# 暗号技術のしくみのデモンストレーション例 ―小学校の剰余計算の学習のみを前提とするRSA暗号での例―

中村博文[1]

# A Demonstration Example of Mechanism of Encryption Technology —An Example with RSA Encryption Assuming Only Learning of Remainder Calculation at Elementary School—

Hirofumi NAKAMURA[1]

(令和2年10月1日受理)

**あらまし**　データを秘密にして通信や記録をする暗号技術が、実際には計算でなされていることについて、小学校で習う剰余計算の学習のみを前提として、23 分程度でデモンストレーションする例を報告する。具体的には、RSA 暗号の暗号化と復号のアイデアを、比較的小さい数で確かめながら、小学 4 年生以上の多くが理解する内容になっている。その中で、0～32 についての 0 乗から 32 乗までの数を 33 で割った余りの一覧表で発見できる余りの性質（33 で割った余りの世界では 0～32 のどれでも 21 乗すると元と同じという性質を、デモンストレーションでは『おもしろい性質』と呼んでいる）と、この 21 が 2 数の積であるため暗号に応用できること（デモンストレーションでは RSA 暗号の『キモ』と呼んでいる）に触れている。また、このような内容だけで提示物を作成すると数と文字だけになり無味乾燥ぎみであるものの、児童・生徒から大人まで比較的多くが視聴している映画『サマーウォーズ』に関連する事柄を織り交ぜて並行させることで、ある程度の興味と期待と集中の中での実施をねらっている。暗号解読に関連した計算の実演も含むものの提示中心であるが、余り計算が暗号として使用できる理由を参加者の多くが理解するデモンストレーションである。本校の毎年1回の科学イベントとなっている『おもしろ科学フェスティバル』において、剰余計算を学習済みの小学生から大人までを対象に実施した状況も報告する。

**キーワード**　[出前授業，科学イベント，小学生，RSA 暗号，サマーウォーズ]

## 1　はじめに

本稿は、科学イベント等や授業で児童・生徒・学生の数理への興味を助長するものとなるようにと考えた一取り組み例の報告である。具体的には、通信や記録において、もし情報が盗まれても、情報の機密性保持が可能で、それが計算でなされていることについて、小学校で習う剰余計算の学習のみを前提として、RSA暗号の暗号化と復号を具体例にした23分程度でのデモンストレーション例の報告である。

小中学生が主対象の本校おもしろ科学フェスティバル（年に1回、校内で1日で開催）で、家族や高大生も対象に誤り訂正を題材に出展[1)]して以来、RSA暗号[2)]などの暗号を扱いたいと思案していた中、関連情報[3~5)]との遭遇や、先述の出展[1)]での余り計算の利用経験などが繋がり、実施に至った。

1 都城工業高等専門学校一般科目　General Education Division, National Institute of Technology(KOSEN), Miyakonojo College

本稿で暗号技術やそのひとつである RSA 暗号を改めて解説することは略す。おもしろ科学フェスティバルについてや、それへの筆者の出展の動機に関しては、文献 1)に多少記載している。

## 2　本デモンストレーションにおける方針等

概ね以下の方針のもと、内容を構成した。

- 関連証明と鍵作成関係は全く省くが、RSA 暗号の符号化から復号までの流れと、暗号として使える理由にはきちんと触れる。
- 余りの計算に慣れてきた小学 4 年生から大人までが対象で、中でも小学 4 年生が確実に理解すること（わり算を既知という小学 3 年生もなるべく）。
- タイトルを「余り計算で分かる映画『サマーウォーズ』の暗号」とし、関連出版物[2,6~9]からの引用で済む範囲で、全参加者の期待に違わぬよう、作品との関連[3,4]も示す。（出展タイトルは、的確で短く、しかし、勘違いされにくいことを心がけた。イベントの来場者が張り紙に書いている出展タイトルの「計算」の字句を気にして敬遠する姿も見かけるが、一方でこの出展への参加者には若干の覚悟を期待できると感じている。）
- 参加者の演習は時間的に設けられないが、計算例は、その場でパソコンで計算して提示する。
- 用語はかけ算、わり算、余り、暗号、解読、RSA 暗号までとし、積、何乗、剰余、暗号化、鍵、素数、素因数分解、アルゴリズムは用いない（都度の若干の補足や後述の「おまけ」で一部例外あり）。
- 画像は使用しない。（使用すると面白くはなるが、肝心の数字に対する集中をそぐ懸念がある。）
- 所要時間は出展場所への出入りの時間以外に 23 分以内とする。多少の時間調整用の省ける内容を、「おまけ」として区別して内包しておく。
- おもしろ科学フェスティバルでは、小中学生と年齢の近い本校学生に可能なら協力者を募り、学生がデモンストレーションできるようスライドとシナリオ例を予め作成しておく。多少のアドリブは可とする。（令和元年の出展では、途中の確認用で後述するスライド 19、20 の 2 枚を足した。）
- おもしろ科学フェスティバルで協力者が得られた場合、1 日計 10 回の 30 分毎の繰り返しを学生 3 人（役割をプレゼン役、案内役と呼ぶことにする。各回各ひとり。更にもうひとりは、立ち合いまたは補助で、非番の時間帯も設ける。）で交替して分担する。主として話す学生ひとり（プレゼン役）は、他の学生に補助を頼んでも構わないことにする。案内役は出入りや着席等を把握する。
- 初歩的な用語の解説や暗号化及び復号の概念図も載せた配布資料を、持ち帰り用に用意する。その中に、その資料のカラー版とスライドを Web 掲載している URL の QR コードも載せておく。

## 3　デモンストレーションの内容

表 1 にデモンストレーションの内容の概要を示す。スライドのページ（頁）番号も記載している。その 13 と 15 は、スライドではなく、計算の実演例の内容である。

本稿の後ろ側に、付録として、デモンストレーションで用いるスライド等の例と、その提示の際のシナリオ例を含むイベント出展での進行例と、配布資料の例を掲載している。

なお、これらには次の実施を想定した修正を含む。

デモンストレーションの中で用いている、2 を 21 個かける例は、小学生等にとって理解に十分でかつ容易な例として、全ての可能性の中から選択した。

表 1　スライド等の順序と触れる事柄

| 頁 | 触れる事柄<br>（この表中では言い回しの初出を太字） |
|---|---|
| 1 | タイトル |
| 2, 3 | 映画『**サマーウォーズ**』も引き合いに**暗号**、**解読**の説明と、以降のあらましの説明（以下のほぼ全スライドで上部に同じ形式の目次を挿入） |
| 4 | 例を用いて余り計算を復習（大人にも有効） |
| 5 | 2 をかける個数を増やしながら 33 の剰余を例示 |
| 6 | 更にかけていきながら、余りが途中で元の数に戻ることの確認と、次ページで多量の数で驚かないようにとの断り |
| 7 | 『実に面白い』（ドラマ『ガリレオ』、東野圭吾原作）を引き合いに『**おもしろい性質**』として印象付けながら、0～32 全てで 21 個かけると元に戻ることを、予め計算した表で確認 |
| 8 | 2 を 21 個かける例、2×2×2=8 を 7 個かける例のあと、7 を知る人だけが元に戻せることを『**キモ**』として印象付け、**RSA 暗号**という名前も紹介（適宜、一言だけ、33 が 2 つの数をかけたものだからと） |
| 9 | RSA 暗号の暗号化と復号のまとめ：2 を 3 回かけた 8 があるとき、8 を 7 回かけた人だけが 2 が分かる |
| 10, 11 | **ガードナー**の**暗号クイズ**[6]を紹介 |
| 12 | RSA 暗号の解読の例示（素因数分解ができたあとをということで提示） |

| | |
|---|---|
| 13 | 小さい数の場合でデータとプログラムをテキストファイルから切り貼りして数式処理系（Maxima）で実際に解読の計算を実演（名前だけ、拡張ユークリッドの互除法を紹介） |
| 14 | **アトキンスら**の素因数分解の使用資源と結果[7]を提示 |
| 15 | アトキンスらの素因数分解結果を用いデータとプログラムをテキストファイルから切り貼りして数式処理系で実際に解読の計算を実演（名前だけ、バイナリ法を紹介） |
| 16 | ガードナーの暗号クイズの内容と解読結果をまず数で表示[7] |
| 17 | ガードナーの暗号クイズの答（英文）[7]を導出 |
| 18 | 映画『サマーウォーズ』ではどのように表れているかについて、OZ（オズ）のパスワードや桁数[8,9]及び暗号文の字面[9]の一部を挙げ比較、これらから、映画で使われている暗号はRSA暗号との推測を提示 |
| 19, 20 | 『おもしろい性質』と『キモ』が分かったかそれぞれ挙手で確認 |
| 21 | （21～25は「おまけ」として）<br>モジュロ演算という言葉が出てくること、余り繋がりであること、曜日が計算で分かること、紹介程度に公式の存在 |
| 22 | 名前だけ、**ショア**（Shor）の方法と量子コンピュータを紹介 |
| 23 | 実用化がまだのためRSA暗号は大丈夫と言及 |
| 24 | 映画にShorという字[9]が出てくるのを探してはと参加者に勧める、また、主人公は積を元の2数に分ける計算をしたかも知れないとの推測を提示 |
| 25 | 時間によって適宜（時間がないなら飛ばす）：使用した例と用語の入った暗号化と復号の概念図で、用語を流れと共に紹介 |
| 26 | 最後に、映画と暗号クイズとの関連、映画の暗号がRSA暗号との推測、RSA暗号が現役など言及 |
| 27 | タイトルを再表示（終了を表す意味と、次の入室者にとっての確認用で） |
| 28, 29 | 参考文献（文献を掲載している資料を配布する場合には提示を省く） |

## 4　実施状況

平成30年と令和元年の第6回と第7回おもしろ科学フェスティバルと授業での実施に関して述べる。KOSENまちなか科学フェスティバル(校外で実施)の出展においては筆者のみでデモンストレーションしたが記録不十分のため割愛する。

おもしろ科学フェスティバルとして来場者にアンケートが実施されており、以下、両年度の集計情報の使用許可を得て記す（都城工業高等専門学校学生課教務係及び小中学校教育支援グループ提供)。

平成30年と令和元年で（以下で、列記はこの順序)、来場者数は1540人と1620人で、アンケートへの回答者数は230[120]人と180[120]人であった（この段落の人数は概数、角かっこ内は以下も小学4年生から大人までと分かる回答者の人数)。

アンケートの中には「楽しかったイベント」という尋ね方で35件と34件の出展の中から複数回答で選択する設問がある。それによると、本稿のデモンストレーションの出展への選択は7[7]人（内小学生が4年生1人）と16[11]人（内小学生が、3、4年生2人ずつと6年生の計5人）であった（出展あたりの平均は33[18]人と20[12]人であった)。本稿の出展への参加者は両年とも10回で少なくとも80人程度以上であった。これらの比率からは、本稿のデモンストレーションは地味で敬遠されがちな題材の割には協力学生の頑張りもあって健闘したと思われる。なお、本稿で参加者という言葉を用いているが、他の出展の殆どが何かしらのいわゆる参加型であるのに対して、本稿のデモンストレーションの出展は視聴のみであったことは、大きな相違点である。

両年度で、シナリオ例とスライドに大きな差異はなかったが、参加者にとっての印象の違いに関わりそうな思いあたる事柄を挙げておく。

平成30年はパソコン演習室で実施した。教卓画面のスライド等の表示が画面転送で全席のパソコンに提示できる。参加者は最初と最後以外では殆どパソコン画面を見る状況であった。(パソコン演習室は来場者の動線からそれるため多少呼び込みもした。)

令和元年は、むやみに省くと参加者に伝わらないことを協力学生により念押しした。また、普通教室でプロジェクタスクリーンに投影した。プレゼン役はその横にいてパソコン操作もする。途中で2つ質問をする機会もあった。姿や身振りも見える位置であり、毎回ではなかったがアドリブ的にドラマや映画の特徴的なセリフを真似る回数がより多かった。

平成30年は、参加者に尋ねておらず理解度は不明であるが、低年齢の参加者を除き、数字の多いスライドでも殆どが注視していた。令和元年は途中で挙手で尋ねた（スライド19、20)。中には参加者が少なく挙手がない場合もあった。遠慮もあったと思われる。多いとき、児童・生徒6人中の5人以上が挙手した。釣られての挙手はないように思われた。

授業では令和元年夏に1年生の情報基礎Iで10分程度に縮めて提示した。映画のテレビ放映が夏にあることを知り、暗号の話題の先取りとして扱った（使用検定教科書にRSA暗号の説明はない)。最後に唐突に確認用のスライドなしで面白い性質とキモ

の理解を尋ねて、多いクラスで半数程度が挙手した。挙手を遠慮した学生もいた。現在、専攻科の担当科目も含め、事前提示課題を伴う活用を模索中である。

## 5　おわりに

暗号技術のひとつであるRSA暗号の原理を23分程度でデモンストレーションする例を報告した。

余り計算が暗号として使用できる RSA 暗号のアイデアを小学4年生以上の多くの参加者が理解する。

今後、一層の時間短縮や、参加部分の創出や、理解に繋がる確認の方法やタイミングも検討したい。

本稿は 2019 年電子情報通信学会総合大会における発表[10]をもとにまとめたものである。

## 謝辞

本校おもしろ科学フェスティバル等において支援頂いた方々や、工夫もしつつ小中学生等来場者に事前準備の上終日一生懸命にデモンストレーション等を行ったボランティアの支援学生各位に感謝します。

## 参考文献

1)中村博文: 誤り訂正技術のしくみのデモンストレーション例, ―小学校の剰余計算の学習のみを前提とするリード・ソロモン符号の変形例―, 都城高専研究報告, 第 52 号, pp.69-80, 2018

2)R. L. Rivest, A. Shamir, L. Adelman: A Method for Obtaining Digital Signature and Public-key Cryptsystems, MIT-LCS-TM-082(MIT Laboratory for Computer Science), 1977

3)いぶき: 映画サマーウォーズの暗号を京大生が解いてみた結果, https://reistenza.com/entame/summer-wars.html

4)HKNEET: 【本気で考えてみた】サマーウォーズのパスワードの暗号の解き方 2056 桁の暗号は解けるのか?, http://win32programmer.seesaa.net/article/421790350.html

5)まいとう情報通信研究会: サルにも分かるRSA暗号, http://www.maitou.gr.jp/rsa/rsa10.php（以上3 件の参照は 2017/12)

6)M. Gardner: A new kind of cipher that would take millions of years to break, Mathematical Games, Scientific American, 237(2), 120-124, 1977

7)D. Atkins, M. Graff, A. K. Lenstra, P. Leyland: The magic words are squeamish ossifrage, Procs. of Asiacrypt '94, pp.263-277, 1994

8)岩井恭著, 原作細田守: サマーウォーズ, 角川書店, 2009

9)アニメスタイル編集部編: サマーウォーズ絵コンテ細田守, スタイル, 2009

10)中村博文: RSA暗号の小学4年生から大人までへの実演例 ―都城高専おもしろ科学フェスティバルにおいて―, 2019 年電子情報通信学会総合大会基礎・境界/NOLTA 講演論文集, A-2-1, p.21, 2019

## 付録

デモンストレーションで用いるスライド等の例を付図1に、その提示の際のシナリオ例を含むイベント出展での進行例を付表1に、配布資料の例を付図2に示す。

本報告では、説明の便宜上、スライド等に一貫した番号を付けているが、協力学生に配布しているシナリオ例においては、スライドは順に並んでいるという前提だけにして、通し番号は掲載していない。それは、シナリオ例配布後から当日までの判断でスライドの追加削除や移動があると無用になるためである。また、次の実施に向けた改善のための修正において、番号の対比の取り直しが必要なくなる。

進行例には、打ち合わせ等の際の記載箇所の特定の容易さから、項番ではなく行番号を付記している。協力学生への配布の際は、1 段組で空行を増やしている。それには、必要な設営に関する事柄も含めている。

おもしろ科学フェスティバルでは予め全出展のあらまし（Web ページではテーマ詳細と称している。出展毎に1ページである。本稿の出展において、内容は、付図2で示した配布資料例から QR コードを除いた内容と殆ど同じである。）を本校の Web ページで公開している。この行事においては、小学生向けに使用漢字に配慮することになっている。本稿の出展に関するものは、小学4年生以上で習う漢字をルビ付き若しくはひらがな表記としている（筆者はオレンジ工房“小学校で習う漢字チェックツール”http://orange-factory.com/tool/kanjicheck.html で確認した）。

参加者への配布資料は、準備の都合から、これまでのところはモノクロである。おもしろ科学フェスティバル終了後でもスライドや配布資料のカラー版（付図2はその例を93%に縮小したものである）を見て頂き易いよう Web 上に掲載し、配布資料にはその QR コードを印刷している。

1

あま　けいさん　わ
余　り　計算　で 分かる

えいが　　あんごう
映画『サマーウォーズ』の 暗号

2

The magic words are squeamish ossifrage …

オズの かんりセンターの にんしょうパスワード

3

あまり せいしつ あんごうへ クイズ かいどく えいがで おまけ

4

あまり せいしつ あんごうへ クイズ かいどく えいがで おまけ

６４÷３３ ＝ １ あまり ３１

１６÷３３ ＝ ０ あまり １６

６４÷３３⇒３１

5

あまり せいしつ あんごうへ クイズ かいどく えいがで おまけ

２÷３３⇒２
２×２÷３３⇒４
２×２×２÷３３⇒８
２×２×２×２÷３３⇒１６
２×２×２×２×２÷３３⇒３２
２×２×２×２×２×２÷３３⇒３１
２×２×２×２×２×２×２÷３３⇒２９
２を ７つかけて÷３３⇒２９

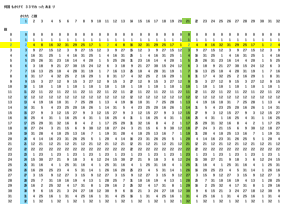
6

あまり せいしつ あんごうへ クイズ かいどく えいがで おまけ

２を　８つ かけて÷３３⇒２５
２を　９つ かけて÷３３⇒１７
２を１０こ かけて÷３３⇒　１
２を１１こ かけて÷３３⇒　２
２を１２こ かけて÷３３⇒　４
　　：
２を２１こ かけて÷３３⇒　２

7

あまり せいしつ あんごうへ クイズ かいどく えいがで おまけ



8

あまり せいしつ あんごうへ クイズ かいどく えいがで おまけ

２１こ かけると
2x2x2x2x2x2x2x2x2x2x2x2x2x2x2x2x2x2x2÷３３⇒2
8 × 8 × 8 × 8 × 8 × 8 × 8 × 8 ÷３３⇒2

３つ かけた８は、さらに７つ かければ元の２にもどる
**８があるとき、７を知っている人だけが元にもどせる**
アールエスエー
ＲＳＡあんごう　（ ⇔ ３３が、２つの数をかけた数）

9

あまり せいしつ あんごうへ クイズ かいどく えいがで おまけ

| |
|---|
| 2 |
| こ数３ |
| ÷33 |
| ⇒ 8 |
| こ数７ |
| ÷33 |
| ⇒ 2 |

アール エス エー あん ごう
Ｒ　Ｓ　Ａ　暗　号

10

あまり せいしつ あんごうへ クイズ かいどく えいがで おまけ

マーチン・ガードナー

１９７７年
サイエンティフィック アメリカン

（参考:日本語版の「日経サイエンス」の最近のものは本校図書館にも所蔵あり。）

11

あまり せいしつ あんごうへ クイズ かいどく えいがで おまけ

| | |
|---|---|
| 2 | ？　（空白→00、A→01、B→02、C→03、…、Z→26） |
| こ数３ | 9007 |
| ÷33 | 1143816257578888676692357799761466120102182967212423625625618429357<br>0693524573389783059712356395870505898907514759929002687954354 1 |
| ⇒ 8 | 9686961375462206147714092225435588290575999112457431987469512093081<br>6298225145708356931476622883986280133919905518299451578154 |
| こ数７ | ？ |
| ÷33 | 1143816257578888676692357799761466120102182967212423625625618429357<br>0693524573389783059712356395870505898907514759929002687954354 1 |
| ⇒ 2 | ？ |

12

あまり せいしつ あんごうへ クイズ かいどく えいがで おまけ

| |
|---|
| ？ |
| こ数３ |
| ÷33 |
| ⇒ 8 |
| こ数？ |
| ÷33 |
| ⇒ ？ |

⇒　もし ３３が ３×11 だとわかると
３と３と11で あるほうほうをつかって、
（かくちょうユークリッドのごじょほう）
すぐ７が計算でき、かい読

13

```
display2d: false:

e: 3 $
p: 3 $
q: 11 $

C: 8 $

yu(a1, a2):=block([a3],
  while 0<a2[3] do ( a3:a1-quotient(a1[3], a2[3])*a2, a1:a2, a2:a3 ),  a1[2]) $
d:yu([1, 0, (p-1)*(q-1)], [0, 1, e]) $
while 0>d do d:d+(p-1)*(q-1) $ "Kaisuu " : d :

ka(a,b,n):=block([r:1, m],
  while 1<=b do block( [b,m]:divide(b, 2),
    if m=1 then r:mod(r*a,n),  a:mod(a^2, n)  ),  r) $
"Kaidoku Kekka" :ka(C, d, p*q) :

(%o1) false
(%o9) "Kaisuu "
(%o10) 7

(%o12) "Kaidoku Kekka"
(%o13) 2
```

14

あまり せいしつ あんごうへ クイズ かいどく えいがで おまけ

アトキンスらが、ネット上でよびかけて、
1143816257578888676692357799761466120102182967212423625625618429357
0693524573389783059712356395870505898907514759929002687954354 1
のもとになった２つの数
3490529510847650949147849619903898134147764638493387843990820577
と
3276913299326670954996198819083446141317764629679929425397982885 33
をもとめた。
（おおよそ20か国、600人、1600台のｺﾝﾋﾟｭｰﾀ、８か月）
9007とこれらをつかって、かい読。1994年にはっぴょう。

15

```
e: 9007 $
p: 3490529510847650949147849619903898134147764638493387843990820577 $
q: 3276913299326670954996198819083446141317764629679929425397982885 33 $

C:9686961375462206147714092225435588290575999112457431987469512093081629822514570835
6931476622883989628013391990551829945157815154 $

yu(a1, a2):=block([a3],
  while 0<a2[3] do ( a3:a1-quotient(a1[3], a2[3])*a2, a1:a2, a2:a3 ),  a1[2]) $
d:yu([1, 0, (p-1)*(q-1)], [0, 1, e]) $
while 0>d do d:d+(p-1)*(q-1) $ "Kaisuu " : d :

ka(a,b,n):=block([r:1, m],
  while 1<=b do block( [b,m]:divide(b, 2),
    if m=1 then r:mod(r*a,n),  a:mod(a^2, n)  ),  r) $
"Kaidoku Kekka" :ka(C, d, p*q) :

(%o21) "Kaisuu "
(%o22) 1066986143685780244428687713289201547807099066339378628012262244966310631259117744708733401685974623065539685445132771090536060 95

(%o24) "Kaidoku Kekka"
(%o25) 2008050013010709030023151804190001180500191721050113091908001519190906180107 05
参考　富岳(ふがく)は、日本のコンピュータで、現在世界最速。
```

16

あまり せいしつ あんごうへ クイズ かいどく えいがで おまけ

| | |
|---|---|
| 2 | ？　（空白→00、A→01、B→02、C→03、…、Z→26） |
| こ数３ | 9007 |
| ÷33 | 1143816257578888676692357799761466120102182967212423625625618429357<br>0693524573389783059712356395870505898907514759929002687954354 1 |
| ⇒ 8 | 9686961375462206147714092225435588290575999112457431987469512093081<br>6298225145708356931476622883986280133919905518299451578154 |
| こ数７ | 1066986143685780244428687713289201547807099066339378628012262244966<br>3106312591177447087334016859746230655396854451327710905360609 5 |
| ÷33 | 1143816257578888676692357799761466120102182967212423625625618429357<br>0693524573389783059712356395870505898907514759929002687954354 1 |
| ⇒ 2 | 2008050013010709030023151804190001180500191721050113091908001519190906180107 05 |

17

あまり せいしつ あんごうへ クイズ かいどく えいがで おまけ

200805001301070903002315180419000118050019172105011309190800151919090618010705

もともと、クイズでは
空白→00、A→01、B→02、C→03、D→04、E→05、
F→06、G→07、H→08、I→09、J→10、K→11、L→12、
M→13、N→14、O→15、P→16、Q→17、R→18、S→19、
T→20、U→21、V→22、W→23、X→24、Y→25、Z→26、
ということだったので
20、08、05、00、…、05 は
⇒THE MAGIC WORDS ARE SQUEAMISH OSSIFRAGE

18

あまり せいしつ あんごうへ クイズ かいどく えいがで おまけ

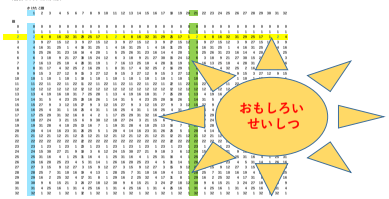
| | |
|---|---|
| 2 | ？ （空白→00、A→01、B→02、C→03、…、Z→26） |
| こ数 3 | 9007 |
| ÷33 | 114381625757888867669235779976146612010218296721242362562561842935709935245733897830597123563958705098989075147599290026879543541 |
| ⇒ 8 | 96869613754622061477140922254355882905759991124574319874095120930816298225145708356931476622883989623013391905518299451578151 54 |
| こ数 7 | ？ |
| ÷33 | 114381625757888867669235779976146612010218296721242362562561842935709693 |
| ⇒ 2 | ？ |

2056けた

The magic words are squeamish ossifrage …

19

あまり せいしつ あんごうへ クイズ かいどく えいがで おまけ




20

あまり せいしつ あんごうへ クイズ かいどく えいがで おまけ

キモ

２１こ かけると
2x2x2x2x2x2x2x2x2x2x2x2x2x2x2x2x2x2x2÷３３⇒2
８ × ８ × ８ × ８ × ８ × ８ × ８ × ８ ÷３３⇒2

３こ かけた８なら、７こ かければ元の２にもどる
**８があるとき、７を知っている人だけが元にもどせる**
アールエスエー
ＲＳＡあんごう

21

あまり せいしつ あんごうへ クイズ かいどく えいがで おまけ

えんざん
モジュロ演算 ： あまりをもとめる計算

年、月、日 ⇒ よう日

日～土 ≠ ０～６

２０２１、 １、 １ ⇒ ５（→金）

こうしき こうしき
（ ツェラーの 公式、 フェアフィールドの 公式 ）

22

あまり せいしつ あんごうへ クイズ かいどく えいがで おまけ

ショア
（ Ｓｈｏｒ ）

りょうし
（ 量子 コンピュータ ）

23

あまり せいしつ あんごうへ クイズ かいどく えいがで おまけ

！

24

あまり せいしつ あんごうへ クイズ かいどく えいがで おまけ

Ｓｈｏｒ

25

あまり せいしつ あんごうへ クイズ かいどく えいがで おまけ

2×2×2÷33

8×8×8×8
×8×8×8÷33

おくりて ひらぶん
送り手 平文 ⇒ あんごうか 暗号化 ⇒ あんごうぶん 暗号文 ⇒ ふくごう 復号 ⇒ ひらぶん うけとりて 平文 受け取り手
2 ↑3,33 8 ↑7,33 2
暗号鍵 復号鍵
あんごうかぎ ふくごうかぎ

26

あま けいさん わ えいが あんごう
余 り 計算 で 分かる映画『サマーウォーズ』の 暗号

じっさい あんごう アールエスエーあんごう
実際 の 暗号 （ＲＳＡ暗号）、

じっさい あんごう かいどく
実際 の 暗号 クイズ と 解読

27

あま けいさん わ
余 り 計算 で 分かる

えいが あんごう
映画『サマーウォーズ』の 暗号

28

参考文献

『サマーウォーズ』は
映画 細田守 原作・監督, サマーウォーズ製作委員会, 2009/8.
小説 岩井恭著, 細田守 原作, 角川書店, 2009/7.
絵コンテ アニメスタイル編集部編:サマーウォーズ絵コンテ細田守, スタイル, 2009/8.
他にも、小説やコミックスがある.
RSA暗号は
R.L. Rivest, A. Shamir, L. Adelman: "A Method for Obtaining Digital Signature and Public-key Cryptsystems, " MIT-LCS-TM-082, 1977.
暗号クイズは
Martin Gardner:"A new kind of cipher that would take millions of years to break," Mathematical Games, Scientific American, 237(2), 120-124, 1977.
アトキンスらの解読は
D.Atkins, M.Graff, A.K.Lenstra, P.Leyland:"THE MAGIC WORDS ARE SQUEAMISH OSSIFRAGE," Advances in Cryptology – ASIACRYPT '94.

29

参考文献

Webページは
いぶき:映画サマーウォーズの暗号を京大生が解いてみた結果,
https://reistenza.com/entame/summer-wars.html

HKNEET:【本気で考えてみた】サマーウォーズのパスワードの暗号の解き方2056桁の暗号は解けるのか?,
http://win32programmer.seesaa.net/article/421790350.html

まいとう情報通信研究会:サルにも分かるRSA 号,
http://www.maitou.gr.jp/rsa/rsa10.php
以上3 件の参照は2017/12
他にも、日本語で解説しているWebページは多数存在する。

付図1 スライド等の例 (2) その 17/29～29/29

付表1　出展等での進行例　(1) その1/5

※進行例（プレゼンのシナリオ例を含む）

留意事項
・余りの計算(小学３年で学習)が分かる４年生なら、わり算の余りの面白い性質と、ＲＳＡ暗号のキモと、映画との関連（わりと有名な暗号クイズと、その解読も）が分かること。
・入室した人は聞く気で来ている。導くつもりで。「難しいですね」などというやる気をそぐ言葉を絶対に安易に挟まないこと。
・プレゼンで、「暗号」と「解読」、途中から「ＲＳＡ暗号」も、という用語を使うが、これら以外の「積」、「剰余」、「素数」、「素因数分解」、「アルゴリズム」、「鍵」、「暗号化」、「復号」、その他の、用語は一切使わないこと。スライドや後述の進行例に含めたものだけは、例外的に用いる。
・参加者のために、０分か３０分丁度での開始、２３分以内のプレゼン、２５分以内で部屋の外まで、を厳守。
・参加者はネット上の記事や当日の配布物などを全く読んでいないという前提で、参加者が迷わないよう進める。
　例：多いなら教室外で整列、入室～着席、席へのプリント配布、プレゼン、退室アナウンス～教室外へ。
　整理券は使わない(以前は発行した)。入口（教室後ろや廊下）に３分前以降、来られている順に、席の分だけ入室を。
・この資料（及び、スライド等の資料）は書き込み可。当日終了後、要らなければ回収。今後の差し替え分も同様。
・サマーウォーズは、映画の他に小説複数とコミックス等がある。ＯＺ(オズ)の管理センターの認証パスワードの後部の具体的な文章と、その暗号文全体の具体的な数字と、Ｓｈｏｒの方法の記事を見ているシーンは、印刷媒体にもある。スライドでの提示は、文字情報に留め、出典を（配布資料等に）記して引用で済む範囲だけにする。
　　//画像は安易に使うと集中の妨げになるため用いない。

・予め、各回のプレゼン役と案内役を決めておくことにする（表を用意するので、それに記入）。
・小学４年生が、余りのおもしろい性質と、ＲＳＡ暗号のキモを、理解するという趣旨が変わらなければ、細かい表現や細かい例示はアドリブで変えて構わない。
　但し、下記の進行例の、順序だった説明の互いの関連性や、小学４年生以上が対象だということを忘れないように。
・勝手に内容を省かないこと。文を抜かないこと。省略は、思考が繋がらなくなるので不可。言い換えは可。
　　(過去にはそういう大小の失敗例があった。)
・無理しなくてよいが、小さいながらも、いくつか山場や笑いを取ってもよい所がある。または、作れる。
・以下で指示した以外にも、間を入れるとよい。間は大事。但し、退室開始まで２３分以内を厳守。
・以下は、基本的な流れである。頭に入れば見なくても良いし、抜けるよりは、読みながらの方がよい。
・以下で、■はスライド進行（切り替え）、◆はアニメーション機能でのスライド内進行、●は別ソフト操作、★は各自が考えて適宜行動。( ) は追加指示。丸かっこは、重要ではない、という意味ではないので、注意。
スライドは、例えばエンターキーで次ページへ。動きを出す機能は、不注意や環境によるコマ飛びの懸念から、使わない。
：☜：はマウス（または、レーザポインタ）での指示。これが無い所でも、参加者はほぼスクリーンしか見ていないので、マウスポインタ（または、レーザポインタ）の活用は必須。その際、操作が速すぎると、伝わらないので注意。
「//」の右側はメモなので、読まないこと。不用意に話題に混ぜると時間オーバーになる。
・全体の所要時間の不確定度が特に高くなるのは、入退室、操作ミス、そしてアドリブ部分である。

以下、３０分毎（計１０回）の１回分の内容。

（ここから。始まりの５分前位に、前の担当者と交代。）
（始まる前、適宜案内：前側から詰めてください。）
（案内役（余裕があればプレゼン役やフリーな人も手伝う。）が、着席を促しながら、各席にもれなく、プリントを裏返しで置く。配布中に参加者が手を出されたときは、手渡しする。参加者が読んでもとがめない。白紙等は取り替える。）
（プレゼン役は、ＰＣ画面がスクリーンに表示されていることを確認。wxMaxima が起動中であることと、テキストエディタでプログラムを開いていることも確認。wxMaxima に前の回でのプログラムが残っていたら、エンターキーを２０回位押して画面を流しておく。毎回新規画面でも可。）
（参考：テキストエディタから最初のプログラムを切り貼りするとき、前回のプログラムが見えない方が良いので、文字サイズや空行挿入等で調整しておく方が良い。）

■１　（プレゼン役がスライド１ページ目を表示。）
（プレゼン役は、ｐｐｔのスライド表示が最初のページであることを確認。違ったら最初のページにする。出展中でないなどと勘違いされないよう表示しておく。）
　　//開始直後前方に注目が行くようタイトルのみ表示。
（３０分毎の開始時刻までには、着席を終えているようにする。教室の内外で適切に入室や着席の案内を。）

（０分と３０分に開始するために。）
（プレゼン役は、原則、時間通りに開始。万が一、大勢の入室が遅れている場合でも１分以上遅らせない。でないと、時間が決まっている別の予約がある人に迷惑。必要なら、途中で、おまけの３つ目を飛ばして時間調整。）
（案内役は、開始時間直前に、適宜、教室前後のドアを閉める。遅刻者へは、次の回に来れない事情があるか尋ね、待てないときは、空き席、または立ち見の、場所を案内する。着席または移動を見届ける。）

★適宜挨拶（皆さん、こんにちは。）★この辺りで、学科や学年や名前等の一部を名乗るかどうかは任意。
これから、外に出るまで、２５分くらい、時間を頂きます。
席にプリントを配っていますが、今は裏返しにしていてください。
では、始めます。
　　//ターゲットをひとり程度決めて、その子供には分かってもらうつもりで話すのもよい。でも、他の人から嫉妬されないように。
■２　（このスライドは、雰囲気のためのもので、中身の直接の解説を今はしない。）
『**暗号**』というのは、ほかの人に分からないように、データを作り変えることです。
そして、それをあばくことを、『暗号解読』とか『**解読**』といいます。
ここでは、短く、『解読』ということにします。
映画とか小説などの『サマーウォーズ』では、暗号や、解読のシーンが、当たり前に出てきます。
★必須ではないが、時間的余裕が確かなら映画を観た人がどれ程いるか、挙手で尋ねてもよい。
（必須ではないが、次の３項目は、指を伸ばしながら数えるようにするしぐさを交えるのも一手。）
サマーウォーズは空想の話ですが、シーンのいくつかには、『実際の暗号』や、『わりと有名な暗号クイズ』や、『その解読』と関連している所があります。
今日は、この三つを、確かめます。

付表1　出展等での進行例　(2) その2/5

//「自分で調べたい方は、これからの話を聴いてはいけません。」というのは、言わないでよい。省略。
暗号以外では、ネタバレがないようにします。（うまく言って笑ってもらってもいい所ではある。）
用語を、ほとんど使わずに進めますが、暗号の基本は、押さえるつもりです。
わり算の余りを習っていれば、分かりますので、頭フル回転で、しっかりついてきてください。
大人の方(かた)も、ぜひ一緒に聴いてください。
//お子さんと後で話されるために。とか、油断すると大人でも分からなくなります。も省いてよい。
★このあとは、小学生の方(かた)向けの言葉遣いで話します。目上の方(かた)は、ご了承ください。
ここからは、前のスクリーンを見ながら聴いてください。
■3　この順番で進めます。
余り：☜：、余りのおもしろい性質、余りの暗号への応用、科学雑誌の暗号クイズと解読、サマーウォーズでの扱い、おまけ、です。
//あまり せいしつ あんごうへ クイズ かいどく えいがで　おまけ　　共通見出し行をずっと表示
『サマーウォーズ』に出てくる暗号は、割り算の余りのおもしろい性質を使っています。
ここで、割り算の授業はしませんが、軽一く、おさらいをしておきます。
（以下では、「2の3乗」や「2を3回かける」(←×算は2個）ではなく、「2を3個かける」のように言うこと。）
■4　例えば、６４÷３３なら、３３がひとつと、引いて、余りが３１です。
１６÷３３なら、余りは１６です。
このあとは、余りだけ注目します。
ですので、矢印を使って、この：☜：ように余りだけを書く場合があります。
今度は、2を、どんどん繰り返しかけてみます。
■5　どんどんかけながら、３３で割った余りを次々と書くと、こんな風になります。
★計算はやってあります。★それを使います。★３３で割った余りだけ注目します。
2だけなら余りは2、2×2は4で、割った余りは4、2が3つなら8で、余りは8という具合です。
2が6個なら６４で、余りは、さっきのスライドと同じで、３１です。
2が7個のときは、計算してあります。２９です。
このあとは、かける個数で表します。
//かけ算記号ではなくて、数字の個数に注目します。
すると、こんな、：☜：風に、短く書けます。2を7つかけて３３で割った余りは２９、という具合です。
//かけて、３３で割ることを、…
もっと続けます。
■6　こんな具合です。8つかけた２５６での余りは、２５です。
ずっと続けることができます。３３で割った余りですので、余りは0から３２までの３３通りしかなくて、2を何度もかけていくと、いつかは必ず繰り返しになります。
例えば、2を１１個かけたら２０４８で、余りを計算すると2です、２１個かけても余りが2です。
//こんな風に繰り返しになります。
2だけではなくて、ほかの数でも、何度もかけるのをやってみました。次のスライドで見せます。
先に言っておきますが、ひとつの表にまとめましたので、データが沢山あります。
今日の話だけでなくて、かずが増えたり、数(すう)が大きくなっただけで、難しいという人がいますが、
でも、本当は難しさは変わっていないということを、皆さんは見抜いてください。（←省略不可。）
では…。
//次のスライドは、コントロールキーとスクロールボタン等で、適宜拡大縮小をしてもよい。
■7　この表は、ひとつ一つ、きまじめに計算した結果です。
（これを見た人が量でびっくりするプレゼンはダメ。）
さっきの、『2』をかけていったのが、この表では、黄色の行です。
1つ：☜：で2、2つ：☜：で4、ずっと行って、１１個：☜：で元のと同じ2、２１個：☜：でも同じ2でしたね。
１１個の所：☜：から後ろは、繰り返しになっています。
今日は、『２１個かけた余り』に注目します。緑の列です。
もしも、かける回数が1回でも違うと、殆どが、元に戻りません。
例えば、2：☜：を２０個なら１：☜：ですし、２２個なら４：☜：です。2にはなりません。
ほかにも、例えば、3：☜：を２１個かけて３３で割った余りは3：☜：になっています。
４：☜：なら４：☜：になっています。
ひとことで言うと、この列：☜：と緑の列：☜：が同じですので、２１個かけると元と同じ数になると言えます。
★次行は単に読むだけでなく、決して必須ではないが、可能なら、セリフはドラマに似せて言ってみる。
『ガリレオ』というドラマのセリフで、『実に、おもしろい』というのがありますが、まさにそれです。
この**おもしろい性質**がサマーウォーズの暗号の種だということが、すぐ後で分かります。
//そのときには、今のが実におもしろい性質なんだということが改めて分かるはずです。
おさらいですが、かけ算した余りには、１１個とか、２１個という、かけ算の特別な回数のときには、元と同じ数になるという、おもしろい性質が確かにありますね。：☜：
//ここに後ろの内容理解の確認を持ってくるのも一手。
★少し間を置く。
2のかけ算で、もう少し続けます。
■8　２１という値は、3×7ですので、２１個かけるのは、3つ分ずつを、7つまとめても同じです。
3つ分かけたら8ですので、8を7つかけても、余りは元と同じ、2になっています。
★少し間を置く。
ここには書いていませんが、6つ分なら２５です。8つ分なら１６です。元の2には戻りません。
★少し間を置く。そして、ゆっくり言う。
言い換えると、7つ分ということを知らない人は、元の数には戻せないということが言えます。
//言っていることが分かりますか？//時間の余裕がないので念押しはし難いが、分からなさそうなら念押しを。
◆つまり、3つ分ということと8は誰に教えてもいいのですが、7つ分ということを知っている人だけが元に戻せるということなので、2を秘密にして送るための、暗号として使えるわけです。
★少し間を置く。
2だけではなくて、3でも4でも5でも、3つかけたのは、7を知る人だけが元に戻せます。
これが今日の**キモ**です。　//おもしろい性質も、キモも、個数はそれぞれ、全体でひとつだけにしている。
繰り返しますが、3つかけたデータは、7を知る人だけが元に戻せるというのが、今日の**キモ**です。
これはさっきのおもしろい性質の応用です。　//時間の余裕がないので念押しはし難いが、必要そうなら念補足を。
★少し間を置く。

付表1　出展等での進行例　(3)その3/5

７を知らなくても、数が小さいときは、かけ算を2回, 3回, 4回と順に試して、すぐに7つを試せますが、普通はとても大きな数にして、単純に試すだけなら世界中のコンピュータを使っても何百年とか、何億年とか、もっととか、かかるようにしています。
この暗号には名前がついています。(これは、いきなり感をなるべく出さないようにするための一言である。)
◆３人の発明者の頭文字をとって『**ＲＳＡ暗号**』です。
サマーウォーズにでてくる暗号は、実は、このＲＳＡ暗号です。理由は、後で分かります。
　　//そう言い切れる理由は、今日の話を最後まで聴いたら分かります。
★ところで、このようなうまいことができるのは、実は、３３が、３×１１のように、２つの数をかけた数だからなんです。このことは、今日は深入りしません。ご了承ください。
おさらいをしておきます。
■９　２を3つかけて、３３で割った８を送ります。
７というのを知っている人だけが、７つかけて余りを求めて、元の２に戻せます。
７つでなくて、近い回数の、８つでも、６つでも元の２には戻せません。
　　//ここに後ろの内容理解の確認を持ってくるのも一手。
このＲＳＡ暗号を使って、**暗号クイズ**が出されました。
■１０　サイエンティフィック・アメリカンという有名な一般向け科学雑誌で、マーチン・**ガードナー**という人が、１９７７年に出した、暗号クイズです。
　　//ＲＳＡ－１２９という言い方もされます。　//上記雑誌和訳本は日経サイエンス。近年のは本校図書館にも。
暗号を解いたら１００ドルもらえるという懸賞問題でした。当時の２万円くらいです。桁数が多いです。びっくりしないでください。(難解と思われないよう前もって言っておく。)
これです。
■１１　さっきの例も、左側に載せています。
位(くらい)が多いです。一行で書き切れないので2行で書いていますが、ひとつの数です。
ここ:☜:は１２９桁です。1万を３２回かけたくらいの数です。
左側に書いたさっきの例と比べると、これ:☜:やこれ:☜:が分かっていて、これ:☜:やこれ:☜:分からないわけです。
クイズが出たときは、解読に、千年くらいかかるとか、もっとかかるとか、言われていました。
　　//例えば、　４京年かかるとか、言われていました。
京は1万を4回かけた数です。
映画のサマーウォーズと違って、実際の解読は楽ではありません。でも、方向性はいくつか考えられています。
サマーウォーズで、健二君の解読方法の説明はありませんが、ひとつだけ、お話しします。
先ほどの例を使います。
■１２　まず、３３は、３と１１をかけたものです。
個数を表していたここ:☜:の3と、今の3と１１とで、ある方法、ここでは名前だけにしますが、『拡張ユークリッドの互除法』というものです、それを使うと、計算で、7が分かります。
今ここにあるパソコンで、計算してみます。
●１３　(テキストエディタのプログラムを表示して。)
３と3と１１というデータがここ:☜:です。　ここ:☜:は、説明は省きますが、コンピュータ・プログラムです。小学生がローマ字の練習をするよりも、字数はずっと少ないですね。　//プログラムは短く作ってある。不十分な所もある。これを読んでいるあなたは読解できるだろうか?
これをマクシマ(Maxima)というフリーソフトで、今から計算してみます。
　(切り貼りする。)　//手間だが計算を感じてもらうため。
●(wxMaxima の画面を表示して。)(wxMaxima での実行は、シフトキーを押しながらエンターキーを押すこと。)
この:☜:ように7が計算できました。ついでに、8を、7つかけた余りも計算していて、元の２が得られています。
(実行結果は、前の表示を流用ではなくて、その都度実行させないと臨場感がない。)
今のように計算できたので、『ＲＳＡ暗号は、暗号としてもうだめ』、かというと、そうではありません。
３３のように小さい数ですと簡単に3と１１をかけたと分かりますが、暗号クイズのように１００桁くらいとか、更に、サマーウォーズのように１０００桁以上とかに増やすと、かける前の２つの数を求めるのに必要な時間が、どんどん増えます。
速い方法を、人類はまだ見つけていません。
もし、ここにいる誰かが発明したら、きっと名前が残ります。でも、悪い奴から見て、この子は暗号やぶりに役立つと思われたら、誘拐されるかも知れません。(この辺りは、うまく笑いを取ってもよい所。)
　　//殆ど冗談です。が、可能性はゼロではありません。//今のは、ブラックユーモアです。　//半分だけ冗談です。
半分冗談です。(この辺りも、うまく笑いを取ってもよい所。)
さて、さっきのクイズは１２９桁でしたので、なかなか2つの数に分けられなかったのですが…。
■１４　**アトキンス**という人や仲間が、ネットで呼びかけて、大勢の協力をもらって成功しました。
★約２０か国の、約６００人の協力をもらって、
★約１６００台のコンピュータを使って、8か月かかったそうです。
１９９４年に結果が発表されています。
千年以上解読はできないという予想もありましたが、クイズが出されてから１７年で解読されました。
それでも、約１６００台のコンピュータで、8か月かけるまでは持ちこたえたわけです。
　　//★皆さんは、この解読にかかった期間を、短いと思いますか、長いと思いますか。　//少し間をとる。
サマーウォーズはＳＦですので、もっとけた数の多いのを、健二君が紙と鉛筆を使って一晩で解くシーンとか、鼻血をこぼしながら暗算で解くシーンもあります。(せりふも入れて、取れたら、笑いを取ってもよい所。)
でも、実際は、ＲＳＡ暗号の解読は簡単ではないので、今も世界中で使われています。買い物などでは当然ですが、最近は普通のホームページでも、何を見ているか、ほかから知られないようにするためにも、よく使われます。
さて、暗号クイズの、解読の続きです。
●１５　(テキストエディタのプログラムを表示して。)
暗号にするときにかける個数がここ:☜:、アトキンスたちが突き止めた、割る数のもとになっていた２つの数がこれ:☜:とこれ:☜:です。　プログラム:☜:はさっきと同じものです。　//「同じ」を強調したいが、さりげなくでよい。
(切り貼りする。)
●(wxMaxima の画面を表示して。)(wxMaxima の実行は、シフトキーを押しながらエンターキーを押すこと。)
もう終わりました。かける前の数が分かっていると、こんなに速いんです。
データを元に戻すためにかける個数が、ここ:☜:に求まっていますので、解読ができます。
これ:☜:を、ここの個数だけ:☜:かければいいわけです。
今ここで気付いた人がいるかも知れませんが、もしも、この個数だけ、本当に気まじめにかけ算するのを待っていると、みーんな、今日は家に帰れません。(面白くしてもよいし、

付表1　出展等での進行例　(4) その4/5

無理して笑いを取らなくてもよい。）　//富岳で頑張っても。
　　//太陽が燃え尽きるまで待っても、終わりません。
でも、うまい方法があって、今日は深入りしませんが、『バイナリ法』という方法で高速化しています。
それで計算して解読したデータが、これ：☜：です。
これを、さっきの表にまとめてみます。
■１６　解読して、これ：☜：が分かったわけです。　（着色してあるので、色を言うと分かりやすい。）
次に、この数：☜：の意味の取り方を説明します。
暗号クイズでは、もともと、数字が２つずつ：☜：、文字と対応させてありました。
ですので…。
■１７　さっきの：☜：を、ふた桁ずつで区切ると、こう：☜：なります。
最初の２０はT：☜：と対応します。次の０８はHと対応します。次の０５はE、次の００は空白です。
　　//最後の０５は、Eと対応していて、最後のここ：☜：のEです。
このような：☜：文字の並びが得られて、これで暗号クイズの解読が完了です。　　//パチパチ。
　　//メッセージは「魔法の言葉は squeamish ossifrage（気難しいヒゲワシ）」　//ossifrage（骨折り）
　　//最後の単語：☜：に、「骨の折れる仕事」の意味があるのを利用した、ジョークだそうです。
最後の単語が、お疲れ様のような意味があって、出題したガードナーからの解読者へのジョークだそうです。　//うまく笑いを取ってもよい。少し間を置いてもよい。
さて、肝心の、サマーウォーズで、どうだったかというと…。
■１８　このように：☜：読みやすいように小文字も使ってあって、更に文が追加されていました。これが、『オズの管理センターの認証パスワード』だったということでした。
それから、サマーウォーズでは、『２０５６桁の暗号』という言い方になっていました。
その中に、暗号クイズにあった、緑のこのあたり：☜：の数字は、大部分がそのまま使われています。
このことから、サマーウォーズに出てくる暗号はＲＳＡ暗号だろう、と推測できます。
　　//オズ（ＯＺ）//今度映画で確認してみてください。
　　//２０５６桁に何を含むかは実際は明確ではない？
　　//ここの緑の数：：：は、皆さんがあとで調べなくていいように、配布プリントに載せておきました。
★少し間を置く。
ちょっと、振り返りの質問をします。（聞き方はアレンジしても差し支えない。）　//そもそもだが、プレゼンの初めで、確認することを、何らか断っておくかどうかは任意。
（中村がいないとき、プレゼン役は、次の２問の挙手者数を記録。退室前までに全体人数や小３以下人数も記録。）
■１９　サマーウォーズの暗号は、２１個かけて３３で割った余りが、元に戻る、というような、余りのおもしろい性質を使っていました。余りにこのようなおもしろい性質があることは分かっている、という人は、手を挙げて知らせてください。
■２０　サマーウォーズの暗号のキモは、◆同じ数を３つかけた８という値は、更に７つかけることを知っている人だけが元に戻せるということでした。これが分かっている、という人は手を挙げて知らせてください。
（少し間をおいて）ありがとうございます。
サマーウォーズの暗号については、ここまでですが、この後、すこーしおまけを追加をします。

★ここで判断。もし例えば約１８分以上経過していたら、３つめのおまけとその説明は飛ばす。おまけの３つ目を飛ばしたからプレゼンがまずいということではないので、気にしないように。
（上記について補足：当日ではなくて事前に、３つ目のおまけ１枚にかかる時間を計っておいて、正確に何分以降なら、全体が２３分以内で終わらなくなり１枚スキップすべきか、時間把握をしておくことが望ましい。）

　　//（おまけの１つ目）
■２１　サマーウォーズでは、健二君が『モジュロ演算』という言葉を、１回だけ使います。
意味が分からなくても、映画を観るのに困りませんが、
モジュロ演算は、『余りを求める計算』という意味です。今日、何回も出てきた計算のことです。
サマーウォーズでは、西暦の年と月（つき）と日の数字から『曜日』を求める話が出てきます。
それは、暗号とは無関係です。でも、余りを使います。言わば、『余りつながり』の話題です。
　　//数を数えたときに、７で割った余りに注目すると、０～６の繰り返しです。
『日曜日から土曜日』を、順に数字の『０から６』で表すと、曜日が、数で扱えます。
年と月（つき）と日の数字から、正しく０～６が出てくるようにうまく調整した数式が、いくつかあります。
『ツェラーの公式』というのが有名です。
　　//本題の暗号の印象が薄まるので公式は表示しない。
　　//どちらも、割った答えの、１より小さい部分は捨てるようなわり算を何回か使います。
３０００より大きい数は出てきませんので、皆さんも、頑張れば、時間はかかっても、暗算でできます。
　　//サマーウォーズの健二君は、速かったですね。　//２１世紀だけならもっと簡単になります。
★飛ばして可：ちなみに、僕/私が初めて暗算したとき、自分の誕生日の曜日を求めるのに★秒かかりました。
　　//世の中には計算しないで曜日が分かる人が少しいますが、その話は、ここでは深入りしません。
これは、ここまでの紹介にしておきます。
　　//７で割った余りで曜日が決まります。//式解説は省く。　　//公式を使いMaximaか何かで参加者の年月日で計算してみせるのもとりあえず省く。個人情報保護をどうクリア？
　　//今日の日付で計算すると、ゼロで、日曜と分かります。

次のおまけです。
■２２　　//（おまけの２つ目）
ＲＳＡ暗号は、3や１１のようなかける前の元の数が、もし分かると、すぐ解読できる、ということを、さっき確認しました。
かける前の数を求めるに、『ミクロの世界』でだけできることを、利用した方法が、発明されています。
『ショア』という人の発明です。（ここでもできるだけいきなり感を減らすためこんな言い方をしている。）
　　//アルゴリズムというのは計算手順とか処理手順という意味です。//今はアプローチが量子ゲート型だけでない
　　//注意：ショアが発明したのは量子コンピュータではなくて、それを使った素因数分解アルゴリズム。
でも、その方法を使うには、特別なコンピュータが必要です。
今、覚えなくてもいいですが、『量子コンピュータ』：☜：といいます。
　　//最近は、ニュースになったりしています。
これ：☜：が、もしも実用化されると、ＲＳＡ暗号は使いものにならなくなります
でも…。

付表1　出展等での進行例　(5)その5/5

■２３　//可能ならよりおもしろいスライドを置きたい。安心してください。
なぜ安心かというと、世界中で研究していますが、とーっても難しくて、本格的な実用化はまだ先だ、と言われています。
　//ＲＳＡ暗号はコンピュータの処理速度の進歩に合わせて桁数を増やしていけば大丈夫と言われています。
　//量子コンピュータの扱える桁数は、２０２０/９　ＩＢＭ公表６５ビット；２０２３に１１２１ビット公表予定
■２４　映画では、誰かがショアの方法の記事を見ているシーンが、ちらっと、最初から最後までのどこかで、出てきます。このつづり：☜：も出てきます。まだ気が付いていない人は、今度映画を観るときに気を付けて探してみてください。
　//健二君は量子コンピュータではありませんが、そのようなシーンがあることも、映画の暗号はＲＳＡ暗号だろうとか、健二君は数をふたつに分ける計算をしたのだろうと、推測できる根拠です。
　//先のことですが、もしかしたら、今の小中学生や高校生の皆さんの子供の世代は、高校で、量子コンピュータについて教わるような時代になっているかもしれません。

（おまけの３つ目は、残り時間によっては、「配布物にあることですので」などと言って、飛ばしても可。）
★最後のおまけです。
　//（おまけの３つ目）
暗号について、いろいろ調べたい人も、いるかも知れません。でも、暗号関係の本やホームページは、基本的な用語でも、説明なしに使われていることが多いです。
特によく出てくる用語を、いくつか紹介したいと思います。すこーしだけ、お勉強をします。これから２分間くらいは、寝ててもいいです。（笑いを取っても良い所。）
　//高専の学生にもたまに寝ている人がいます。とかは言わない。失望する人がいてもいけないため。
後で見られるように配布プリントに書いてありますが、今は、パソコン画面を見ていてください。
　//ここまでで暗号のひとつであるＲＳＡ暗号のしくみが分かりましたので、それになぞらえて紹介します。
さっきの例になぞらえて紹介します。
■２５　まず、暗号を使う前の、もとのデータのことを『ひらぶん』：☜：といいます。専門家はこの字をひらぶんと読みます。今日の最初の例では『２』：☜：のことです。
それを分からなくしたデータを、『暗号文』：☜：といいます。今日の例では『８』：☜：のことです。
　//ひらぶんから、暗号文を作ることを…
暗号文を作ることを『暗号化』：☜：といいます。
暗号化はデータを作り変えているのですが、どう作り変えるかを指示するデータを、『暗号鍵』：☜：といいます。ちょっとカッコいい響きの言葉です。
今日の例では『３と３３』：☜：のことです。初めての人は、鍵という言い方が、少し変に聞こえるかもしれませんが、分からないように『封印するための鍵の役割』と思ったらいいです。
暗号文を元に戻すことを『復号』：☜：といいます。復号には『化ける』という漢字を付けないのが普通です。
復号もデータを作り変えているのですが、それを指示するデータを、『復号鍵』：☜：といいます。
今日の例では『７と３３』：☜：のことで、『封印を解くための鍵の役割』だと思ったらいいです。
復号鍵がばれると、暗号になりませんので、この復号鍵を、部外者には教えないようにします。
　//今日の例で復号鍵は７と３３のことですが、
３３：☜：は、暗号鍵：☜：にもありますので、ＲＳＡ暗号で、外に出さないのは、この７だけです。
復号をすると、元と同じひらぶんが得られます。今日の例では『２』：☜：のことです。

さて、今日(きょう)は…。
■２６　これらを確認しました。（時間がないので、原則、スライドの字を読みあげないこと。）
★以下の６行は、時間があるなら言う。ゆっくりと。
サマーウォーズに出てくる暗号は、今も使われているＲＳＡ暗号のようでした。映画で最初に出てくる解読結果には、科学雑誌の暗号クイズと同じ部分がありました。
ＲＳＡ暗号が、今も暗号として使える理由は、余りを求めるための３３のような数を大きくしたとき、かける前の３や１１のような数を求める速い方法が、まだないからでした。

パソコン画面はここまでです。
■２７　//最後の表示スライドはタイトルのみのもの。入退室後入ってきた次の人が、見てもよい内容である。
計算で機能を持たせる技術は沢山使われています。データを守る暗号以外では、例えば、印鑑やサインと同じことをデータだけでする技術や、２次元コードのように少しデータが消えても壊れても直す技術や、データの量を減らす技術や、電波や電気で一度に沢山のデータを送る技術です。
　//今日は、データを守る暗号技術について、一部だけ、お話ししました。）

机の上に配っているプリントには、もう少し、追加して書いてあります。家で読んでください。　//今読まないでという意味。
大人の方(かた)も、持って帰ってください。　（もし複数枚持って帰る人がいても、大目に見る。）
この部屋は、前からも、出られます。　//部屋によって適宜退室の際は、忘れ物がないようにお願いします。

以上で終わりです。
★適宜お礼（ありがとうございました。）
では、退室してください。
（プレゼン役は、教室前側のドアがあるなら開ける。）
（プレゼン役は、次のために、スライドを１ページ目にしておく。また、wxMaxima は、エンターキーを２０回位押して画面を流しておく。別画面を作ってもよい。）
（案内役は、後部入口のドアを開ける。混み合うとき、退室優先や、次のグループに待って頂くことや、入室のタイミングを、適宜アナウンス。）
（プレゼン役と案内役は、忘れ物が無いか、もし有ってもできるだけ早く発見してあげられるように留意。）
（プレゼン役、案内役とも、次の担当者に引きつぐ。）

その他
　ここからは中村用のメモ。読まなくてもよい。
　シナリオ例その他を予め読んでおくことを念押し。
　可能ならスライドを電子データで見られるように（または、Web 掲載）。
　この出展の協力者は昼食時以外に後学のために４０分程度離れられる時間を設けることを伝達（連続する１時間の始まりと終わり以外か、３０分の始まりと終わり以外を２回、但し、朝から２回目までは仮に非番でも抜けずに互いに他の学生の動きを見ておくこと）。
　当日の服装は任意（状況にもよる）。
　できるだけ事前に飲み物代プラスアルファ位までは。
　用意：ローテーション記入用の表、張り紙を全て。
　整理券を用いる場合には印刷して用意、整理用の箱も。

# 余り計算で分かる映画『サマーウォーズ』の暗号（実演）

所　属　一般科目
担当者　中村 博文、他

映画『サマーウォーズ』*1では、暗号や暗号解読（以下、解読）があたり前に出てきて、解説はありません。しかし、一部のシーンは、世界中で広く使われている実際の暗号*2や、実在の解読の公開問題*3や解読*4と関連しています*5～7。

今日は、**その暗号の原理**と、**解読の公開問題**や**解読**を、一緒に**確認**します。

**わり算のあまりの面白い性質**を使っています。**あまりが主役**です。

**対象**　あまりの計算ができる小学生 ～ 大人。

**所要時間**　２５分くらい。　毎時０分と３０分に開始（昼休み以外）。　自由席。

**実施人数**　２０人×１０回。同伴者を含む。各回で部屋の入り口への５分前の先着順。

**その他**　現代社会を人知れず支えている「計算を使って役立つ働きを持たせる**しかけ**」*8のひとつについて、今日、自分の頭で、その**ひらめきを追体験**してみませんか。

**aha!**

---

**発展**（もしよろしかったら、いろいろ調べて、もう少しきわめてみてください。自由研究になるかは提出先に確認を。）

・データを他の人に分からなくするために、うまく作り変えたデータにしてしまうという方法があります。それが**暗号**です。関連して、元のデータのことを**平文**（ひらぶん）、作り変えたデータを**暗号文**、暗号文を作ることを**暗号化**といいます。暗号文を作るとき、どのように作り変えるかを指示するデータを**暗号鍵**といいます。 暗号文を元のデータ（**平文**）にもどすことを**復号**といいます。元にもどすのも、一種の作り変えです。元にもどすために、どのように作り変えるかを指示するデータを**復号鍵**といいます。暗号鍵とペアになっている復号鍵を使わないと、元の平文にはもどりません。 広く使われるように暗号のしくみを公開する暗号を**現代暗号**と呼んでいます。現代暗号では、外部にもらさないのは復号鍵だけです。 暗号鍵も復号鍵も**数**で表します。守りたい情報も**数**に直して扱います。つまり、**現代暗号の正体は計算**です。

例　*送り手*　平文 2　⇒　暗号化（2×2×2÷33）　⇒　暗号文 8　⇒　復号（8×8×8×8×8×8×8÷33）　⇒　平文 2　*受け取り手*

（21 こかけて÷33 で元にもどるので）　暗号鍵 3, 33 ……> *盗聴者*　復号鍵 7, 33

・復号鍵を持たない人が、暗号文などから元の平文を導き出すことを、暗号解読とか**解読**といいます。

・鍵は数ですので、その可能性をすべて試せば解読できます。解読に十分長い時間がかかる暗号を**強い**暗号、反対を**弱い**暗号といいます。試し方の工夫や技術の進歩で、だれかが解読に成功すると、強い暗号ではなくなります。暗号は鍵のけた数をふやすと強さがますため、それで強さを保ち続けている暗号もあります。

・声のほか、途中の電波や光や電気の信号からデータを盗むことも、**盗聴**といいます。暗号で盗聴をふせぐことはできませんが、強い暗号を使えば、もし盗難や盗聴をされて解読を試されても、情報は守られます。

・今日とりあげるＲＳＡ暗号*2は、**かけた数**を鍵に使っていて、かける前の数がもし分かると、解読が速いことが知られていますが、かける前の数を求める特別速い方法はまだありません。量子コンピュータというのが強敵ですが、実用化は遠そうなため、まだＲＳＡ暗号は大丈夫で、世界中で使われています。

---

・発信元の確認にも、印鑑やサインの代わりにも使えます：
上の図の矢印を逆にすると、2⇐29⇐2。3つ かけて 元の 2 にもどる 29 を作れるのは、7を知る人だけなので。

・年長の方と調べてみては：色々な暗号と解読、素数、フェルマーの小定理、RSA暗号、素因数分解、拡張ユークリッドの互除法、RSA-129、計算量的安全性、RSA暗号解読コンテスト、公開鍵暗号、秘密鍵暗号、ハイブリッド暗号、https、ディジタル署名、ディジタル証明書、量子コンピュータ、量子ゲート型、Shorのアルゴリズム、ツェラーの公式。備考：**aha!** はマーチン・ガードナーの著書より。

*1 細田守 原作・監督.出版物は 岩井恭著 角川書店、蒔田陽平著 角川つばさ文庫、アニメスタイル編集部編:サマーウォーズ絵コンテ細田守 スタイルなど.
*2 R.L. Rivest, A. Shamir, L. Adelman: “A Method for Obtaining Digital Signature and Public-key Cryptsystems,” MIT-LCS-TM-082,1977.
*3 Martin Gardner:“A new kind of cipher that would take millions of years to break,” Mathematical Games, Scientific American, 237(2),120-124,1977.
かけた数 114381625757888867669235779976146612010218296721242362562561842935706935245733897830597123563958705058989075147599290026879543541
*4 D.Atkins, M.Graff, A.K.Lenstra, P.Leyland:“THE MAGIC WORDS ARE SQUEAMISH OSSIFRAGE,”Advances in Cryptology - ASIACRYPT ’94.
*5 いぶき: 映画サマーウォーズの暗号を京大生が解いてみた結果, https://reistenza.com/entame/summer-wars.html *6HKNEET:【本気で考えてみた】サマーウォーズのパスワードの暗号の解き方 2056 桁の暗号は解けるのか?,http://win32programmer.seesaa.net/article/421790350.html
*7 サルにも分かる RSA 暗号,http://www.maitou.gr.jp/rsa/rsa10.php
*8 情報を守る、データで印鑑やサインの代わり、データが少し壊れても直す(例:QR コード)、データの量を減らす、一度に沢山のデータを送るなど。

資料ＵＲＬ（一応年末まで）　このプリント→（カラー）　関連スライド→など

https://www.miyakonojo-nct.ac.jp/g21/sw-rsa-p-pdf.htm　https://www.miyakonojo-nct.ac.jp/g21/sw-rsa-s-pdf.htm

付図２　配布資料例