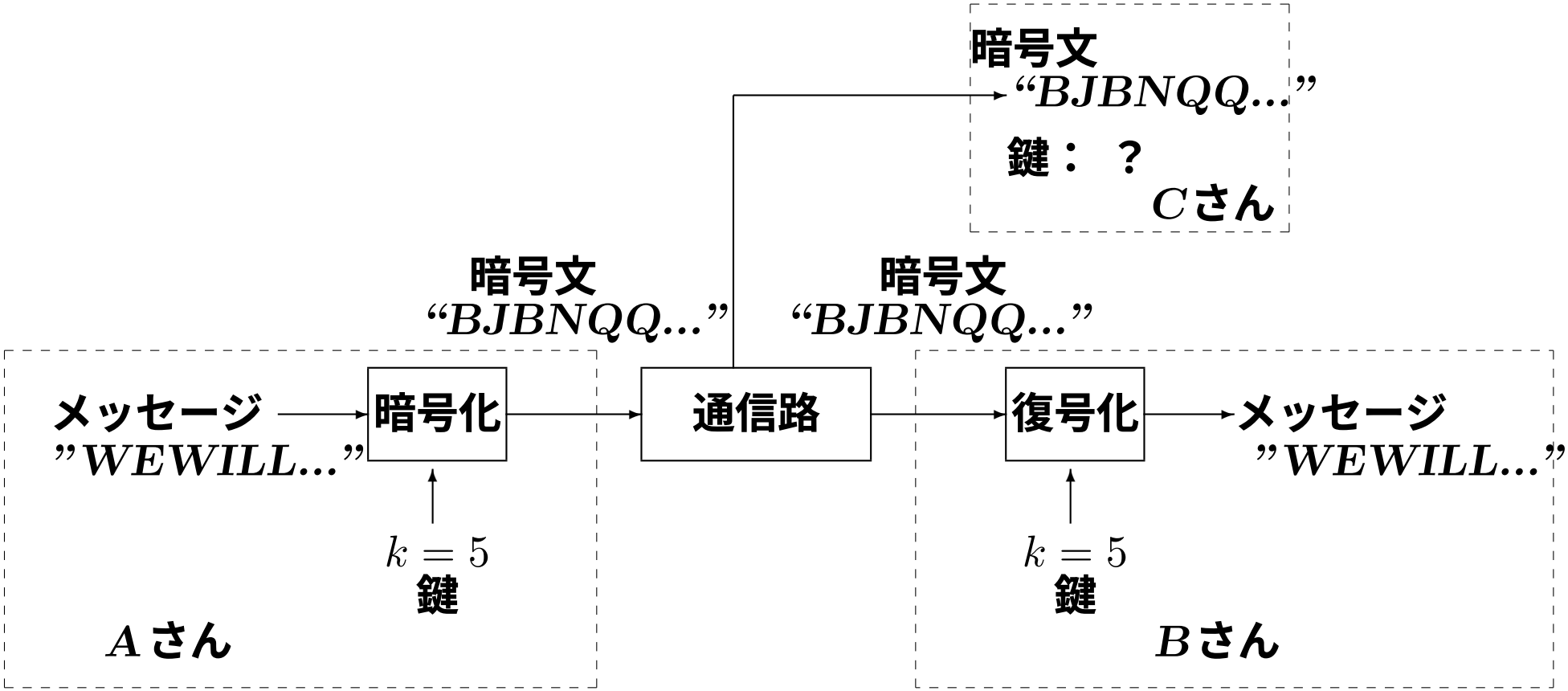


Figure 2: シフト暗号を用いたデータ伝送の様子

暗号システムの形式的記述

暗号の目的：

1. Aさん と Bさん の二人の間で, 盗聴可能な通信路 (公開通信路) を利用して, 情報を通信することができる こと。
2. ただし、第三者の Cさん には, その情報の内容が分からない方法で, 通信できなければならない。

1. **平文 (ひらぶん)** M ：伝達したいメッセージや情報
2. 暗号化用の**鍵** K_e
3. **暗号文** C ：平文 M を暗号化用の鍵 K_e で暗号化したもの
4. **公開通信路**：盗聴可能な通信路
5. 復号化用の**鍵** K_d

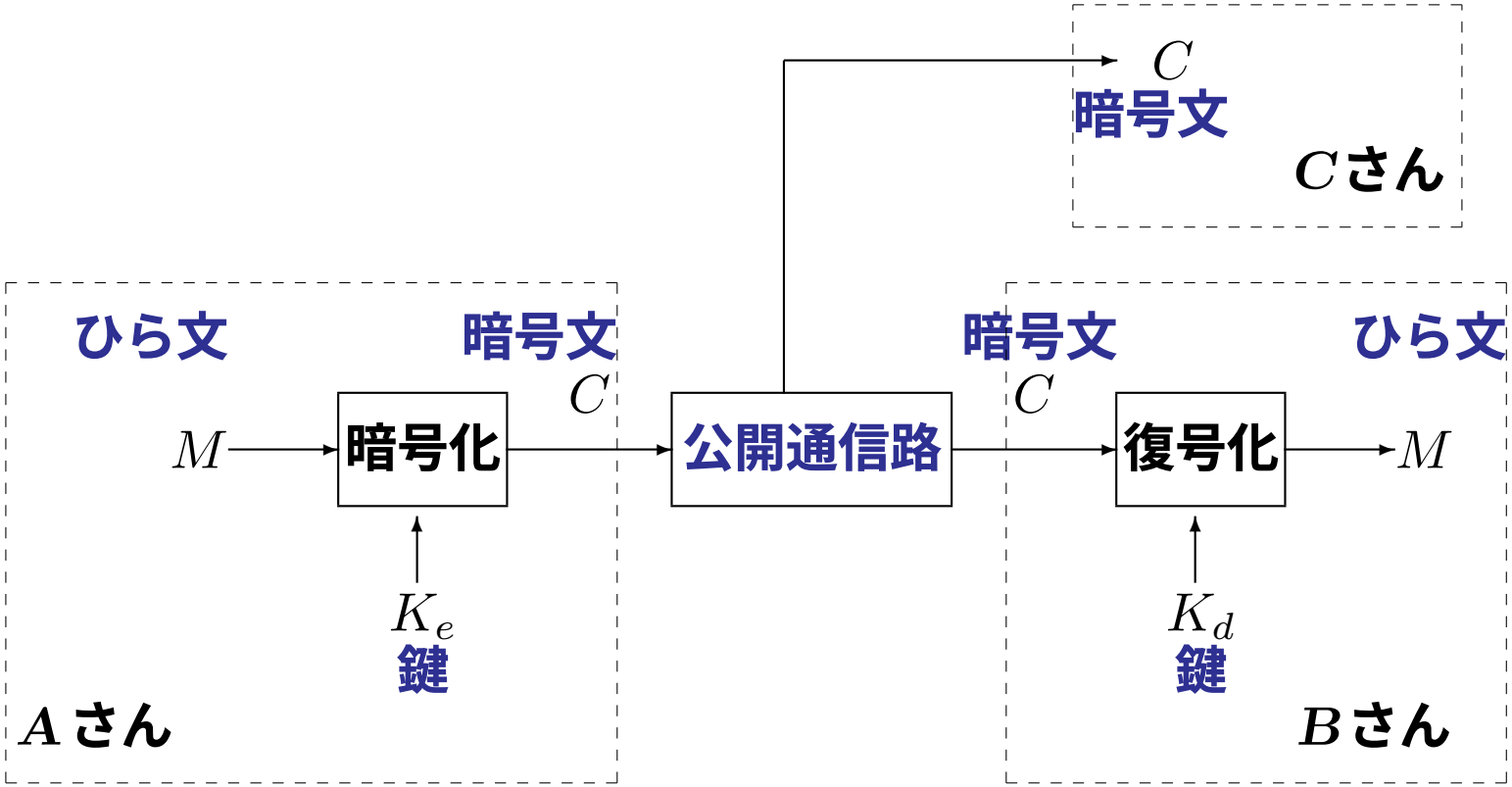


Figure 3: 形式的記述に対応する暗号システムの概略図

定義 3. 暗号システムは次の 6 項目を満たす 5 つの要素 $(\mathcal{M}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ から構成されるものと考える (定義しよう)。

1. $\mathcal{M}$：**平文**の全体からなる有限集合
2. $\mathcal{C}$：**暗号文**の全体からなる有限集合
3. $\mathcal{K}$：**暗号化鍵**の全体からなる有限集合
4. $\mathcal{E}$：各鍵 $K \in \mathcal{K}$ に対し定まる**暗号化の規則**の全体からなる集合
   鍵 K による規則 $e_K \in \mathcal{E}$ は $\mathcal{M}$ から $\mathcal{C}$ への写像と考える。
   $\boxed{M \in \mathcal{M} \text{ に対し、} e_K(M) = C \in \mathcal{C}}$ $\mathcal{M} \xrightarrow{e_K} \mathcal{C}$
5. $\mathcal{D}$：各鍵 $K \in \mathcal{K}$ に対し定まる**復号化の規則**の全体からなる集合
   鍵 K による規則 $d_K \in \mathcal{D}$ は $\mathcal{C}$ から $\mathcal{M}$ への写像と考える。
   $\boxed{C \in \mathcal{C} \text{ に対し、} d_K(C) = M' \in \mathcal{M}}$ $\mathcal{C} \xrightarrow{d_K} \mathcal{M}$
6. 任意の暗号化鍵 $K \in \mathcal{K}$ と平文 $M \in \mathcal{M}$ に対し、以下を満たす。
   $\boxed{d_K(e_K(M)) = M}$ $\mathcal{M} \xrightarrow{e_K} \mathcal{C} \xrightarrow{d_K} \mathcal{M}$

シフト暗号の形式的記述

1. **シフト処理 ⇒ 算術演算：アルファベットの文字を数字に対応させる.**

$$\{A, B, \ldots, Z\} \Leftrightarrow \mathbf{Z}_{26} := \{65, 66, \ldots, 90\}$$

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

2. **算術演算:**

足し算 $\oplus$ と引き算 $\ominus$ の定義：任意の $a, b \in \mathbf{Z}_{26}$ に対し、

$$a \oplus b = c \quad \text{such that} \quad a + b \equiv c \pmod{26} \text{ and } 65 \leq c \leq 90$$

$$a \ominus b = c \quad \text{such that} \quad a - b \equiv c \pmod{26} \text{ and } 65 \leq c \leq 90$$

常に $a \oplus b \in \mathbf{Z}_{26}$ と $a \ominus b \in \mathbf{Z}_{26}$ が成り立つ。

ASCHII

下位\上位	0	1	2	3	4	5	6	7
0	NUL	DLE	SP	0	@	P	‘	p
1	SOH	DC1	!	1	A	Q	a	q
2	STX	DC2	”	2	B	R	b	r
3	ETX	DC3	#	3	C	S	c	s
4	EOT	DC4	$	4	D	T	d	t
5	ENQ	NAC	%	5	E	U	e	u
6	ACK	SYN	&	6	F	V	f	v
7	BEL	ETB	’	7	G	W	g	w
8	BS	CAN	(	8	H	X	h	x
9	HT	EM	)	9	I	Y	i	y
A	LF/NL	SUB	*	:	J	Z	j	z
B	VT	ESC	+	;	K	[	k	{
C	FF	FS	,	<	L	\	l	|
D	CR	GS	-	=	M	]	m	}
E	SO	RS	.	>	N	^	n	~
F	SI	US	/	?	O	_	o	DEL

大文字“ A ”の 2進数表現、10進数表現

ASCHII の表より、

上位： $4 \Leftrightarrow 0100$

下位： $1 \Leftrightarrow 0001$

これより、

$\mathrm{A} \Leftrightarrow 01000001 \Leftrightarrow 65$

なぜなら、

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

1. $(a, b) = (70, 76)$ **の場合：** $70 \oplus 76 = 68$

$$70 + 76 = 146 \equiv 120 \equiv 94 \equiv 68 \pmod{26}$$

$$(65 \leq 68 \leq 90)$$

2. $(a, b) = (78, 89)$ **の場合：** $78 \oplus 89 = 89$

3. $(a, b) = (70, 76)$ **の場合：** $70 \ominus 76 = 72$

$$70 - 76 = -6 \equiv 20 \equiv 46 \equiv 72 \pmod{26}$$

$$(65 \leq 72 \leq 90)$$

4. $(a, b) = (89, 78)$ **の場合：** $89 \ominus 78 = 89$

以上より、シフト暗号を形式的に記述する: $(\mathcal{M}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$

1. $\mathcal{M} = \mathbf{Z}_{26} = \{65, 66, \ldots, 90\}$.
2. $\mathcal{C} = \mathbf{Z}_{26} = \{65, 66, \ldots, 90\}$.
3. $\mathcal{K} = \mathbf{Z}_{26} = \{65, 66, \ldots, 90\}$.
4. $\mathcal{E}$: $e_K(M) := M \oplus K$ **for** $K \in \mathcal{K}$, $M \in \mathcal{M}$.
5. $\mathcal{D}$: $d_K(C) := C \ominus K$ **for** $K \in \mathcal{K}$, $C \in \mathcal{C}$.
6. $d_K(e_K(M)) = d_K(M \oplus K) = (M \oplus K) \ominus K = M \oplus (K \ominus K) = M$

シフト数 k **に対応する暗号化鍵** $K \in \mathbf{Z}_{26}$ **は、**

$k \equiv K \pmod{26}$ **を満たすもの**

$k = 5$ **の場合、** $5 \equiv 83 \pmod{26}$ **より、** $K = 83 \in \mathbf{Z}_{26}$

例 4. (続き) メッセージ

$$\boxed{WEWILLMEETATCHOFUSTATION}$$

を数字に対応させて変換すると

$$\boxed{87\ 69\ 87\ 73\ 76\ 76\ 77\ 69\ 69\ 84\ 65\ 84\ 67\ 72\ 79\ 70\ 85\ 83\ 84\ 65\ 84\ 73\ 79\ 78}$$

となる。シフト数 $k = 5$ の場合、鍵は $K = 83$ となり、その暗号文は、

$$\boxed{66\ 74\ 66\ 78\ 81\ 81\ 82\ 74\ 74\ 89\ 70\ 89\ 72\ 77\ 84\ 75\ 90\ 88\ 89\ 70\ 89\ 78\ 84\ 83}$$

となる。

ここで、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。

$$\boxed{876987737676776969846584677279708583846584737978}$$

$$\boxed{667466788181827474897089727784759088897089788483}$$

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

と

公開鍵暗号システム

の二つに分類する。

2.3.1 秘密鍵暗号システム

1. 暗号化鍵 K から 復号化の規則 d_K を導出する困難さが
   暗号化の規則 e_K を導出するのと同程度
2. 暗号化鍵 K を第三者には秘密にする

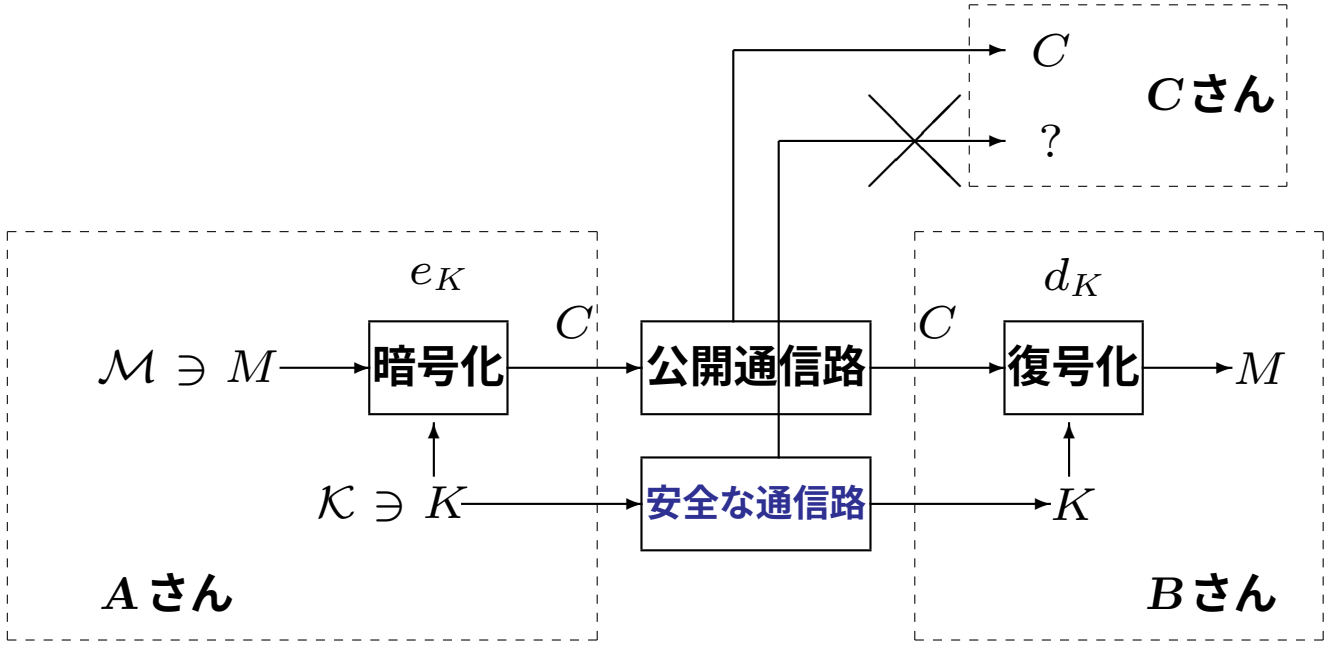


Figure 4: 秘密鍵暗号システム

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
⇒ 安全な通信路を利用して送信する必要がある

2.3.2 公開鍵暗号システム

1. 暗号化鍵 K から 復号化の規則 d_K を導出する困難さが 暗号化の規則 e_K を導出するのと比較して**計算量的に実行不可能**である
2. 暗号化鍵 K を第三者にも**公開する**ことができる
3. ゆえに、安全な通信路を利用して通信する必要がない
4. 公開された暗号化鍵 K とは異なる**秘密鍵** K_d により暗号文を復号化することができる
5. ***RSA* 暗号**は、この**公開鍵暗号システム**の一種である

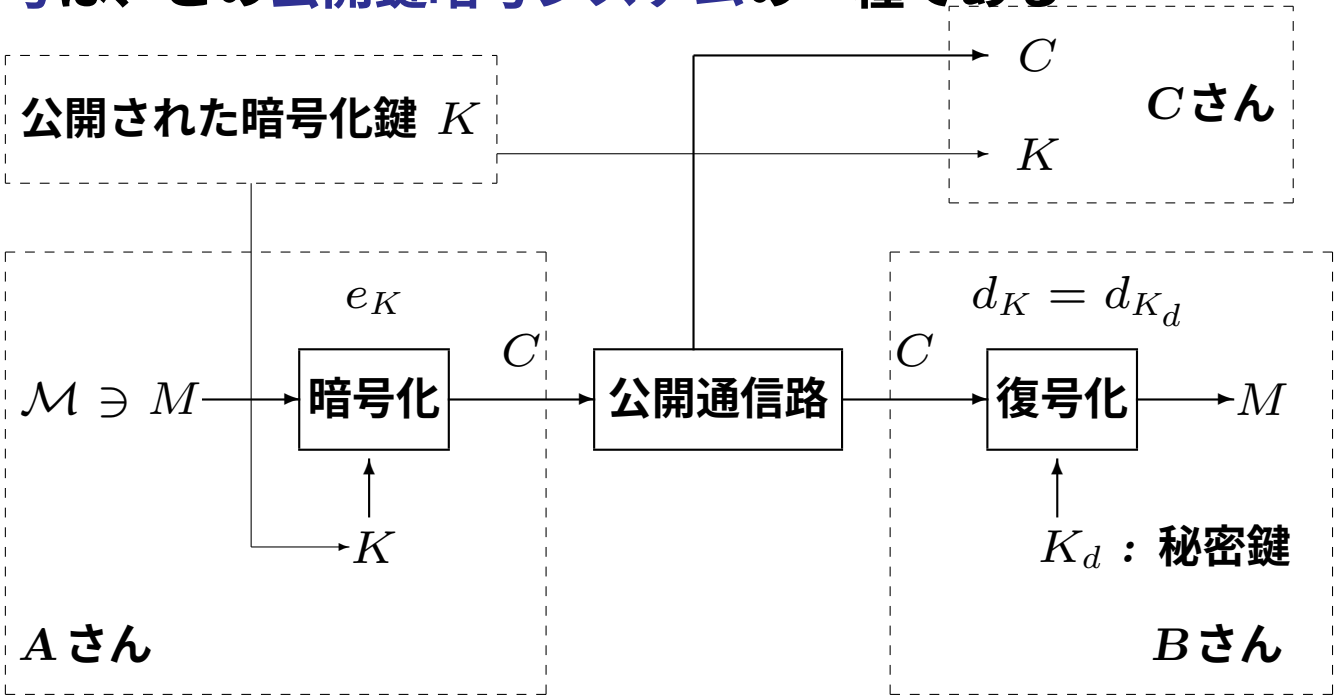
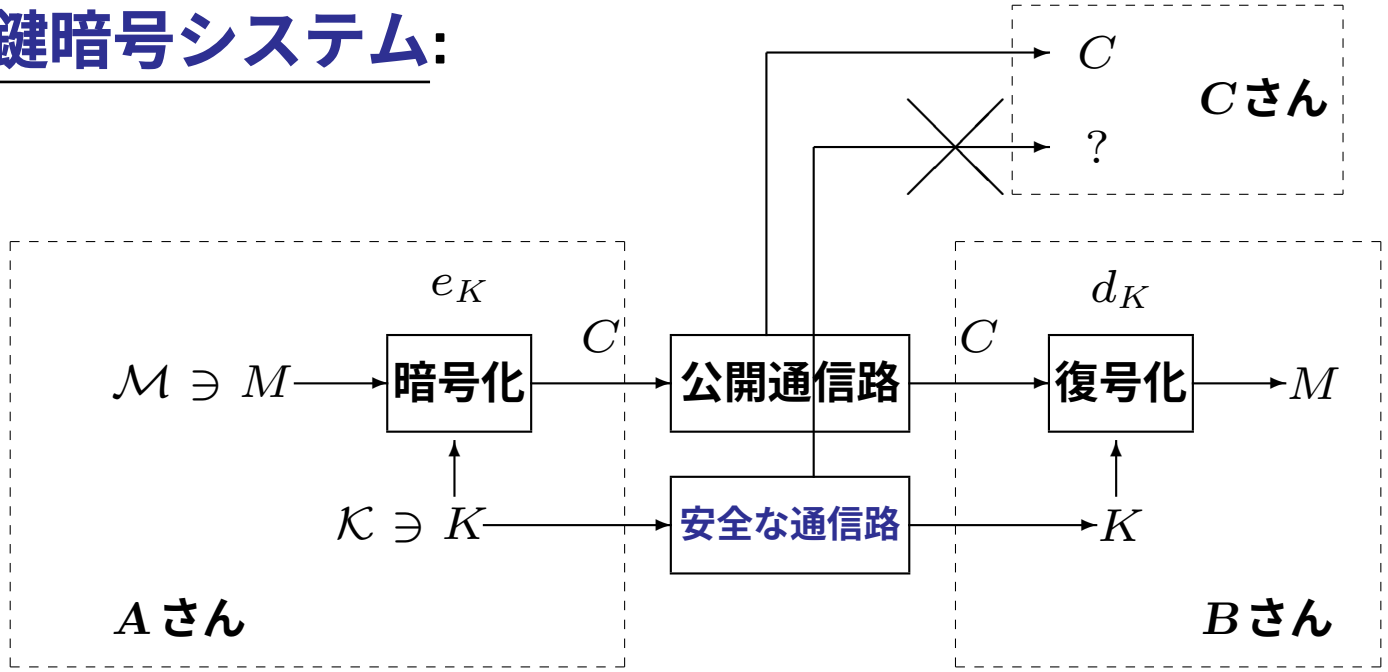
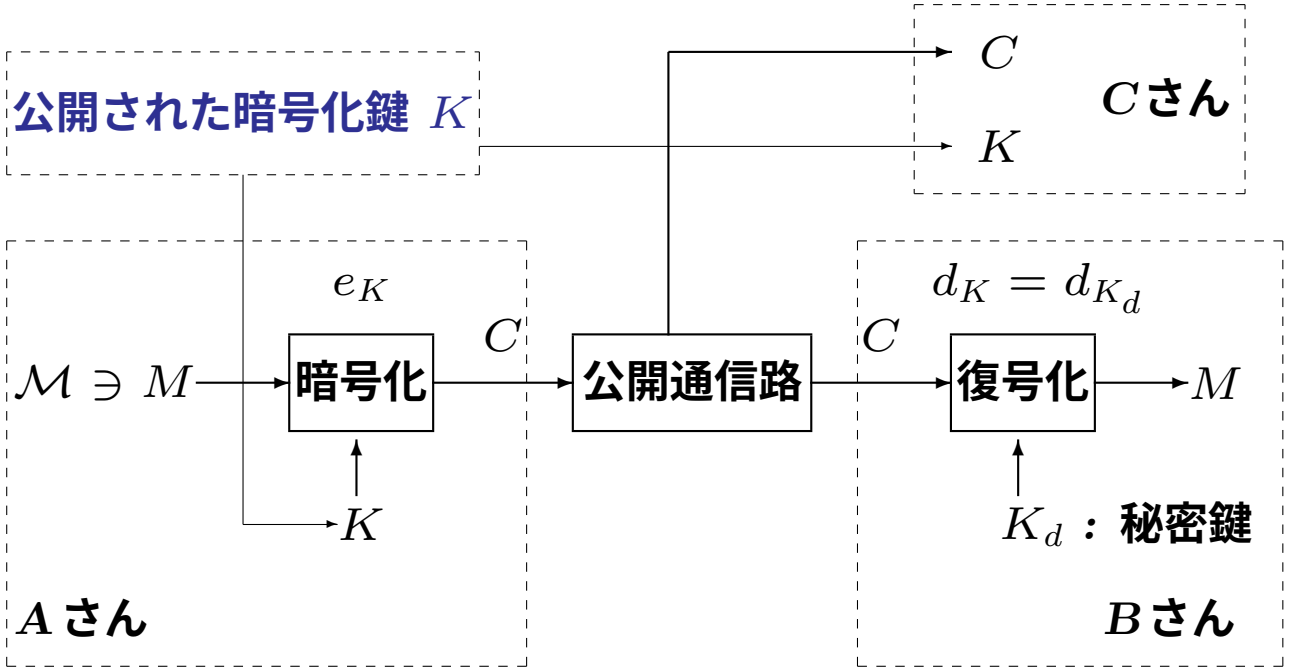


Figure 5: 公開鍵暗号システム

秘密鍵暗号システム:



公開鍵暗号システム:



整理：

1. **秘密鍵暗号システム**：「暗号化鍵 K_e」 $=$ 「復号化鍵 K_d」

   ⇒ 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**

2. **公開鍵暗号システム**：「暗号化鍵 K_e」 $\neq$ 「復号化鍵 K_d」

   ⇒ 暗号化鍵を**共有する必要はない**

公開鍵暗号システムの手続き

i. 暗号文を受け取る側の B さんは、B さん専用の **暗号化鍵** と **復号化鍵** を作成し、暗号化鍵は **一般に公開し**、復号化鍵は **秘密** にしておく。

ii. A さんは、B さんに伝えたい**平文**を公開されている B さんの**暗号化鍵**を用いて**暗号文**を作成し、公開通信路を利用して B さんに送信する。

iii. B さんさんは、自分しか知らない **復号化鍵** を用いて A さんからの**暗号文** を復号し、**平文** を得る

iv. 第三者の C さんは、公開されている **暗号化鍵** と公開通信路を利用して **暗号文** を入手できるが、その二つだけでは暗号文を元の平文に**容易には復号できない**。

4. *RSA*暗号

はじめに、いくつかの整数を選択したり、計算したりする。

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。

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

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

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)*

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

1. **Select** (p, q)
2. $n := p \times q$
3. $L := \mathrm{lcm}(p-1, q-1)$
4. e ***such that*** $\gcd(e, L) = 1$ ***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. $L = \mathrm{lcm}(17-1, 19-1) = \mathrm{lcm}(16, 18) = 2 \times 2 \times 2 \times 2 \times 3 \times 3 = 144$
4. $e = 5$ ***such that*** $\gcd(e, 144) = 1$ ***and*** $1 < e < 144$
   $e \in \{5, 7, 11, 13, \ldots, 143\}$
5. $d_e = 29$ ***such that*** $5 \times d_e \equiv 1 \pmod{144}$

このとき，*RSA*暗号の形式的な記述 $(\mathcal{M}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ **は以下のようになる:**

1. $\mathcal{M} = \mathbf{Z}_n$
2. $\mathcal{C} = \mathbf{Z}_n$
3. $\mathcal{K} = \{(e, n) \mid \gcd(e, L) = 1 \text{ and } 1 < e < L\}$
4. $\mathcal{E}$ **:** $e_K(M) := M^e \pmod n$ **for** $K = (e, n) \in \mathcal{K},\ M \in \mathcal{M}$
5. $\mathcal{D}$ **:** $d_K(C) := C^{d_e} \pmod n$ **for** $K = (d_e, n) \in \mathcal{K},\ C \in \mathcal{C}$
6. $d_K(C) = d_K(e_K(M)) = M$ **が成り立つ:**

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

i. **任意の互いに異なる素数** p, q **に対し、** $n := p \times q$ **とする。**

ii. $L := \mathrm{lcm}(p - 1, q - 1)$.

iii, d_e**:** $e \times d_e \equiv 1 \pmod L$ **を満たす整数。**

iv. **公開:** **暗号化鍵** (e, n)

v. **秘密:** $p,\ q,\ d_e$**;** d_e**: 秘密鍵;** (d_e, n)**: 復号化鍵.**

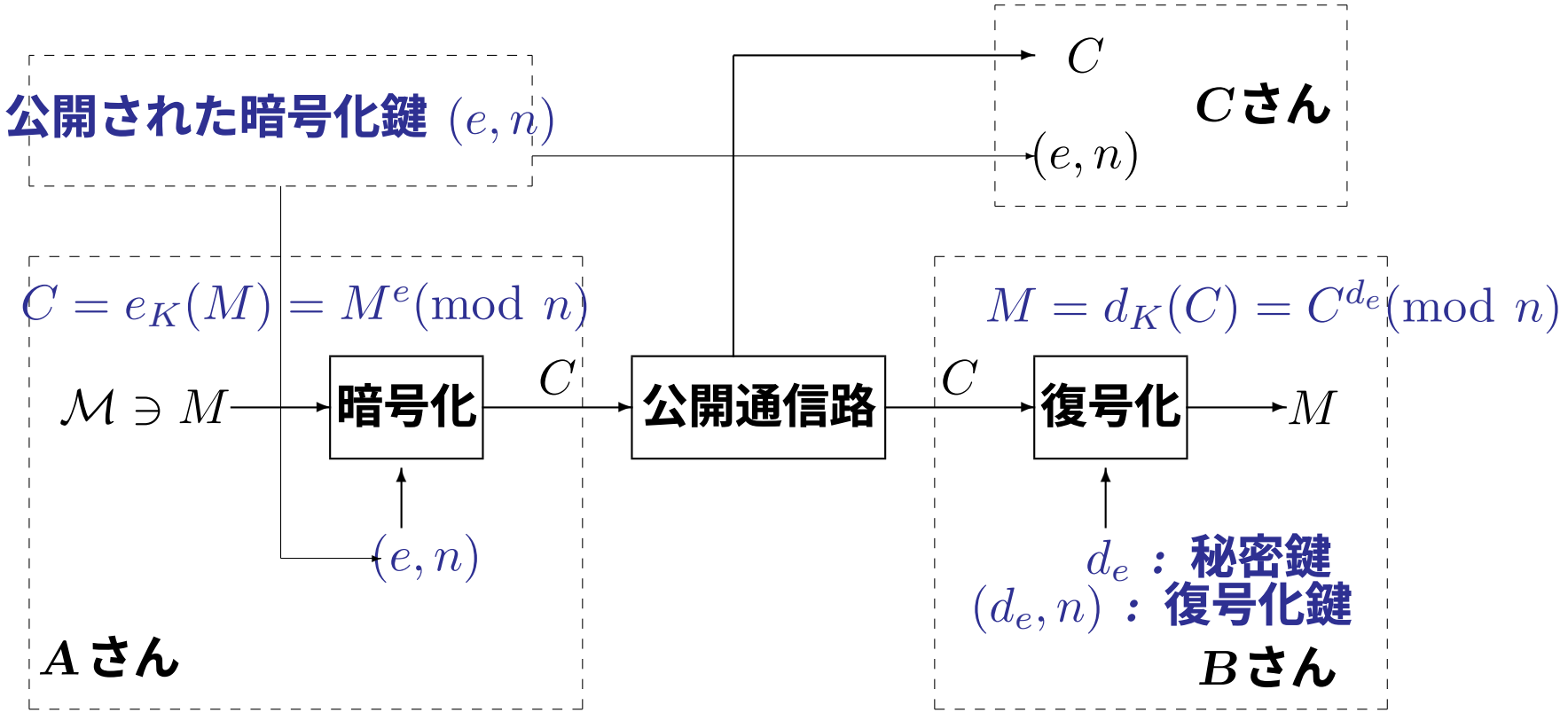


***Figure 6: RSA*暗号を用いた公開鍵暗号システム**

***RSA*暗号の暗号化規則 e_K と 復号化規則 d_K の合成写像は、$d_K(C) = d_K(e_K(M)) = M$ となる。つまり、**

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

***RSA*暗号において、この関係の成立が保証されていることが大切**

例 5. *26*文字のアルファベットからなる平文を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
   $\Rightarrow \quad n = 323$
2. $(p-1)$ と $(q-1)$ の最小公倍数 $\Rightarrow \quad L = 144$
3. $1 < e < 144 = L$ を満たし、L と互いに素な整数 $e \quad \Rightarrow \quad e = 5$
4. 秘密鍵 d_e を計算する $\Rightarrow \quad d_e = 29$

公開鍵（暗号化鍵）： $K = (e, n) = (5, 323)$

秘密鍵： $d_e = 29$

復号化鍵： $(d_e, n) = (29, 323)$

文字 “ C ” ⇔ 数字 “67”： これを 暗号化/復号化 してみよう。

ひら文 $M = 67$,

暗号化鍵 $K = (e, n) = (5, 323)$, **復号化鍵** $(d_e, n) = (29, 323)$.

暗号化：$C = M^e = (67)^5 \equiv 288 \pmod{323}$ ⇒ $e_K(67) = 288$

復号化：$M' = C^{d_e} = (288)^{29} \equiv 67 \pmod{323}$ ⇒ $d_K(288) = 67$

電卓でもできる、

1) $(67)^2 = 67 \times 67 = 4489 \equiv 290 \pmod{323}$,

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

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:
```

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

$\boldsymbol{WEWILLMEETATCHOFUSTATION}$

を暗号化：まず, 各文字を数字に変換:

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

暗号文:

83 103 83 99 247 247 229 103 103 50 12 50 288 21 129 185 187 87 50 12 50 99 129 10

2. **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)を復号する.**

注意 : 暗号文に区切り記号の空白がないと...

8310383992472472291031035012502882112918518787501250991291O

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 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_e, n) と 暗号化されたファイル.**
出力	**: 元のひら文のファイル.**

このとき、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。

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 $L = \mathbf{lcm}(p-1, q-1)$ を求めるプログラムを作成し、実装せよ。
4. 整数 L に対し、$\mathbf{gcd}(e, L) = 1$ 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、$ed \equiv 1 \ (\mathbf{mod}\ L)$ 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。

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)*

References

[1] *Douglas R. Stinson,* 暗号理論の基礎，櫻井幸一監訳、共立出版，*1996*.

[2] 池野信一, 小山謙二, 現代暗号理論（電子情報通信学会)、コロナ社，*1986*.

[3] 松坂和夫、代数系入門（第*28*刷発行)、岩波書店、*2003*.

[4] 石田信、代数系入門（第*12*刷発行)、実教出版、*1990*.

[5] ***R.L.Rivest, A. Shamir and L. Adleman, "A Method for Obtaining Digital Signatures and Publick-Key Cryptosystems,"*** *Communications of the ACM,* ***21(1978), pp.120–126, 1978.***

[6] 椋田 *(*むくだ*)* 實, はじめての *C (*改訂第三版*)*, 技術評論社, *1995(*平成 *7*年*)*.

[7] 平林雅英，*ANSI C*言語辞典 *(*初版 第*10*刷発行*)*, 技術評論社, *2000(*平成*12*年*)*.