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)」

課題説明用資料

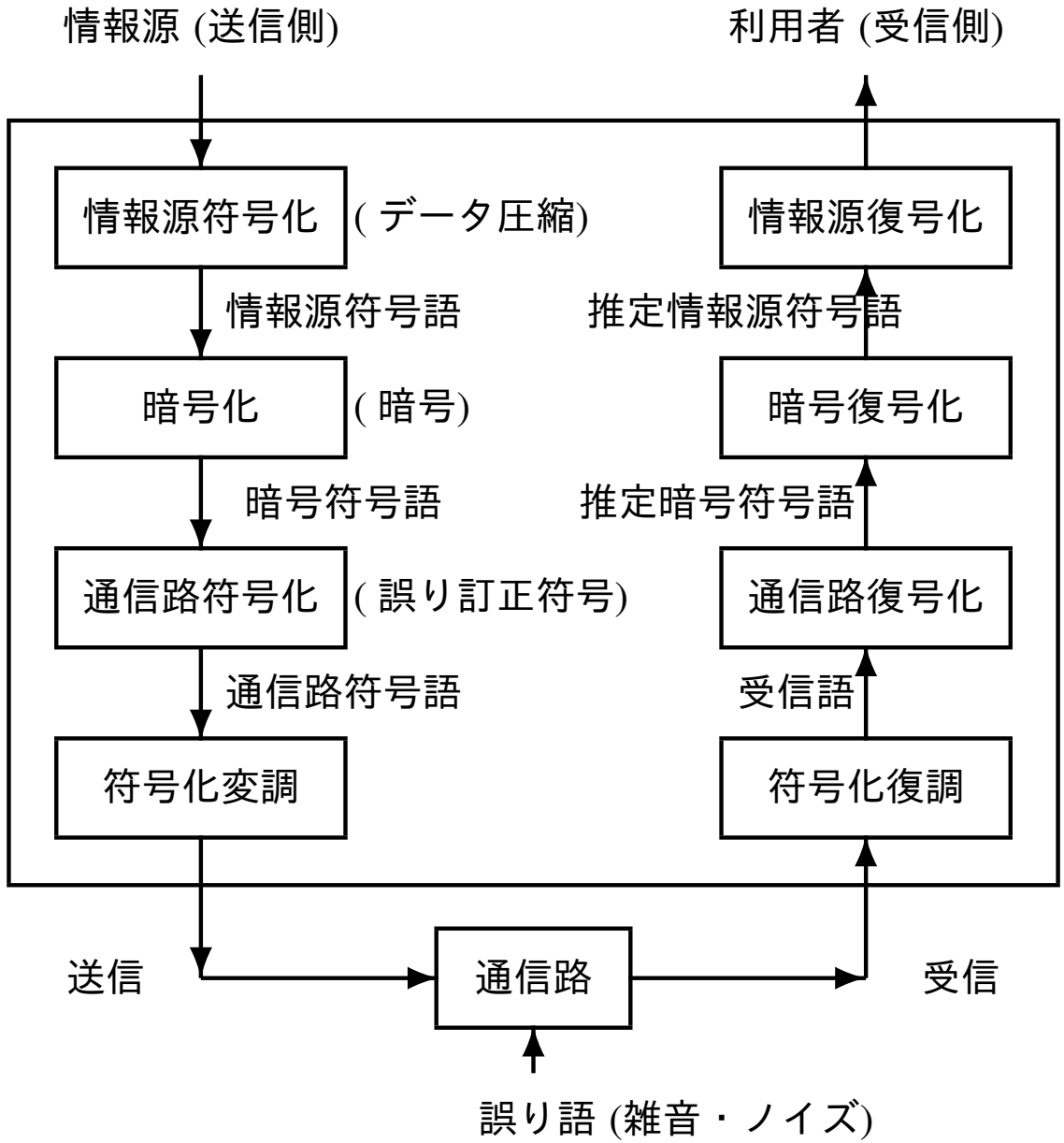
sol: /doc/class/jikken/jikken2018/text/rsasetsumei2018-LF-UTF-8-unix.tex
(Cloud:/home-uec/class/jikken/jikken2017/text/rsasetsumei2016-LF-EUC.tex)

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)

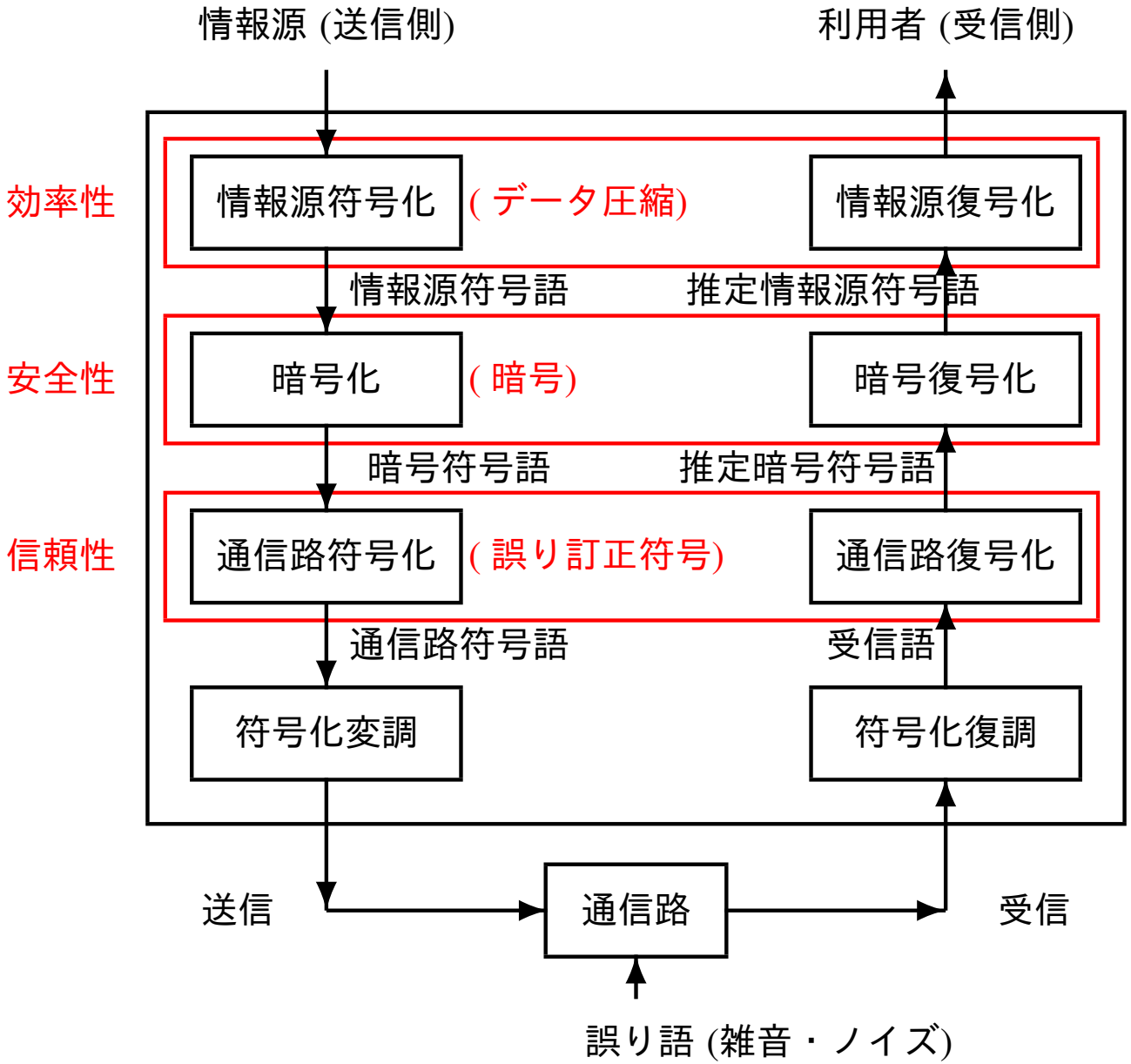
「暗号化の理解と実装」
— RSA 暗号の理解と実装 (プログラミング) —

キーワードは『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



テキストの構成

「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) —

1. 目的
2. 提出レポートの内容 (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
   - 4.1 暗号の具体例（シフト暗号）
   - 4.2 暗号化システムの形式的記述
   - 4.3 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） ← （必要な場合に参照する）
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. 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.

2. 提出レポートの内容（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) 「RSA 暗号（公開鍵暗号）」と「認証」の関係について調べ，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. プログラムの実装，およびその出力結果の様子をレポートに記す．
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. 工夫した点（詳細はテキストの 2 節を参照）
5. 考察（詳細はテキストの 2 節を参照）
6. 感想とコメント（詳細はテキストの 2 節を参照）
7. 参考文献 （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）
8. 紙のレポートとは別に、ソースプログラムを電子メールにて提出する．
   提出先は、担当教員が、別途示す．

3. はじめに

テキストの目的：

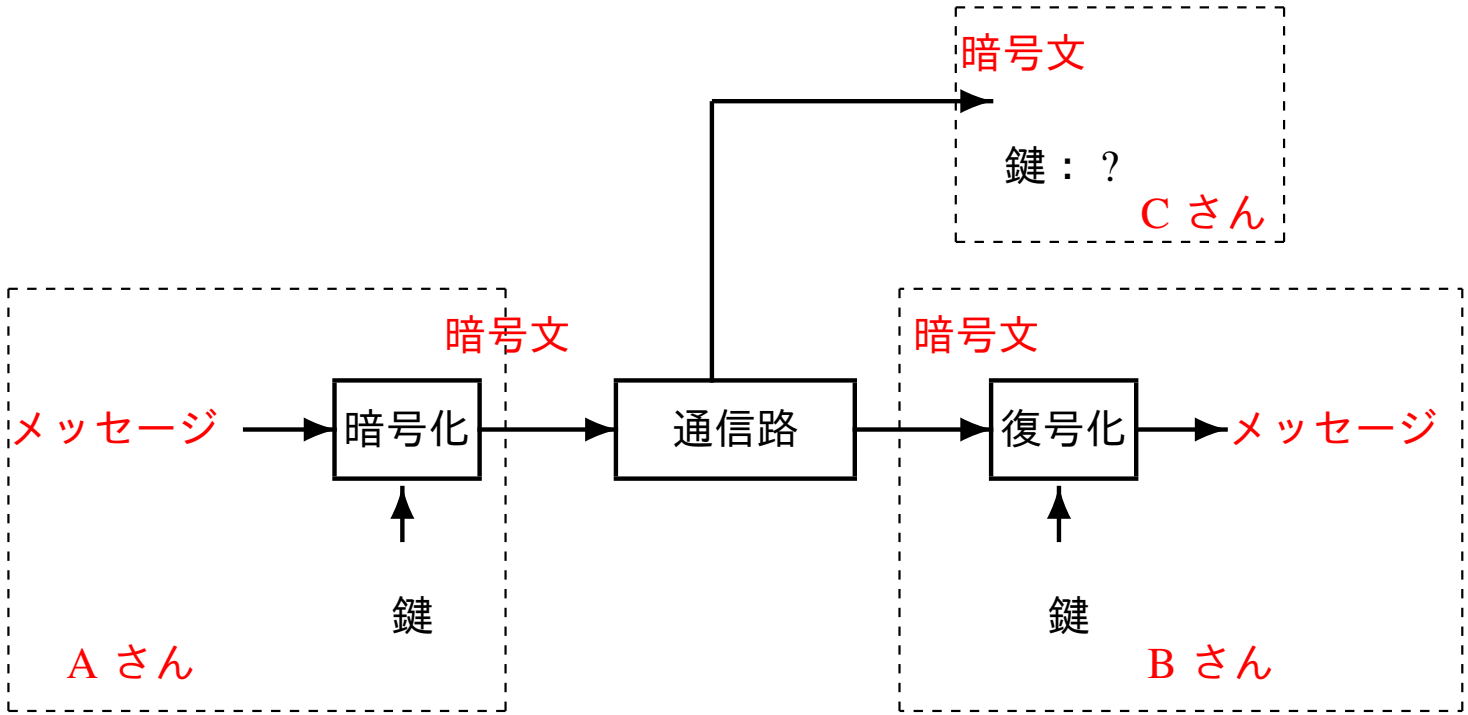
本実験課題で扱う RSA 暗号とよばれる暗号化アルゴリズムの説明、
および、その実装のための諸注意などを説明することにある。

R.L.Rivest, A. Shamir and L. Adleman,
“A Method for Obtaining Digital Signatures and 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ゆずる。

4. 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。



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

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：

ABCDEFGHIJKLMNOPQRSTUVWXYZ

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, . . . , Z}**
2. 暗号文集合 **:= {A, B, . . . , Z}**

暗号化と復号の方法　（ここで、鍵 k は整数。）

1. 暗号化 (鍵 k): メッセージ → 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 → 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

「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　・・・

→　　→　　→　　→　　→

1　　2　　3　　4　　5

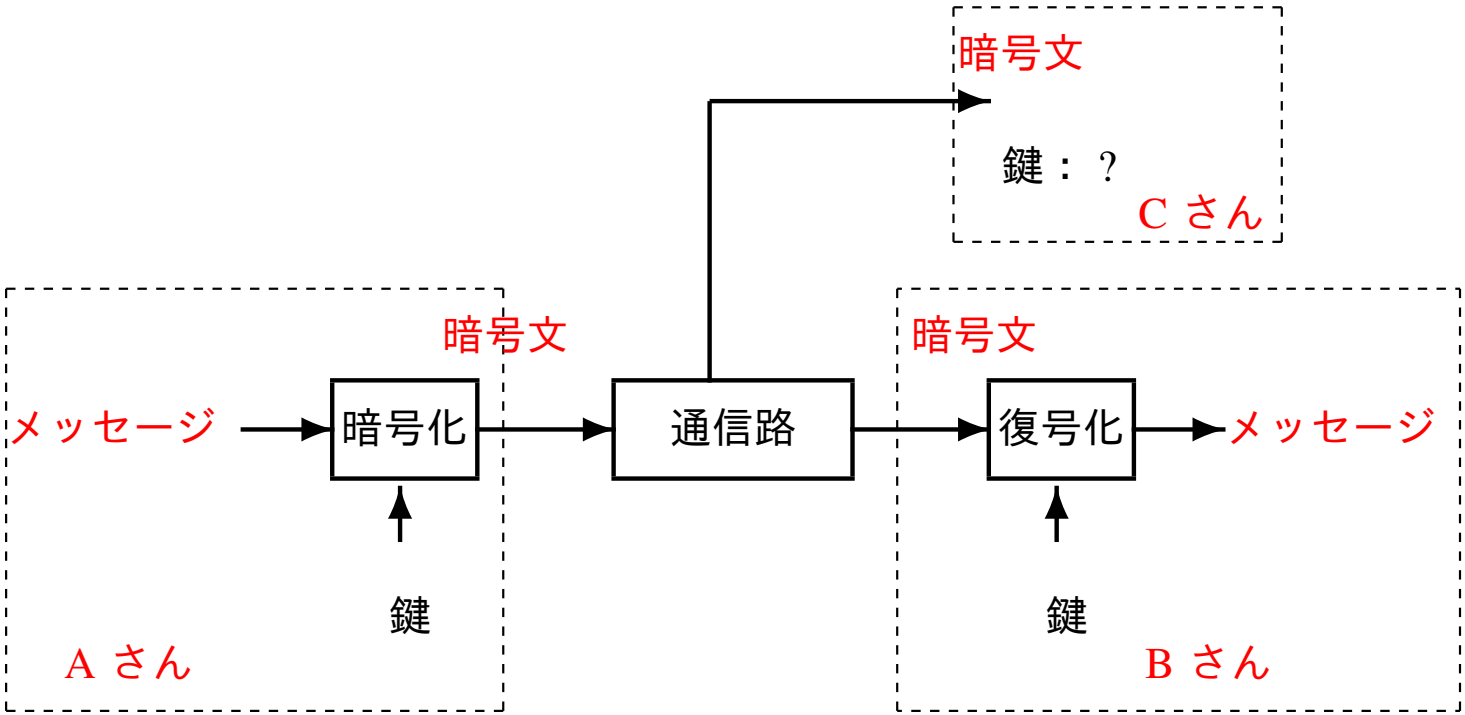
2. “ **W** ” を 右へ **5** だけ (循環) シフト変換すると “ **B** ”

・・・　W　　X　　Y　　Z　　A　　B　・・・

→　　→　　→　　→　　→

1　　2　　3　　4　　5

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、鍵の情報は、第三者の C さん には知られていないものとする。

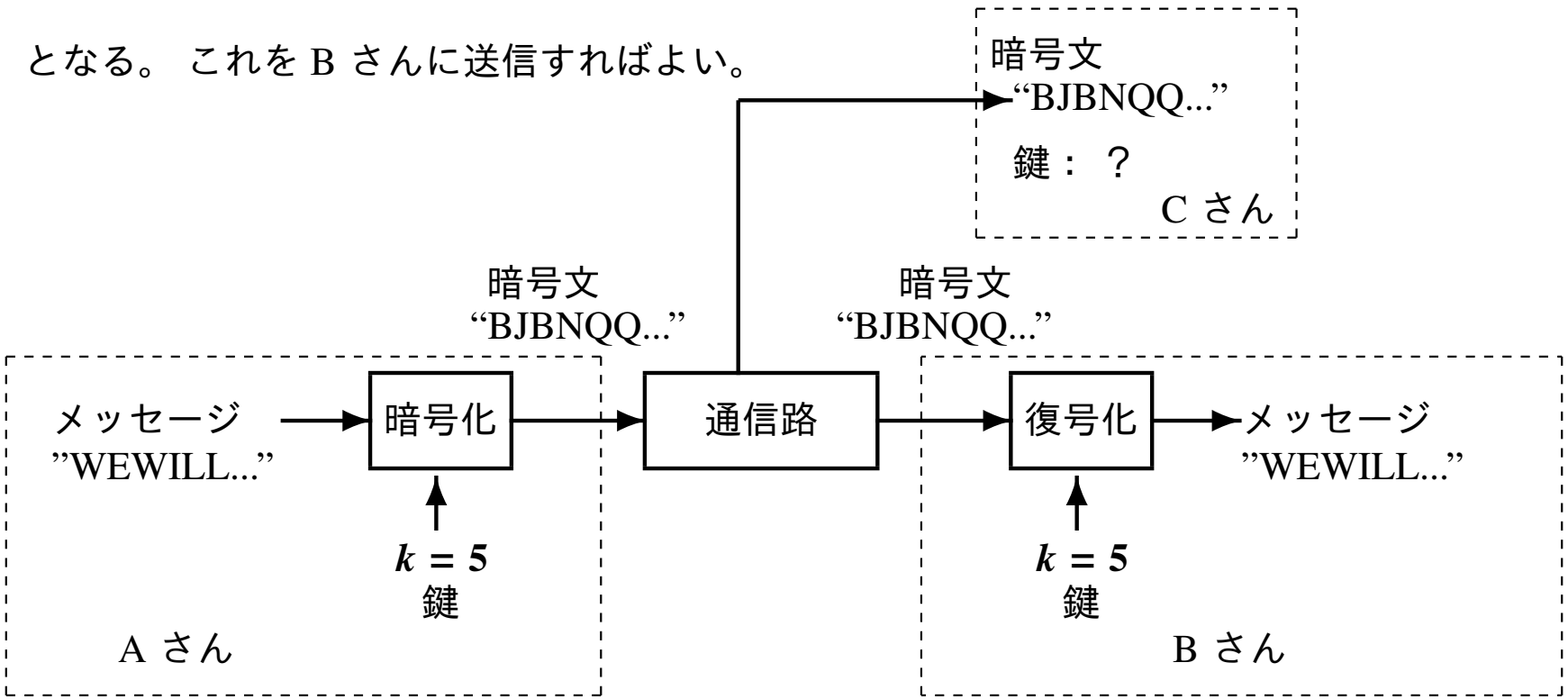
例えば、シフト暗号において鍵 を $k = 5$ として、A さんが B さんに伝えたいメッセージ

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。



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」へ

を考える。そこで、

「ASCII」(文字コード)

を復習しよう。

たとえば、大文字 “ A ” の **2** 進数表現、**10** 進数表現

ASCII の表より、

上位 : **4 ⇔ 0100**

下位 : **1 ⇔ 0001**

これより、

A **⇔ 01000001 ⇔ 65**

なぜなら、

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

「文字」 ⇒ 「整数」

文字：{A,B,C,. . . ,Y,Z}
整数：$\mathbf{Z_{26} = \{65, 66, \ldots, 89, 90\}}$（ASCII による 10 進数表現）
余り：$\mathbf{Z_{26} = \{0, 1, 2, \ldots, 24, 25\}}$（26 を法とする合同関係を考える）
つまり、26 で割った余り

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**	**6**	**7**	**8**	**9**	**10**	**12**

「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	**74**	**75**	**76**	**77**	**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	**88**	**89**	**90**	**91**	**92**	
					65	**66**	

87 + 5 = 92,

92 ≡ 66 (mod 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。

876987737676776969846584677279708583846584737978

667466788181827474897089727784759088897089788483

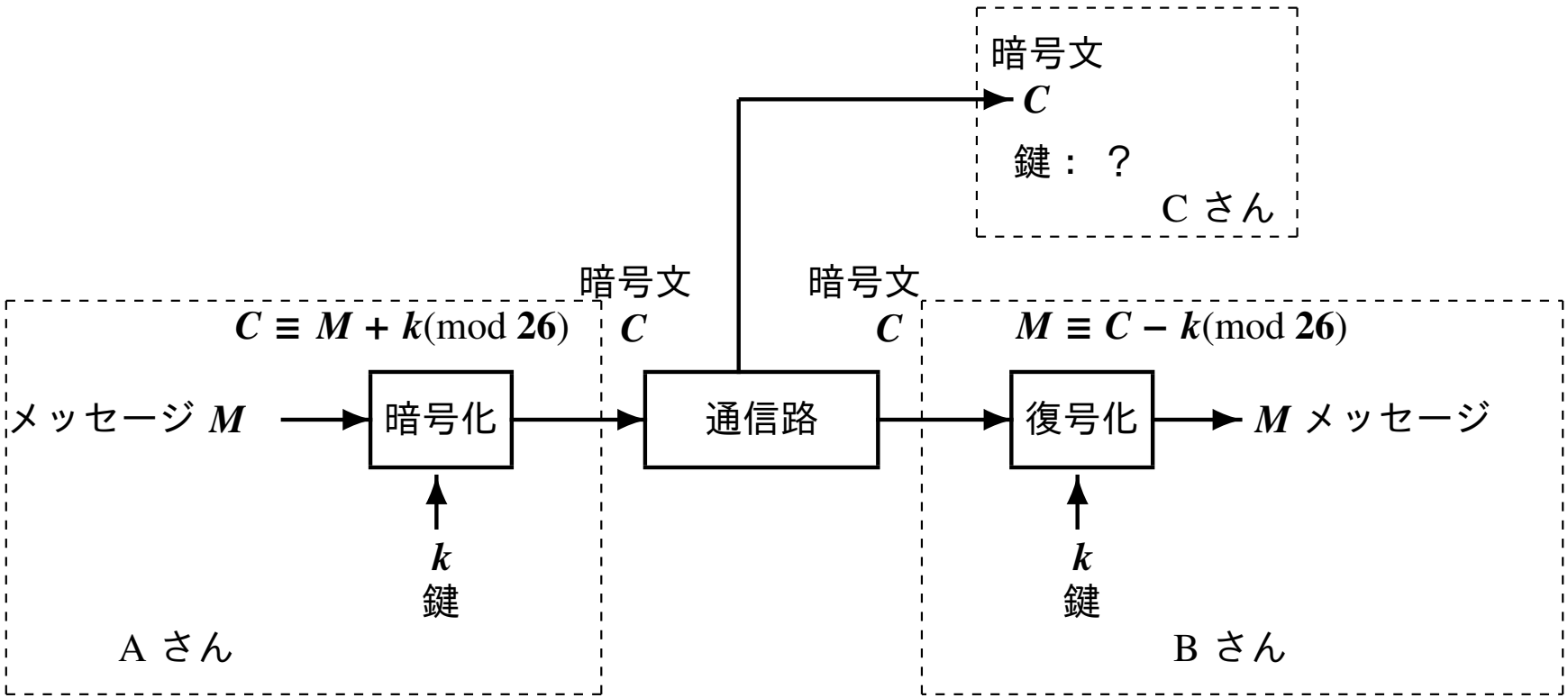
上記の例の場合、全てが 2 桁の数字のみであるから、区切り記号の空白がなくても、先頭から順に 2 桁の数字を読むことで文字を対応できる。しかし、一般には、1 桁、2 桁、3 桁などが混在する。このような場合は、区切り記号を入れたり、固定長で表現するなどの工夫が必要となる。

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 を整数に変換：

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**

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　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)

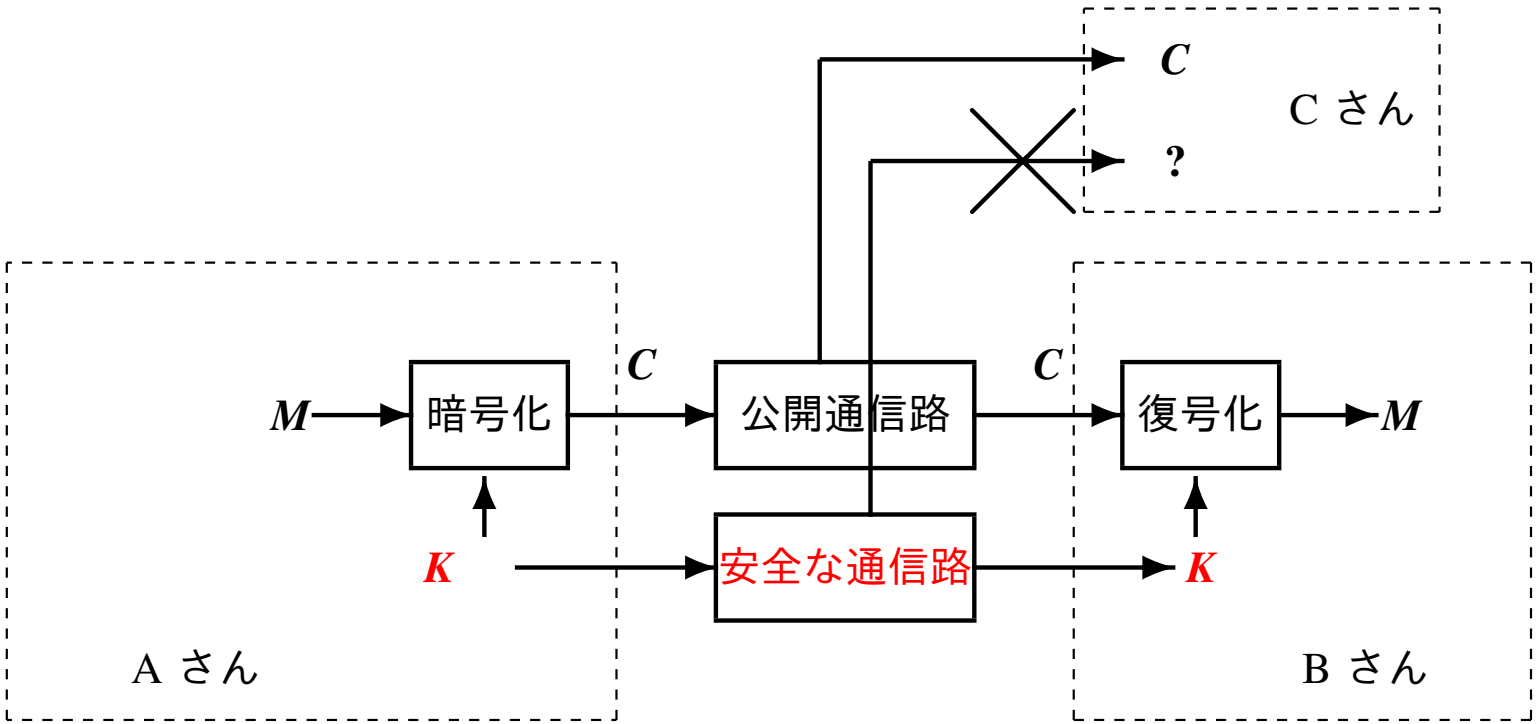
と

「公開鍵暗号システム」

の 2 種類に分類する。

4.3.1 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
2. 鍵の作成は、Ａさんまたはｂさんのどちらでも可能



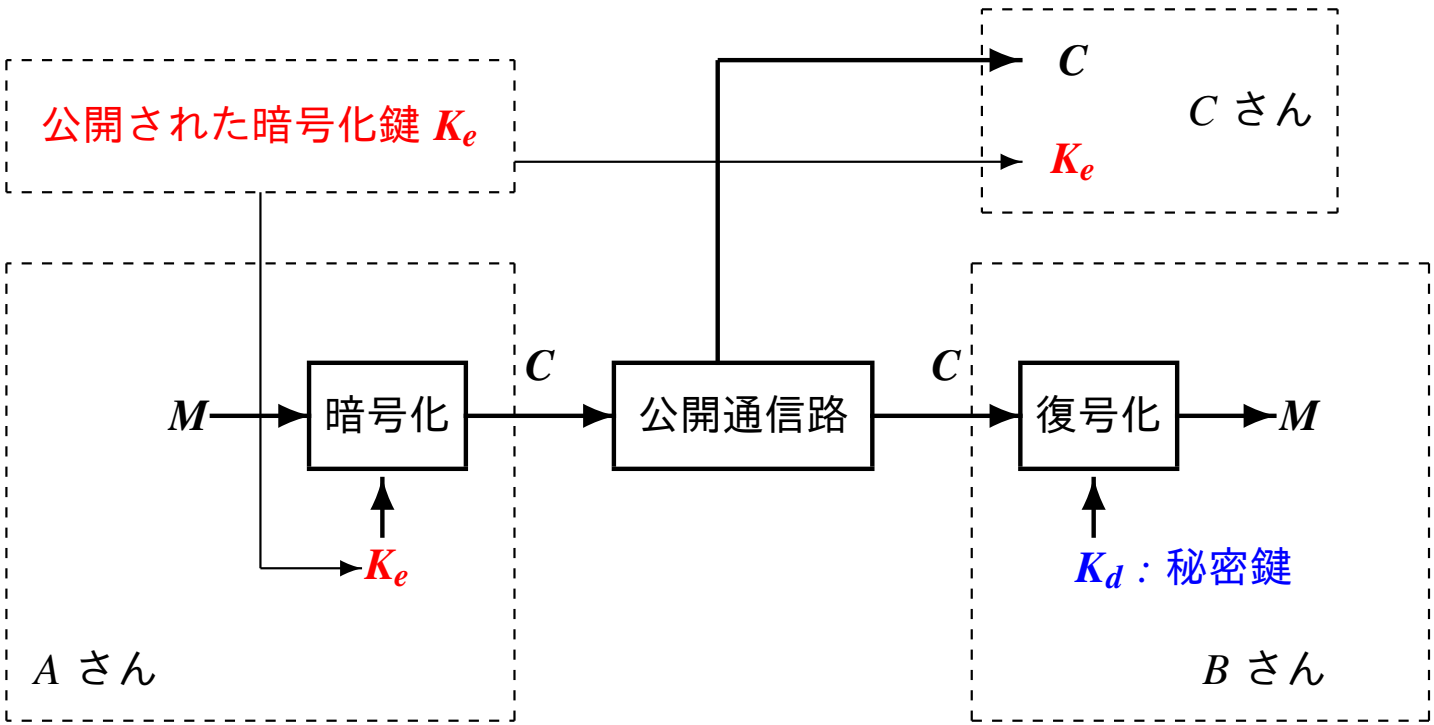
秘密鍵暗号システムの問題点

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.

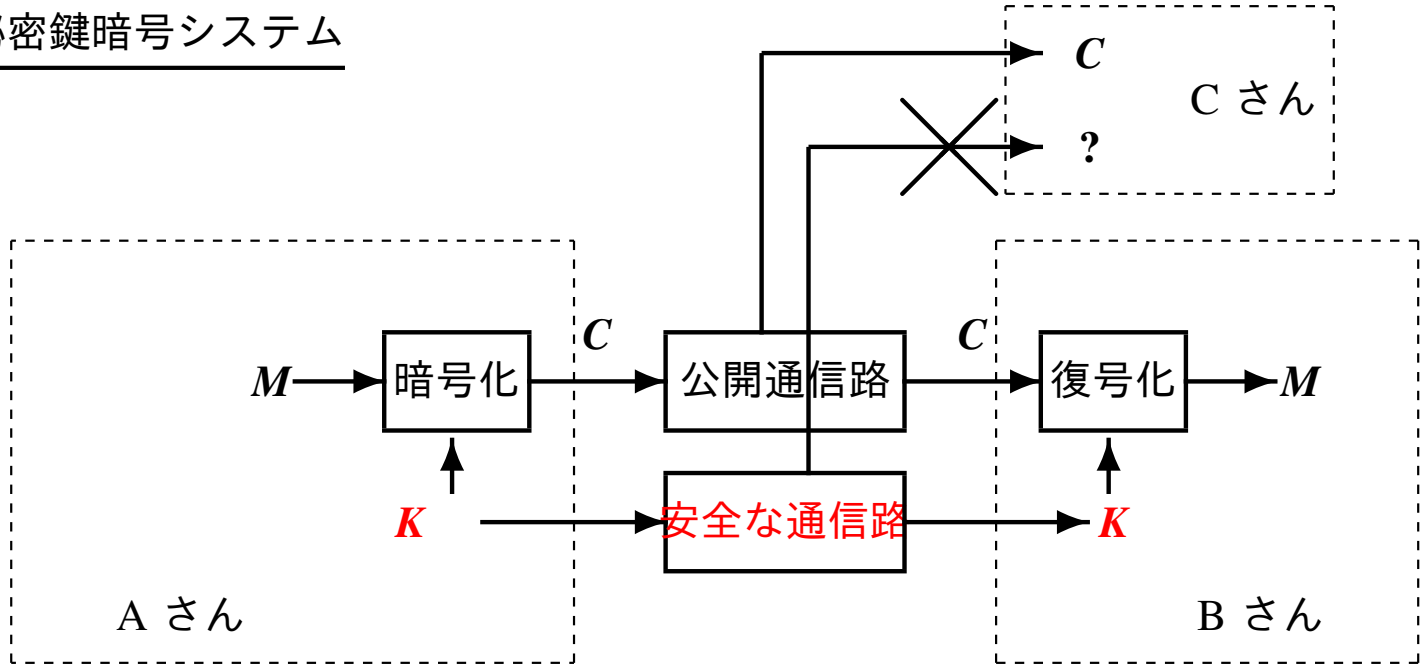
すなわち、安全な通信路を利用して送信する必要がある

4.3.2 公開鍵暗号システム

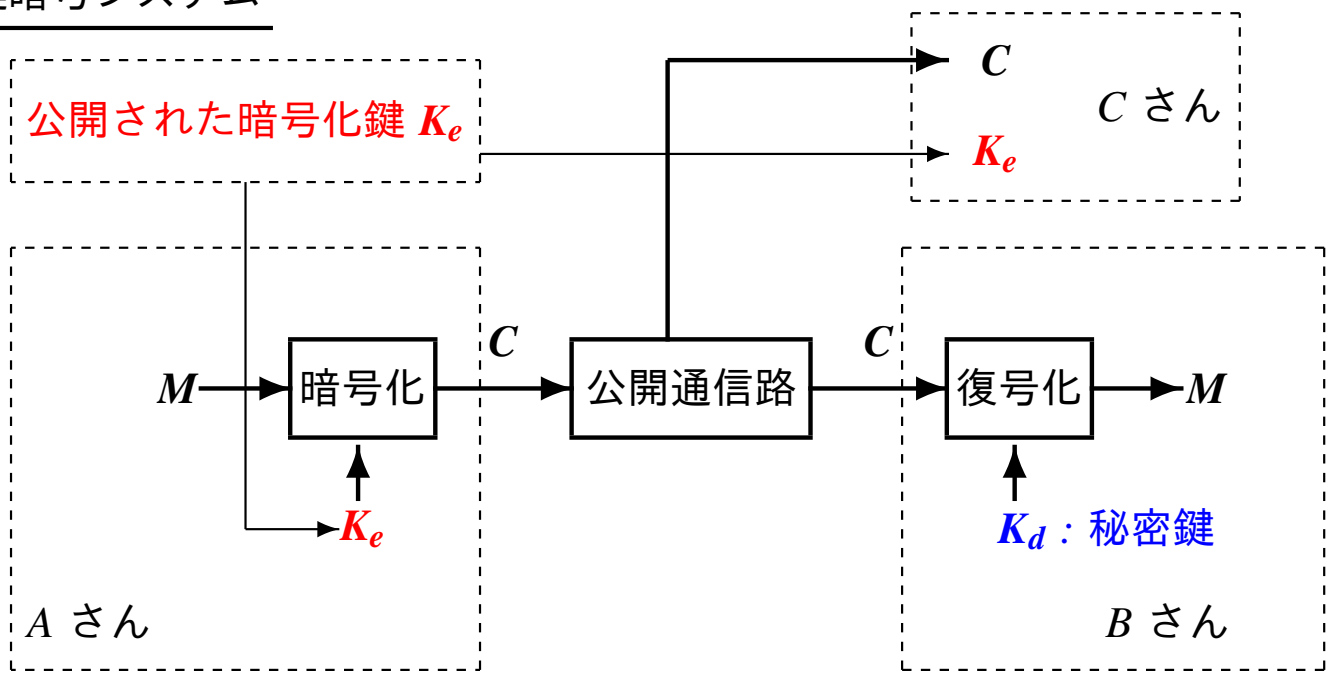
1. 暗号化鍵 K を第三者にも 公開する ことができる
2. ゆえに、安全な通信路を利用して通信する必要がない
3. 公開された暗号化鍵 K_e とは異なる秘密鍵 (復号化鍵) K_d により暗号文を復号することができる。しかし、暗号化鍵では復号できない。
4. 下記のシステムでは、暗号文を受信するＢさんが暗号化鍵と秘密鍵のペアを作成する
5. これから学ぶ RSA 暗号 は、公開鍵暗号システムの一種である



秘密鍵暗号システム



公開鍵暗号システム



〇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：「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

2. 公開鍵暗号システム：「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はない

〇誰が鍵を作成するのか？

1. 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。

2. 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。

6. RSA 暗号 (パラメータ p, q, n, L, e, d_e)

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. 互いに異なる任意の素数 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 を計算する.

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

3. L と互いに素で L より小さな任意の整数 e を選ぶ。

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

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

4. 次式を満たす整数 d_e を計算する。

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

(d_e を求める手法として拡張 Euclid 法を利用する方法がある。テキストの例 6.1 を参照)

各パラメータ p, q, n, L, e, d_e と鍵および秘密にする情報の対応

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

↓

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, L, d_e

$(p, q) = (5, 11)$ の場合の例:

1. $(p, q) = (5, 11)$ とすると, $n = p \times q = 5 \times 11 = 55$　となる
2. $L = \mathrm{lcm}(p - 1, q - 1) = \mathrm{lcm}(4, 10) = 20$
3. 次の e の選択候補の中から $e = 7$ とする. ただし, $\gcd(e, 20) = 1$ かつ $1 < e < 20$
   $e \in \{3, 7, 11, 13, 17, 19\}$（$e$ の選択候補）
4. $d_e = 3$. ただし, $7 \times d_e \equiv 1 \pmod{20}$
   具体的に計算すると, 求める d_e は $1 \sim 20$ の中に唯一つ存在することが分かる

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

このときの鍵は,

1. 暗号化鍵 (公開鍵): $(e, n) = (7, 55)$
2. 復号化鍵 (秘密鍵): $(d_e, n) = (3, 55)$

$(p, q) = (17, 19)$ の場合の例:

1. $(p, q) = (17, 19)$ とすると， $n = p \times q = 17 \times 19 = 323$ となる
2. $L = \mathrm{lcm}(17 - 1, 19 - 1) = \mathrm{lcm}(16, 18) = 2 \times 2^3 \times 3^2 = 144$
3. 次の e の選択候補の中から $e = 5$ とする.

   ただし, $\gcd(e, 144) = 1$ かつ $1 < e < 144$

   $e \in \{5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35, \ldots, 139, 143\}$（$e$ の選択候補）
4. $d_e = 29$. ただし, $5 \times d_e \equiv 1 \pmod{144}$

このときの鍵は,

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

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.

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

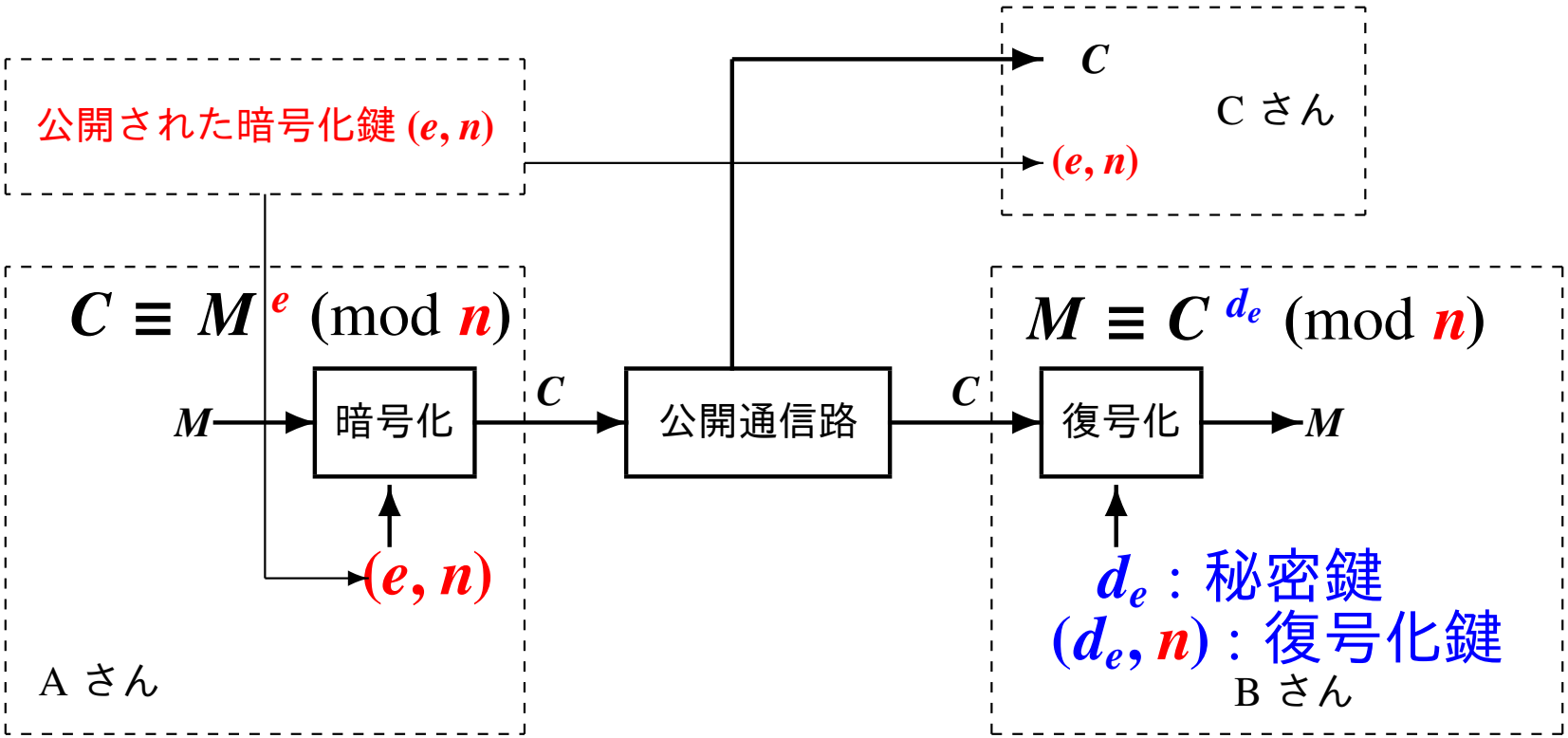
$\widehat{M}$ が C を復号したメッセージになる。ただし、$0 \leq \widehat{M} \leq n-1$ とする。

3. 復号したのであるから $\widehat{M} = M$ であって欲しい。

実際に、次式が成り立つ事より、 $\widehat{M} = M$ が保証される。

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

RSA 暗号を用いた公開鍵暗号システム



先程に示した鍵を例に計算してみよう！　.

1. 暗号化鍵 (公開鍵): $(e, n) = (5, 323)$.　　メッセージ M を暗号文 C に暗号化
2. 復号化鍵 (秘密鍵): $(d_e, n) = (29, 323)$

たとえば、大文字 “ C ”（10 進数表示で “67”）を 暗号化し、復号してみよう　.

1. メッセージ $M = 67$ を 鍵 $(e, n) = (5, 323)$ で暗号化すると暗号文は $C = 288$ となる：

   $$C \equiv M^e = (67)^5 \equiv 288 \pmod{323}$$

2. 次に、暗号文 $C = 288$ を鍵 $(d_e, n) = (29, 323)$ で復号すると復号後のメッセージは $\widehat{M} = 67$ となる：

   $$\widehat{M} \equiv C^{d_e} = (288)^{29} \equiv 67 \pmod{323}$$

上記の計算は、電卓でもできる:
(オーバーフローにならないように 1 回の乗算ごとに modulo で計算することが重要.) つまり、毎回、割り算をして余りを計算することがポイントとなる。

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

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

どれだけ大きな数字を扱うのかを実感するために、数式処理システム Mathematica(マセマティカ) を利用して計算してみよう（Wolfram Alpha を利用）

1. Move to http://www.wolframalpha.com/
2. $\mathbf{67^5}$ と $\mathbf{288^{29}}$ を計算してみよう。

   $\mathbf{67^5}$ を計算したい場合は、次のように書いてみよう：

   (67)^(5)

   ここで、 記号 ”^ ” はべき乗の記号
3. $\mathbf{67^5}$ (mod **323**) と $\mathbf{288^{29}}$ (mod **323**) を計算してみよう。

   $\mathbf{67^5}$ (mod **323**) を計算したい場合は、次のように書いてみよう：

   mod[(67)^(5), 323]

暗号化 : RSA 暗号の暗号化鍵 $(e, n) = (5, 323)$ 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、どこで区切ればよいか分からない. :
固定長で扱うことを考えよう.

831038399247247229103103501250288211291851878750125099129108

7. 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_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) のファイル.

2. 例 6.3 に示した二進展開法を採用した RSA 暗号のプログラムを作成し、実装せよ。

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 の値 **{16, 32, 64, 128, 256,512, 1024, 2048, 4096, 8192}** に対し，それぞれの実行処理時間を計測し，表にまとめ，それをグラフに示せ.

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し、実装せよ。
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し、実装せよ。
6. 整数 L に対し、$\gcd(e, L)=1$ 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し、実装せよ。
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し、実装せよ。

8. プログラミング

8.1 プログラミングの準備

8.2 参考プログラム

1. テキストに示した参考プログラム
    1. RSA 暗号の暗号化（符号化）と復号化プログラム
2. ホームページ記載の指示で得られる参考プログラム
    1. a2a.out ：ファイルコピーをするプログラム (a2a.c)
    2. a2AA.out ：大 (小) 文字を小 (大) 文字に変換するプログラム (a2AA.c)
    3. shift.out：シフト暗号のプログラム (shift.c)
    4. rsa.out ：RSA 暗号のプログラム
    5. prime.out：素数を求めるプログラム
    6. gcd.out ：拡張ユークリッド法を実行し、最大公約数を求めるプログラム
    7. lcm.out ：最小公倍数を求めるプログラム（実行ファイル）
    8. findinge.out：与えられた正整数 L に対し、$\gcd(e, L) = 1$ かつ $1 < e < L$ を満たす e をすべて求めるプログラム