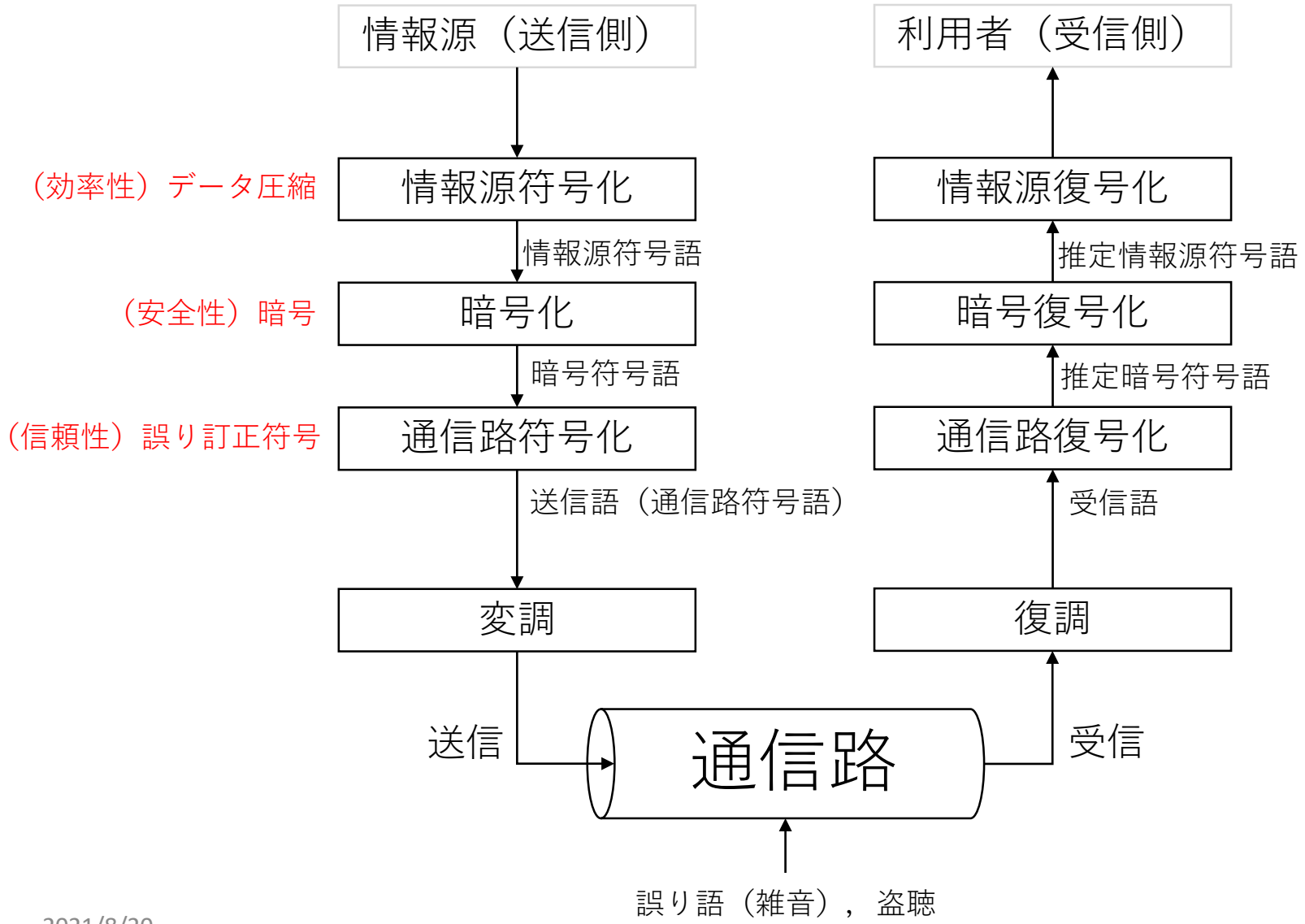
電気通信大学情報理工学域II類
情報通信工学プログラム/電子情報学プログラム

情報通信工学実験B/電子情報学実験B

実験項目　「情報通信（情報セキュリティ）」

「暗号化の理解とプログラミング」
－RSA暗号の理解とプログラミング－

ディジタル通信システム



「暗号化の理解とプログラミング」－RSA暗号の理解とプログラミング－

テキストの構成

1. 課題の目的
2. 提出レポートの要件（内容）（テキストの2節を確認すること（必須））
3. はじめに
4. 暗号化
    1. 暗号の具体例（シフト暗号）
    2. 暗号化システムの形式的記述
    3. 二つの暗号システム　⇒　公開鍵暗号と秘密鍵暗号（共通鍵暗号）
5. 数学的準備（整数の諸性質）
6. RSA暗号　←（公開鍵暗号）
7. 課題（テキストの7節を確認すること（必須））
8. プログラミング

1節　課題の目的

1. RSA暗号の暗号化と復号化の方法について理解する
2. RSA暗号の暗号化と復号化のプログラムを作成する（具体的には、7節に示す課題を行う）

2節　提出レポートの要件(内容)（詳細はテキストの2節を確認すること（必須））

1. 下記の内容を簡潔にまとめ、レポートせよ。
   a. RSA暗号の構成法（公開鍵と秘密鍵の作成手続き）とその利用法について説明せよ。
   b. 公開鍵暗号を利用した認証方式について説明せよ。
   c. 現時点において、RSA暗号の鍵の長さ（ビット長）は、どの程度が妥当であると議論されているかを調べ、レポートに記せ。
2. 7節の課題3の計測した実行処理時間の表とグラフを記述する。
3. 7節の課題4～7の問題の解答を記述する。
4. プログラミングで工夫した点
5. 考察
6. 感想とコメント
7. 参考文献
8. 各課題のプログラムのソースファイルと実行例を印刷したものをレポートに添付する。
9. レポート（PDFファイル）とは別に、各課題のプログラムのソースファイル（拡張子が「.c」のもの）を提出する。

３節　はじめに

1. テキストの目的は、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と、そのプログラム作成と実装のための諸注意などを説明することにあります。そのため、一般的な暗号については、講義や専門書を読んで下さい。

2. RSA暗号のRSAは、RSA暗号を発表した下記の論文著者名の頭文字になります。

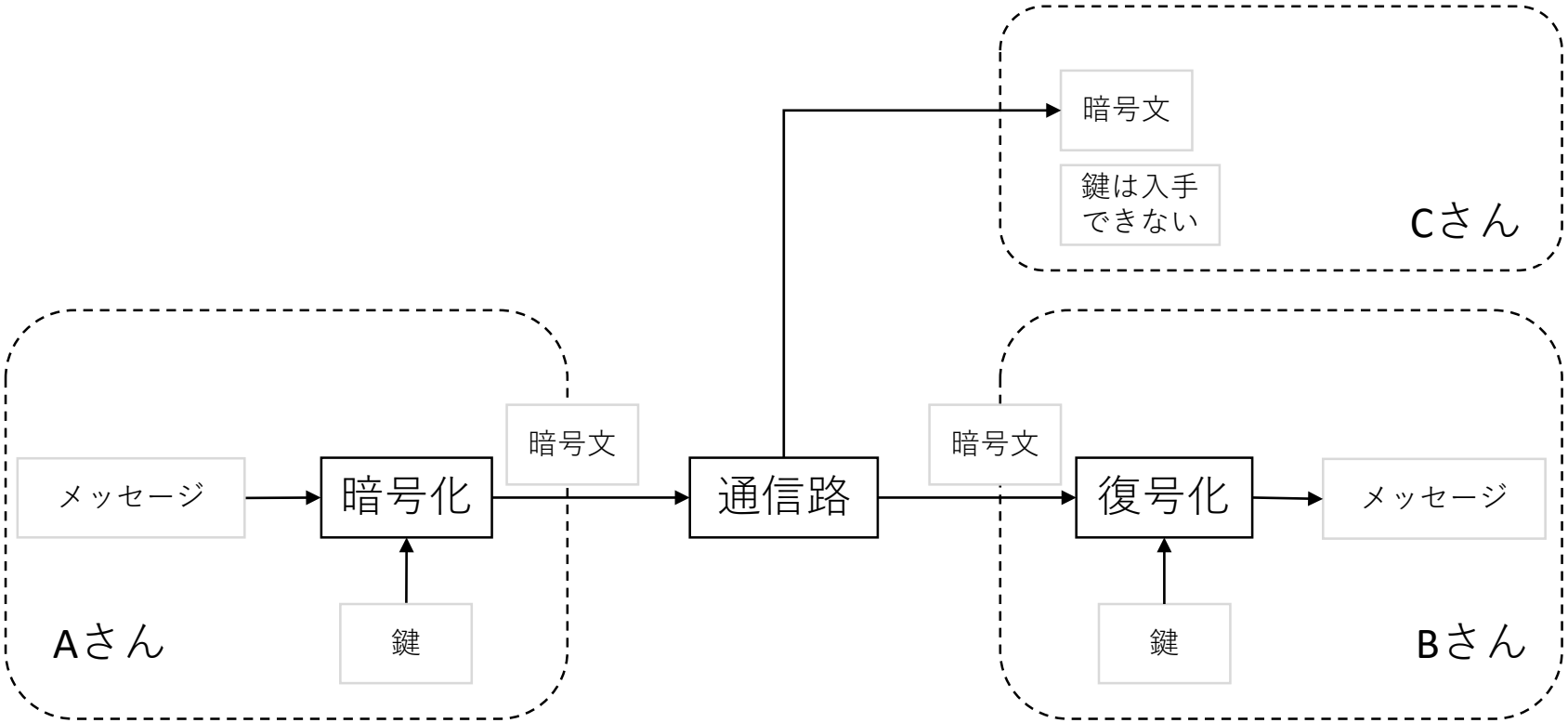
   R. L. Rivest, A. Sharmir, and L. Adleman,

   “A method for obtaining digital signatures and public-key cryptosystem,”

   Communications of th ACM, 21(1978), pp.120-126, 1978

4節　暗号化

1. 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.



上記の場合、AさんからBさんへ暗号文を送信する前に、AさんとBさんの間で鍵情報を共有しておく必要がある. しかも、鍵情報は、第三者のCさんには知られないようにする必要がある.

４.１節　暗号の具体例（シフト暗号）パラメータ：文字数 $n = 26$,　鍵 k

1. メッセージ集合と暗号文集合

   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の大文字 $A, B, C, \ldots, Z$ により構成されているものとする。つまり、

   1. メッセージ集合 $:= \{A, B, C, \ldots, Z\}$
   2. 暗号文集合 $:= \{A, B, C, \ldots, Z\}$

2. 暗号化と復号の方法（鍵の値 k は整数）

   1. 暗号化：辞書順に従って、右に k だけ（循環）シフトさせる変換
   2. 復号化：辞書順に従って、左に k だけ（循環）シフトさせる変換

3. 「（循環）シフト」の例（鍵 $k = 5$ とする）

   1. （シフト）メッセージ「H」を暗号化する場合：「H」→「M」

…	H	→	I	→	J	→	K	→	L	→	M	…
		1		2		3		4		5		

   2. （循環シフト）メッセージ「W」を暗号化する場合：「W」→「B」

…	W	→	X	→	Y	→	Z	→	A	→	B	…
		1		2		3		4		5		

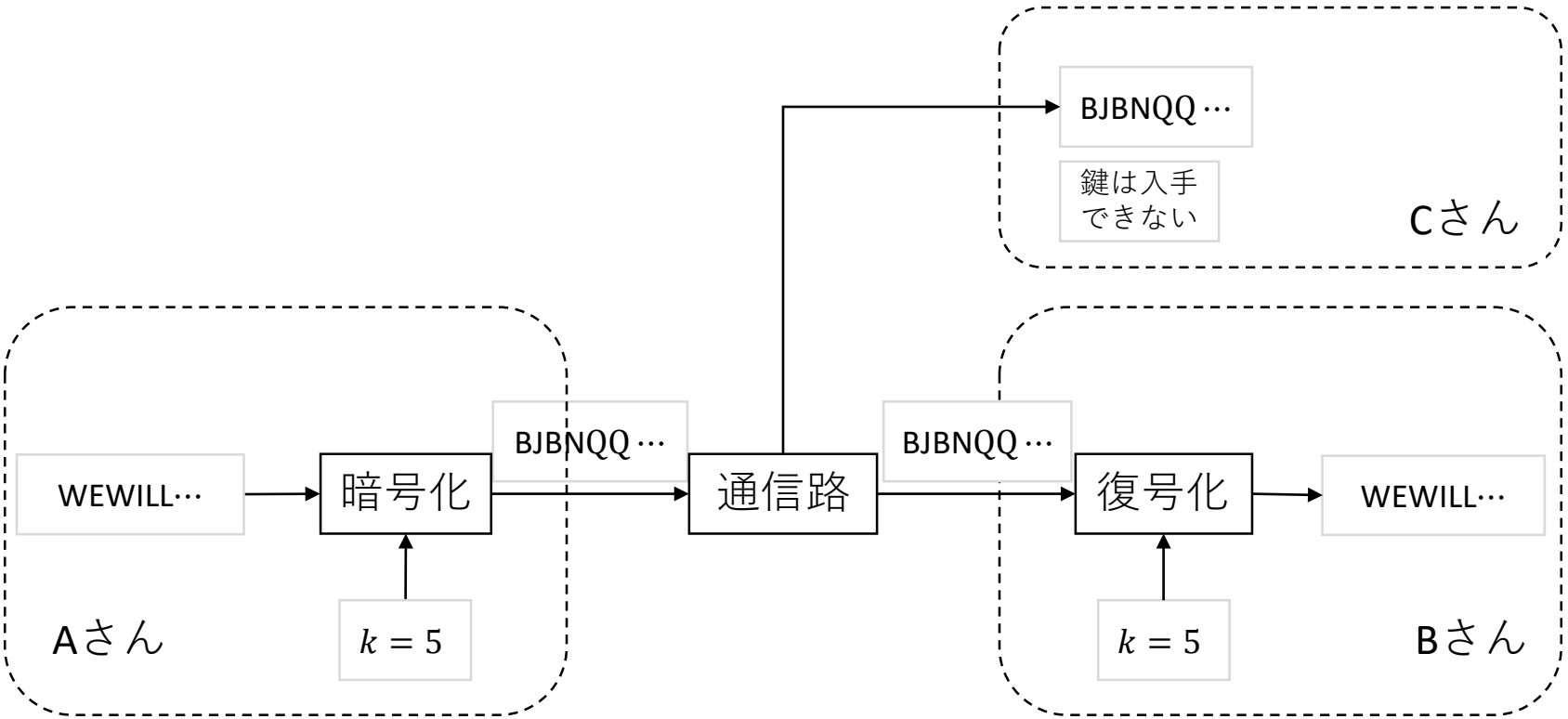
例えば、鍵$k = 5$としてシフト暗号を用いて、AさんからBさんへメッセージ

「WEWILLMEETATCHOFUSTATION」（単語間にスペースがないのはメッセージ集合に空白がないから）

を暗号化すると、その暗号文は、

「BJBNQQRJJYFYHMTKZXYFYNTS」

となる．Aさんは、この暗号文をBさんへ送信する．



算術演算を利用しよう！

「文字」から「整数」へ

すなわち、

「シフト処理」から「算術演算処理」

を考える．そこで、

「ASCII」（文字コード）

を復習しよう。

例えば、大文字「A」の10進数表現

ASCIIの表より、

			上位
	16進		4
		2進	0100
下位	1	0001	A

したがって、

文字	16進数	2進数	10進数
A	41	01000001	65

$$65 = 4 * 2^4 + 1 * 2^0$$
$$= 1 * 2^6 + 1 * 2^0$$

「文字」から「整数」への対応関係（ASCIIと合同関係）

1. 文字の集合：$\{A, B, C, \ldots, Z\}$
2. 整数の集合：$\mathbb{Z}_{26} = \{65, 66, 67, \ldots, 90\}$　（ASCIIによる10進数表現）
3. 余りの集合：$\mathbb{Z}_{26} = \{0, 1, 2, \ldots, 25\}$　（26を法とする合同関係を考える）

文字	A	B	C	D	E	F	G	H	I	J	K	L	M
整数	65	66	67	68	69	70	71	72	73	74	75	76	77
余り	13	14	15	16	17	18	19	20	21	22	23	24	25

文字	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
整数	78	79	80	81	82	83	84	85	86	87	88	89	90
余り	0	1	2	3	4	5	6	7	8	9	10	11	12

「（循環）シフト処理」から「算術演算処理」への例（鍵 $k = 5$ とする）

1. （シフト）メッセージ「H」を暗号化する場合：「H」→「M」

…	H	→	I	→	J	→	K	→	L	→	M	…
	72		73		74		75		76		77	

$72 + 5 = 77$

2. （循環シフト）メッセージ「W」を暗号化する場合：「W」→「B」

…	W	→	X	→	Y	→	Z	→	A	→	B	…
	87		88		89		90		91		92	
									65		66	

$87 + 5 = 92 \equiv 66 \pmod{26}$

$92 = 3 * 26 + 14$
$66 = 2 * 26 + 14$

算術演算処理によるシフト暗号の表現（鍵 $k = 5$ の場合）

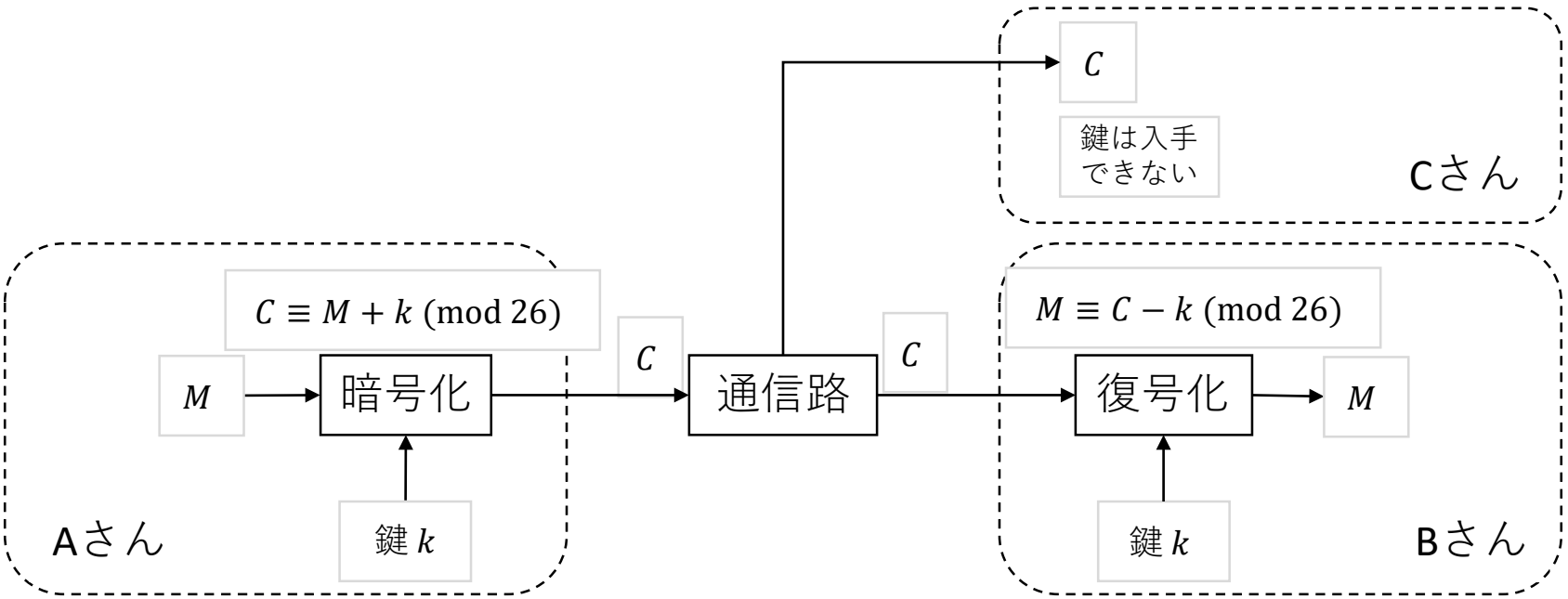
メッセージ：「WEWILLMEETATCHOFUSTATION」

をASCIIに従って整数に変換すると、

メッセージ：「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、メッセージMに対する暗号文Cは、$C \equiv M + k \pmod{26}$より、以下のようになる．

暗号文：「66 74 66 78 81 81 82 74 74 89 70 89 72 77 84 75 90 88 89 70 89 78 84 83」



４.３節　二つの暗号システム

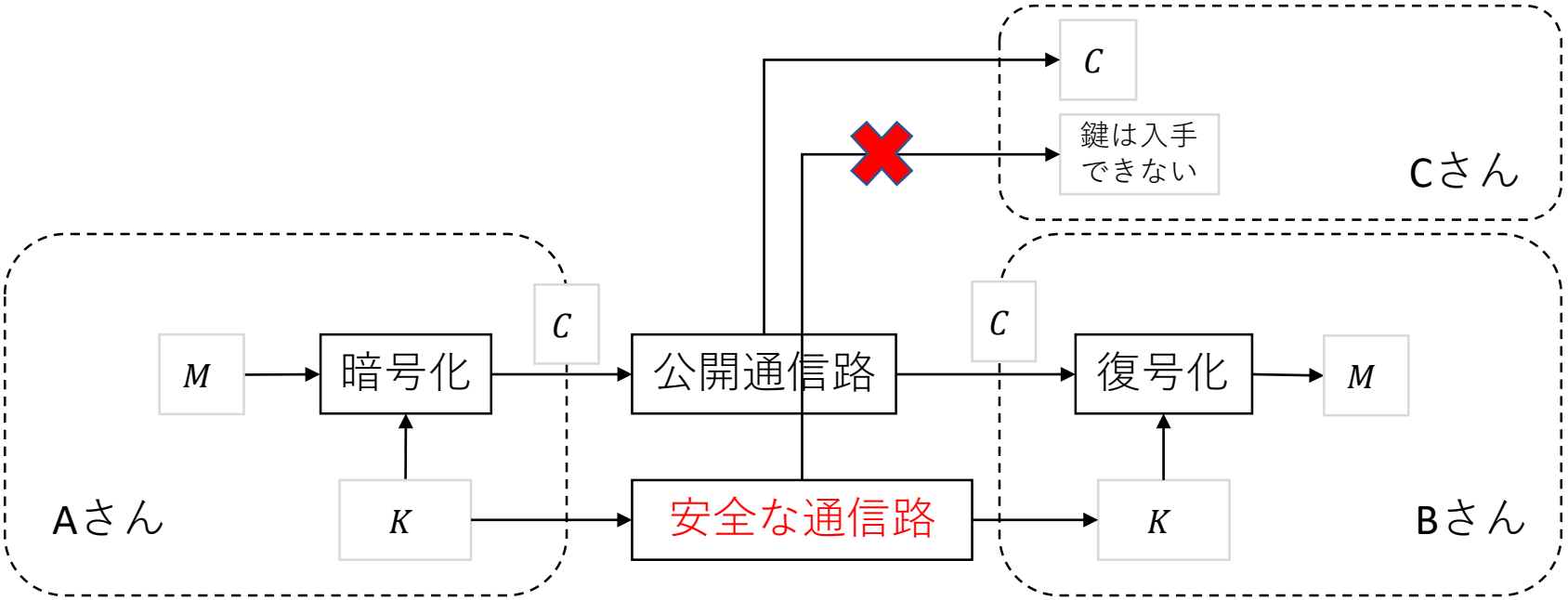
暗号システムを以下の2種類に分類する.

1. 「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）

2. 「公開鍵暗号システム」

4.3.1節　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
2. 鍵の作成者は、AさんまたはBさんのどちらでも可能



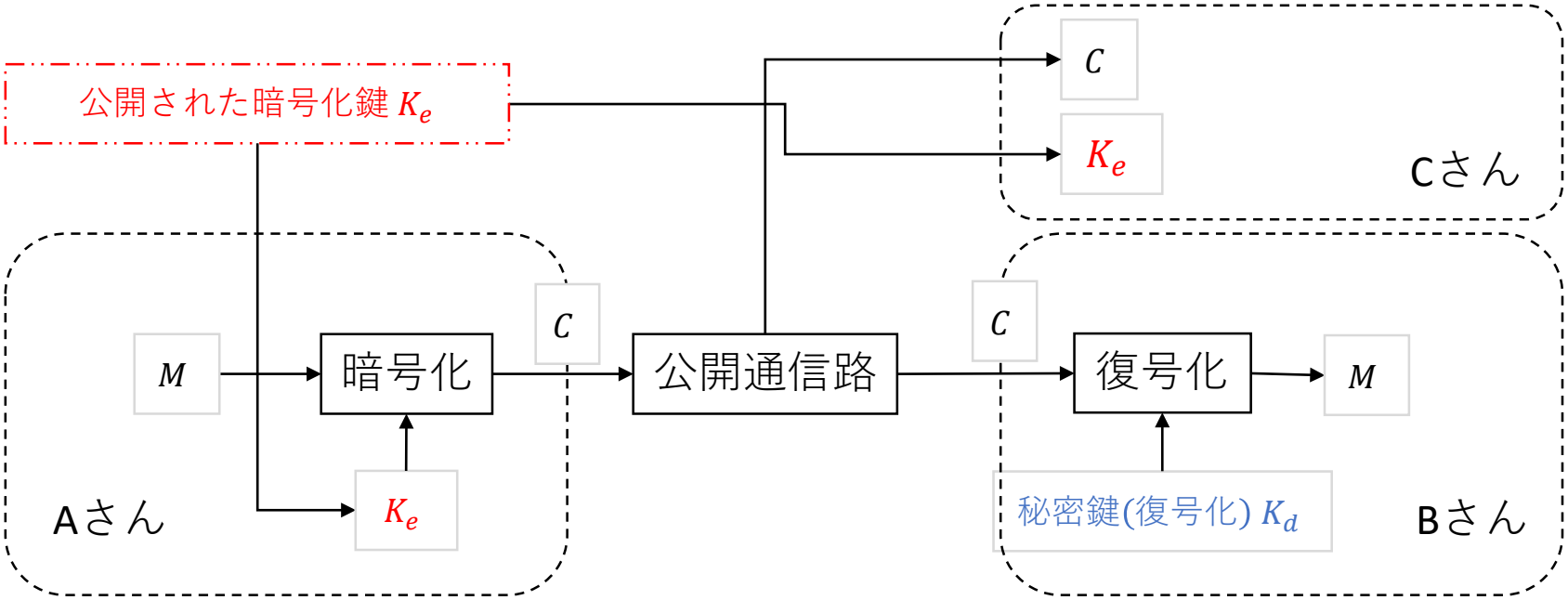
秘密鍵暗号システムの問題点

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から.

4.3.2節　公開鍵暗号システム

1. 暗号化鍵 K_e を第三者にも公開することができる
2. ゆえに、安全な通信路を利用する必要がない
3. 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することができる．しかし、暗号化鍵では復号できない、とする．
4. 下記システムでは、暗号文を受信するBさんが暗号化鍵と秘密鍵のペアを作成する
5. これらから学ぶRSA暗号は、公開鍵暗号システムの一種である



1. 秘密鍵暗号システムと公開鍵暗号システムの違い
    1. 秘密鍵暗号システムでは、「暗号化鍵 K_e」 ＝ 「復号化鍵K_d」
       その結果、鍵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では、「暗号化鍵 K_e」 ≠ 「復号化鍵K_d」
       その結果、暗号化鍵を共有する必要がない

2. 誰が鍵を作成するのか？
    1. 秘密鍵暗号システムでは、Aさん（送信者）またはBさん（受信者）のどちらかが鍵を作成する．そして、第三者に知られないように、相手に鍵を渡す．
    2. 公開鍵暗号システムでは、Bさん（受信者）が、公開鍵と秘密鍵（復号化鍵）を作成する．そして、公開鍵のみを公開し、秘密鍵は第三者に知られないように保管する．

6節　RSA暗号（パラメータ：p, q, n, L, e, d）

1. 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、計算する。
   1. 互いに異なる任意の素数pとqを選ぶ
   2. p と q の積 $n := p \times q$ を計算する
   3. $(p-1)$と$(q-1)$の最小公倍数 $L := \mathrm{lcm}(p-1, q-1)$ を計算する
   4. Lと互いに素で、Lより小さな任意の整数 e を選ぶ
      すなわち、e は、 最大公約数 $\gcd(e, L) = 1$ かつ $1 < e < L$ を満たす整数
      ここで、 e と L が互いに素であるとは、 e の L の最大公約数 $\gcd(e, L) = 1$であることに注意する。
   5. eとLに対し、$e \times d_e \equiv 1 \pmod{L}$を満たす整数 d_e を求める

2. このとき、公開鍵（暗号化鍵）と秘密鍵（復号化鍵）は以下のようになる
   1. 公開鍵（暗号化鍵）：(e, n)
   2. 秘密鍵（復号化鍵）：(d_e, n)
   3. 秘密にする情報：(p, q, L, d_e)

1. 鍵作成の例（$(p,q)=(5,11)$ の場合）
   1. $(p,q)=(5,11)$を選ぶ
   2. $n:=p\times q=55$ を計算する
   3. 最小公倍数 $L:=\mathrm{lcm}(4,10)=20$ を計算する
   4. Lと互いに素で、Lより小さな任意の整数 $e=7$ を選ぶ
      最大公約数$\gcd(e,20)=1$ かつ $1<e<L$ を満たす整数$e\in\{3,7,11,13,17,19\}$
   5. $7\times d_e\equiv 1\ (\mathrm{mod}\ 20)$を満たす整数 $d_e=3$ を求める
      具体的に計算すると、求める d_e は $1\sim 20$ の中に必ず存在し、その個数は唯一つであることが分かる

$7\times 1=7\ (\mathrm{mod}\ 20)$	$7\times 8=56\equiv 16\ (\mathrm{mod}\ 20)$	$7\times 15=105\equiv 5\ (\mathrm{mod}\ 20)$
$7\times 2=14\ (\mathrm{mod}\ 20)$	$7\times 9=63\equiv 3\ (\mathrm{mod}\ 20)$	$7\times 16=112\equiv 12\ (\mathrm{mod}\ 20)$
$7\times 3=21\equiv 1\ (\mathrm{mod}\ 20)$	$7\times 10=70\equiv 10\ (\mathrm{mod}\ 20)$	$7\times 17=119\equiv 19\ (\mathrm{mod}\ 20)$
$7\times 4=28\equiv 8\ (\mathrm{mod}\ 20)$	$7\times 11=77\equiv 17\ (\mathrm{mod}\ 20)$	$7\times 18=126\equiv 6\ (\mathrm{mod}\ 20)$
$7\times 5=35\equiv 15\ (\mathrm{mod}\ 20)$	$7\times 12=84\equiv 4\ (\mathrm{mod}\ 20)$	$7\times 19=133\equiv 13\ (\mathrm{mod}\ 20)$
$7\times 6=42\equiv 2(\mathrm{mod}\ 20)$	$7\times 13=91\equiv 11\ (\mathrm{mod}\ 20)$	$7\times 20=140\equiv 0\ (\mathrm{mod}\ 20)$
$7\times 7=49\equiv 9\ (\mathrm{mod}\ 20)$	$7\times 14=98\equiv 18\ (\mathrm{mod}\ 20)$	$7\times 21=147\equiv 7\ (\mathrm{mod}\ 20)$

2. このとき、公開鍵（暗号化鍵）と秘密鍵（復号化鍵）は以下のようになる
   1. 公開鍵（暗号化鍵）：$(e,n)=(7,55)$
   2. 秘密鍵（復号化鍵）：$(d_e,n)=(3,55)$
   3. 秘密にする情報：$(p,q,L,d_e)=(5,11,20,3)$

今後の例題のためにもう一つ具体的な鍵作成の例を示しておく（テキスト記載の例と同じもの（$2^8 \leq n < 2^{16}$を満たすようにpとqを選んだ例））

1. 鍵作成の例（$(p,q) = (17,19)$ の場合）
   1. $(p,q) = (17,19)$を選ぶ
   2. $n \coloneqq p \times q = 323$ を計算する
   3. 最小公倍数 $L \coloneqq \mathrm{lcm}(16,18) = 144$ を計算する
   4. Lと互いに素で、Lより小さな任意の整数 $e = 5$ を選ぶ
      最大公約数 $\gcd(e,144) = 1$ かつ $1 < e < L$ を満たす
      整数 $e \in \{5,7,11,13,\ldots,139,143\}$
   5. $5 \times d_e \equiv 1 \pmod{144}$を満たす整数 $d_e = 29$ を求める

2. このとき、公開鍵（暗号化鍵）と秘密鍵（復号化鍵）は以下のようになる
   1. 公開鍵（暗号化鍵）：$(e,n) = (5,323)$
   2. 秘密鍵（復号化鍵）：$(d_e,n) = (29,323)$
   3. 秘密にする情報：$(p,q,L,d_e) = (17,19,144,29)$

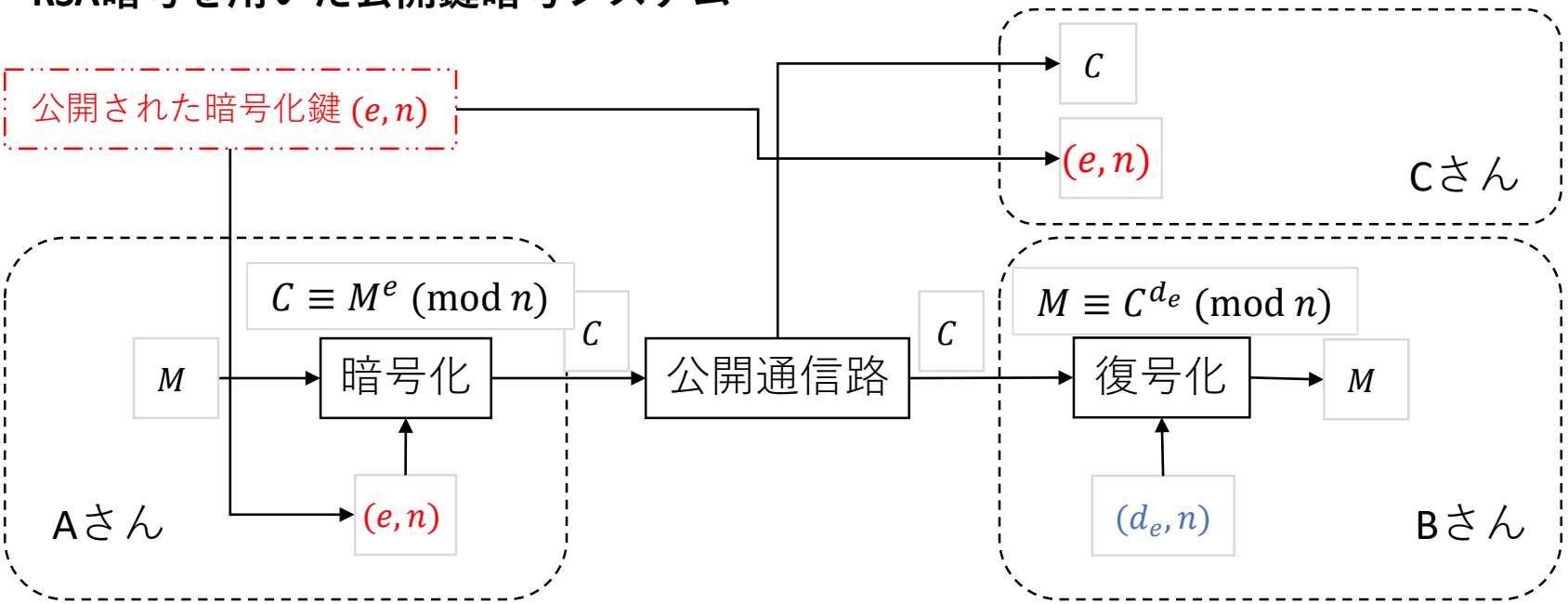
前述まででは、鍵作成について説明をしてきた．次に、具体的な暗号化、復号化の手続きについて説明をする

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**：暗号化鍵（公開鍵）(e,n)を用いてメッセージ（整数）M を暗号化し、暗号文C を生成する。 ここで、$0 \leq M \leq n-1$ とする。
   （課題のプログラムでは、 Mは1バイトで表現できる範囲で考える。すなわち、 $0 \leq M \leq 255 = 2^8 - 1$.）
   $$C \equiv M^e \pmod{n}$$
   ただし、$0 \leq C \leq n-1$ とする
2. **復号化**：復号化鍵（秘密鍵）(d_e,n)を用いて暗号文（整数）C を復号し、メッセージ $\widehat{M}$を復元する
   $$\widehat{M} \equiv C^{d_e} \pmod{n}$$
   ただし、$0 \leq \widehat{M} \leq n-1$ とする
3. 復元したメッセージ $\widehat{M}$ と元のメッセージ M が同じであって欲しい．次式が成り立つことより、$\widehat{M} = M$が成り立つ

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

RSA暗号を用いた公開鍵暗号システム



暗号化鍵$(e,n) = (5,323)$と復号化鍵$(d_e,n) = (29,323)$による計算例

例えば、大文字「C」（10進数で67）を暗号化、復号化してみよう。

1. メッセージ$M = 67$を暗号化すると、$C \equiv 67^5 \equiv 288 \pmod{323}$より、暗号文は$C = 288$となる
2. 暗号文$C = 288$を復号化すると、$\widehat{M} \equiv 288^{29} \equiv 67 \pmod{323}$より、復元したメッセージは$\widehat{M} = 67$となる

（べき乗の計算についての注意としてテキストの例6.2を確認すること）

RSA暗号の暗号化と復号化の例

- 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、シフト暗号の場合と同様に，整数に変換する

  メッセージ：「87 69 87 73 76 76 77 69 69 84 65 84 67 72 79 70 85 83 84 65 84 73 79 78」

  次に、暗号化鍵$(e,n)=(5,323)$を用いて暗号化すると以下の暗号文を得る

  暗号文：「83 103 99 247 247 229 103 103 50 12 50 288 21 129 185 187 87 50 12 50 99 129 108」

  83

- 復号化：暗号化と同様の演算処理を用い、復号化鍵$(d_e,n)=(29,323)$に対応する計算をし、暗号文を復号すればよい

- 注意：下記に示すように、暗号文に区切り記号の空白がないと、復号する際に、どこで区切ればよいか分からない．したがって、何らかの工夫が必要である．そこで、プログラムを作成する際には、データを固定長で扱うことを考えみよう．

  「8310399247247229103103501250288211291851878750125099129108」

  83

2022/11/3 修正

7節　課題（詳細はテキストの7節を確認すること（必須））

1. RSA暗号の暗号化および復号化のプログラムを作成せよ．具体的には、次の暗号化と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_e,n)と暗号化されたファイル 出力：　元のメッセージ（ひら文）ファイル

2. 例6.3に示した2進展開法を採用したRSA暗号のプログラムを作成せよ．

3. 課題1と2において作成したプログラムに対し、次の 10 通りの e の $\{16,32,64,128,256,512,1024,2048,4096,8192\}$ を実装し、それぞれの実行処理時間を計測し、表にまとめ、それをグラフに記せ．

4. 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せよ．

5. 異なる素数 p と q に対し、$p-1$と$q-1$の最小公倍数$L=\mathrm{lcm}(p-1,q-1)$を求めるプログラムを作成せよ．

6. 整数 L に対し、最大公約数 $\gcd(e,L)=1$ かつ $1<e<L$ を満たすすべての整数 e を求めるプログラムを作成せよ．

7. 整数 L とe に対し、 $ed\equiv 1 \pmod{L}$ かつ $1<d<L$ を満たす整数 d を求めるプログラムを作成せよ．

８節　プログラミング

1. プログラミングの準備
2. 参考プログラミング
    1. テキストに示した参考プログラム（RSA暗号の暗号化と復号化プログラム）

その他の参考プログラム

1. 本課題のwebページに示した参考プログラム（以下を確認すること）
    1. 「参考資料」→「参考プログラム」
    2. 「参考資料」→「課題 1 のプログラムを作成するためのヒント(練習プログラム)」