連載

情報の授業をしよう！

本コーナー「情報の授業をしよう！」は，小学校や中学校で情報活用能力を育む内容を授業で教えている先生や，高校で情報科を教えている先生が，「自分はこの内容はこういう風に教えている」というノウハウを紹介するものです．情報のさまざまな内容について，他人にどうやって分かってもらうか，という工夫やアイディアは，読者の皆様にもきっと役立つことと思います．そして「自分も教え方の工夫を紹介したい」と思われた場合は，こちらにご連絡ください．
（E-mail：editj@ipsj.or.jp）

鍵はなぜ2つあるのか
― RSA暗号の体験から学ぶ公開鍵暗号方式 ―

基般

伊藤大貴　大分県立日田高等学校

鍵を安全に渡せないという難問

生徒はWebサイトやメッセージサービスを日常的に使うが，暗号を「読めない文字列に変換する技術」と捉えがちである．公開鍵暗号方式は，鍵の生成，公開，暗号化，復号が別々の主体と段階に分かれるため，アルゴリズムだけを示しても，どの鍵が相手へ渡り，どの鍵が手元に残るのかは捉えにくい．ただし，教材を操作するだけで理解に至るとも限らない．手順どおりに進めば暗号文は得られるが，「ボタンを押したら読めない文字になった」で終われば，鍵の役割は説明できない．阿南（2014）[1]は，言語活動が論理的な理解を促す可能性を報告している．そこで本稿では，「手順のトレース」「体験」「言語化」を組み合わせた授業を報告する．

導入では，生徒が日常的に利用するメッセージサービスの構造を示し，送信した情報が端末から相手へ届くまでのどこで漏えいする可能性があるかを考えさせる．暗号化は，情報の漏えいそのものを完全に防ぐ技術ではなく，仮に通信内容を取得されても，その意味を読み取られにくくするための対策であることを押さえる．続いてシーザー暗号や上杉暗号を取り上げ，暗号化と復号に同じ鍵を用いる共通鍵暗号方式へつなぐ．ポケベルコードも文字を数値へ置き換える体験として扱うが，これは暗号ではなく符号化の例であることを明示する．

共通鍵暗号方式は，送受信者が同じ鍵を共有する方式である．処理は高速だが，通信前に鍵を安全に共有しなければならない．鍵を通信経路で送れば，盗み見た第三者も暗号文を復号できる．また，相手ごとに鍵を分ける場合，利用者が増えるほど管理する鍵の組合せも増える．図-1で「鍵配送の問題」を確認させ，公開鍵暗号方式なら何を変えられるのかを予想させた．

閉める鍵と開ける鍵を分ける

公開鍵暗号方式では，受信者が互いに対応する公開鍵と秘密鍵の組を生成する．受信者は公開鍵だけを外部へ公開し，秘密鍵は自分で保持する．送信者

は受信者の公開鍵で平文を暗号化し，受信者は対応する秘密鍵で暗号文を復号する．公開鍵は「誰でも使える閉める鍵」，秘密鍵は「受信者だけが持つ開ける鍵」とたとえると，2つの鍵の役割を捉えやすい．重要なのは，受信者が秘密鍵を送信者へ渡さなくても，送信者から暗号文を受け取れる点である．

ここで，「秘密鍵を使って公開鍵を作り，その公開鍵を送る」と説明すると，鍵生成と鍵の公開という別の操作が混同される．授業では，受信者が鍵の組を生成し，次に公開鍵だけを相手へ知らせる，という順に分けて表現する．また，公開鍵で暗号化し秘密鍵で復号する機密性の仕組みと，秘密鍵による署名と公開鍵による検証を扱うデジタル署名は，目的と処理の向きが異なる．本時は暗号化と復号に焦点を絞り，デジタル署名は次時に扱うこととした．

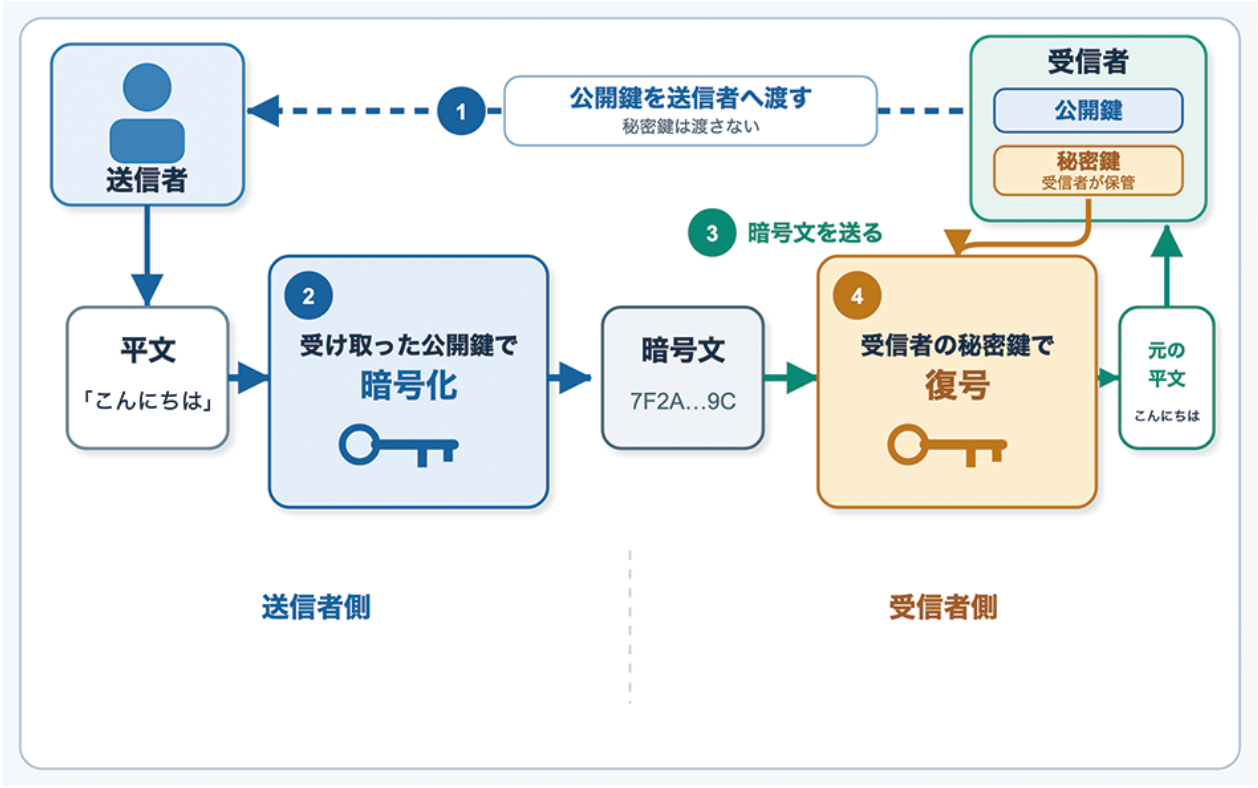
図-2を最初から教師が解説するのではなく，生徒に読ませ，想像させるようにした．送信者と受信者，公開鍵と秘密鍵，平文と暗号文の関係を自分でたどり，「共通鍵暗号方式より優れている点」を記述させた．読み取りが止まった生徒には，2色のペンを用意させ，一方を公開鍵，もう一方を秘密鍵として図中の流れをトレースさせた．トレースによって，どの鍵が移動し，どの鍵が受信者の手元に残るのかを可視化することがねらいである．



■図-1　共通鍵暗号方式で生じる鍵配送の問題

言語活動のための実践

実践は，大分県立日田高等学校普通科1年生を対象に，学習指導要領（文部科学省 2018）[2] の「情



■図-2　公開鍵暗号方式における暗号化・復号の流れ

報通信ネットワークとデータの活用」を 7 時間構成とし，その第 6 時として行った．中心となる研究授業は 2025 年 11 月 10 日に 35 名を対象として，情報科教員と国語科教員が担当した．目標は，公開鍵暗号方式の利点を理由とともに説明すること，手順の理解に基づいて RSA 暗号の鍵生成，暗号化，復号を体験することである．

単元は，ネットワーク通信とプロトコル，インターネットの仕組み，情報システム，データベース，情報セキュリティ，暗号化アルゴリズム，デジタル署名と振り返りの 7 時間で構成した．第 5 時までに，通信の経路や情報システムの中でデータがどこを流れるかを扱い，パスワードの重要性やコンピュータウイルスなどの脅威も確認している．本時では，通信の内容を守る仕組みとして暗号化を扱い，第 7 時のデジタル署名と TLS へつなぐ．

本校は SSH 指定校として，「探究する力」，「波及させる力」，「基盤となる力」の育成を学校全体の目標としている．2025 年 7 月の生徒授業アンケートでは，情報科において，「波及させる力」の下位項目である「発信する力」と「実践する力」に関する生徒の意識が低かった．Web アプリケーションの作成や話し合いの活動は取り入れていたが，作業の結果を自分の言葉で説明する場面は十分ではなかった．そこで本時では，操作の前後に説明を書く時間を設けた．

授業の流れは，大石（2017）[3] が公開鍵暗号方式の実践で示した，手順のトレース，言語活動，実践という順序を基にした．これに，個人で図を読み取る段階を最初に置き，実習後にもう一度説明を書く段階を加えた．表 -1 に本時の展開を示す．

■表 - 1　本時の展開

段階	時間	主な学習活動	教師の支援・確認点
導入	5 分	身近な通信で情報が漏えいし得る個所を考える	暗号化の意義を「漏えい後のリスク低減」として確認する
展開	40 分	古典暗号と共通鍵の課題を確認し，公開鍵暗号方式を読解・トレース・説明する．ペアで RSA を体験し，説明を再検討する	公開鍵と秘密鍵の所在，暗号化と復号の対応，操作の役割交替を確認する
整理	5 分	共通鍵と公開鍵を組み合わせる実社会の通信へ見通しを持つ	教材の単純化と，実運用の暗号との差を明示する

授業は，①個人で図を読み取る，②2 色のペンで手順をトレースする，③考えを言葉にして他者と確かめる，④ Web 教材で操作する，⑤体験を踏まえて説明を書き直す，という順で進めた．③の言語活動は全クラスで実習前に行った．操作前に予想を書かせ，実習では「どのボタンを押すか」ではなく，「図で読んだ鍵の役割が，実際の処理のどこに現れるか」を確かめさせた．

実習後の⑤では，最初の記述を消さず，別の欄に書き直させた．前後の記述を並べると，学習者自身が新たに加わった語や因果関係を見比べられる．さらに，グループで代表となる説明を選び，「誰がどの鍵を持つか」「どの鍵で暗号化・復号するか」「第三者が公開鍵を入手してもなぜただちに復号できないか」の観点から改善した．国語科教員には，結論だけでなく理由をつないで述べることや，主語と述語の対応を意識させる支援を依頼した．評価したのは技術用語の数ではなく，関係を筋道立てて説明できたかどうかである．

暗号化を体験する教材開発

easyRSA を開発した理由

RSA は，提案者である Rivest，Shamir，Adleman（1978）[4] の姓の頭文字である．RSA を数式から説明すると，生徒の注意は式変形や鍵の値に向き，「誰が鍵を生成するのか」「どの値を相手へ渡すのか」「何を残すのか」を見失いやすい．完成した模式図を読むだけでは，公開鍵だけが相手へ移動し，秘密鍵は受信者の端末に残るという非対称性も実感しにくい．そこで，鍵とデータの移動を役割の中で体験する Web 教材「easyRSA」を開発した [5]．

教材では，鍵生成，暗号化，復号を画面上で分けた．公開鍵には「相手に教える値」，秘密鍵には「絶対に秘密にする値」と表示し，生成した公開鍵と暗号文は，ペアで受け渡せるようにした．受信者，送信者，再び受信者という操作順を画面と活動に持たせ，計算結果を見るだけの実習にしなかった．

現在公開している GitHub Pages 版は，HTML，CSS，JavaScript と Bootstrap で構成した静的 Web アプリケーションである．暗号計算は端末のブラウザ内で行うため，専用ソフトウェアをインストールせずに利用できる．ソースコードも公開しており，授業者は動作や画面表示を確認した上で利用できる．実践でも，GitHub Pages で公開しているこの版を用いた．授業で使用した後も，画面表示と操作手順の改善を続けている．図 -3，図 -4，図 -5 には，2026 年 8 月 2 日現在の公開版を用い，同一の鍵とメッセージで再現した結果画面を示す．

小さな値でも手順は省略しない

鍵生成では，生徒が 2 つの素数 p，q を画面に用意した 2 から 97 までの素数から選ぶと，n＝pq と z＝(p－1)(q－1) を求め，z と互いに素となる公開指数 e を選ぶ．次に，補助変数 m について，zm を e で割った余りと，－1 を e で割った余りが一致する値を探し，d＝(mz＋1)/e として秘密指数 d を求める．これは $ed \equiv 1 \pmod{z}$ を小さな値で確かめるための教材の手順である．選んだ 2 つの素数が同じ場合や，文字を数値化するのに必要な大きさ (n≥143) を n が満たさない場合，公開指数 e が z を割り切れる場合，補助変数 m の条件を満たさない場合には，それぞれ理由を画面に示し，入力し直させる．どこを直せばよいかが分かるため，生徒は教師を待たずに選び直せる．誤った値のまま次の段階へ進むこともない．この下限は，後述するポケベルコードが 00 から 99 までの 2 桁の数値であり，暗号化する数値が n より小さくなければ復号できないことによる．最小の 2 桁の素数の積が 11 × 13＝143 であるため，2 桁の素数を 2 つ選べばこの条件を満たす．図 -3 では p＝61，q＝53 を選び，n＝3233 としている．補助変数との混同を避けるため，ここでは数値化した平文を x，暗号文を c とすると，暗号化は $c = x^e \bmod n$，復号は $x = c^d \bmod n$ として計算する．大きな整数を扱える JavaScript の BigInt と繰り返し二乗法を用い，画面が固まりにくい構成とした．

日本語の短いメッセージを扱うため，平文はポ



■図 -3　easyRSA の鍵生成結果画面



■図 -4　easyRSA の暗号化結果画面



■図 -5　easyRSA の復号結果画面

easyRSA（公開版）
鍵生成・暗号化・復号を
ブラウザ上で体験できます
QRコードを読み取る
https://itou-daiki.github.io/easy_RSA/

ケベルコードを用いて数値列へ変換する．ポケベルコードは，かつてポケットベルで文字を伝えるために用いられた 2 桁の数字であり，あ ＝11，い ＝12 のように，五十音表の行と段の組合せで決まる．たとえば「ねむい」は 54，73，12 となる．生徒にとってポケットベル自体はなじみがないが，表を見て文字を数字へ置き換える操作は理解しやすい．暗号化の前に，文字を数値へ変える段階があることを確認できる．濁点を含む文字は，基底となる文字と濁点に分けて処理し，復号後に文字列へ戻す．「が」であれば「か」と濁点に分け，21 と 04 として扱う．これにより，文字が数値へ変わり，その数値が暗号計算の対象になる過程を画面で追える．送信者は暗号文をコピーして受信者へ渡し，受信者は自分の秘密鍵で復号する．「暗号化ボタンを押したら読めない文字になった」という印象で終わらず，文字，数値，暗号文，復号後の文字という変化を追えるようにした．

ペアの情報移動を授業にする

ペアの一方を受信者，もう一方を送信者とし，次の手順で進める．

1. 受信者が小さな素数を選び公開鍵と秘密鍵を作る．
2. 受信者は公開鍵のみ送り，秘密鍵は送らない．
3. 送信者は短いメッセージを入力し，受信者の公開鍵で暗号化する．
4. 送信者は生成された暗号文を受信者へ渡す．
5. 受信者は自分の秘密鍵を用いて暗号文を復号する．
6. 役割を交替し，同じ流れをもう一度行う．

受信者が伝えた公開鍵は，送信者がプリントに書き取ってから入力させる．値を書き写す操作を挟むことで，「相手に教える値」と「手元に残す値」の区別を確認できる．単なる成功体験で終わらせないため，各段階で「いま誰の端末を操作しているか」「相手へ渡してよい値は何か」「この処理は図 -2 のどこに当たるか」を確認する．役割を交替することで，1 人の生徒が送信者と受信者の両方を経験できる．秘密鍵に当たる値をペアへ見せないという制約そのものが，仕組みを理解するための活動になる．

学習用と実用を混同しない

easyRSA は，小さな素数と単純な文字―数値変換を用いた学習用のモデルであり，実用上安全な暗号ではない．ポケベルコードも暗号ではなく，文字を数値へ置き換える符号化である．実際の RSA では十分に大きな鍵と適切な符号化・パディングが必要であり（Moriarty et al. 2016）[6]，通信全体を RSA だけで暗号化するわけでもない．たとえば実際の通信では，公開鍵暗号方式を共通鍵の安全な共有などに用い，その後のデータ暗号化には高速な共通鍵暗号方式を用いる構成が一般的である．授業用教材と実社会の技術の境界を明示することは，「画面で暗号化できたから安全である」という誤解を防ぐ上で欠かせない．

体験後の言葉に何が現れたか

記述の評価では，単に「公開鍵暗号方式は安全である」と結論を書けたかではなく，安全性を支える関係を説明できたかを見た．A 評価は，受信者だけが秘密鍵を保持すること，公開鍵で暗号化し秘密鍵で復号すること，そのため秘密鍵を共有せずに通信できることなどを根拠として結び付けた記述である．B 評価は利点に触れているが，誰がどの鍵を持つか，または安全である理由の一部が曖昧な記述，C 評価は利点を説明できていない記述とした．

たとえば A 評価には，「復号できるのが受信者だけになる．秘密鍵を共有しない限り，第三者に情報が伝わることがない」との記述があった．一方，「送信者側と受信者側でそれぞれ公開鍵と秘密鍵があるため，途中で鍵を取られる心配が減る」という記述は，安全性に言及しているものの，鍵の所有者と暗号化・復号の対応が明確ではない．この記述には，教師が「公開鍵と秘密鍵を作るのは誰か」「送る鍵と送らない鍵はどちらか」と問い返す．そうすると，説明を具体化できる．なお，掲載した記述例は匿名化し，表記上の明らかな誤りのみ整えた．

研究授業を行った学級の記述について，語の共起ネットワークを作成した．A 評価では「鍵」を中

心に「秘密」「公開」「送信」「受信」が結び付いていた．B 評価では語のまとまりが 4 つに分かれ，安全である理由に至る前に説明が途切れていた．記述の評価と語の結び付き方が対応していたため，以後は「誰が」「どの鍵で」「何をするか」が一文でつながっているかを確認することとした．

実習後にもう一度書く活動の意味を検討するため，授業条件がそろわない 1 学級を除き，4 学級の記述を比較した．すべての学級で実習前に言語活動を行った上で，2 学級は「言語活動→実習→追加の言語活動」，別の 2 学級は「言語活動→実習」で授業を終えた．各条件の分析対象を 69 名にそろえ，記述評価を表 -2 に示す．

A 評価は，実習後にも言語活動を行った条件で 14.5 ポイント高かった．概念の被覆数，説明構造，復号への言及も同じ傾向を示した．本実践では，実習後の言語活動によって概念理解が向上したと捉えている．ただし，既存授業を用いた探索的な比較であり，個人を無作為に条件へ割り付けていない．学級間の差もあり，多重比較後には明確な差を確認できなかった．これらは本実践の範囲での課題であり，今後は事前理解と記述条件をそろえた検証が必要である．

体験後に再び言語活動へ戻る時間は，公開鍵と秘密鍵の役割を整理し，説明の因果関係を組み直す機会になったと考える．一方，実習前の読解・トレース・対話だけでも説明へ到達した生徒がいた．

小さな数の教材を実社会へつなぐ

ほかの授業で本実践を用いるなら，まず RSA の数式ではなく，「同じ鍵を安全に共有できない」という問題から始めたい．公開鍵暗号方式を，覚えるべき別方式ではなく，鍵配送の問題への工夫として捉えやすくなる．実習前には説明を書かせる．予想を言葉にしておくと，操作が自分の考えを確かめる行為になる．実習では送信者と受信者を交替させ，秘密鍵を相手へ渡さないという制約を守らせる．実習後は別の欄に説明を書き直し，自分の言葉の変化を残す．

授業時間が限られる場合も，鍵配送の問題，ペアでの情報移動，実習後の書き直しは省かない．古典暗号の復習や RSA の計算過程は別時に回し，本時では鍵の役割を説明する活動に時間を確保する．

操作につまずいた生徒には，公開鍵，秘密鍵，平文，暗号文を同じ位置に置いた手順図を用意し，教材画面の各段階と対応させた．鍵生成ができない場合や，暗号文を写し間違えた場合に，どの段階へ戻るかも示しておく．ただし，教員が手順を最初にすべて説明すると，生徒が図を読み，関係を解釈する余地がなくなる．最初は個人で読ませ，必要に応じて 2 色ペン，ペアでの確認，手順図の順に支援した．

研究授業後の協議では，読解に用いた図が分かりにくく，図を選び直す必要があること，実習は知識・技能の評価に当たるため，手順を理解した段階と実践できた段階を分けた規準が必要なことを指摘された．指導案では，手順の理解にもとづいて RSA 暗号の通信を実践できたかを「知識・技能」，論理的な理解にもとづいて利点を説明できたかを「思考・判断・表現」の規準とし，操作の成否だけでは評価しないこととした．協議では，操作につまずいた生徒への手順の押さえと，説明を別の欄へ書き直させる工夫も課題として挙がった．本稿で述べた手順図と書き直しの欄は，この指摘を踏まえて整えたものである．

本時では全員が復号まで到達したため，操作の成否からは理解の差を読み取れない．そこで，「誰がどの鍵を持つか」「どの鍵で暗号化・復号するか」「なぜ安全といえるか」の 3 つが説明に含まれるかを確認した．本稿の記述評価も，この 3 つの観点による．

また，授業で扱う秘密は教材上の値に限定し，実在するパスワードや個人情報を入力させない．公開鍵暗号方式は，「公開鍵なら真正性も自動的に保証

■表 - 2　実習後の追加言語活動の有無と記述評価

評価	実習後にも言語活動あり（n=69）	実習後の言語活動なし（n=69）
A	29 名（42.0%）	19 名（27.5%）
B	36 名（52.2%）	45 名（65.2%）
C	4 名（5.8%）	5 名（7.2%）

される」と誤解されることもある．公開鍵が本当に意図した相手のものかを確かめる仕組みや，デジタル証明書，TLS については次時へつなぎ，暗号化，認証，署名を区別して学ばせる．小さな数の RSA 体験を，現実の安全性を過度に単純化する終着点ではなく，実社会の仕組みを問う入口にする．

実習を言葉でつなぎ直す

「鍵はなぜ 2 つあるのか」という問いへの答えは，単に「公開鍵と秘密鍵があるから」ではない．誰にでも渡せる暗号化のための鍵と，受信者だけが保持する復号のための鍵に役割を分けることで，秘密鍵そのものを相手へ渡さずに暗号文を受け取れるからである．この関係は，図を見ただけでも，画面を操作しただけでも十分に理解できるとは限らない．

この見取りには，国語科教員との協働が役立った．情報科の教員は，用語が正しく使われていれば説明として読み取りやすい．一方，国語科の視点からは，理由と結論が接続しているか，主語と述語が対応しているかが問われる．「受信者だけが秘密鍵を持つ」と「だから第三者は復号できない」が一文でつながったとき，2 つの鍵は別々の用語ではなく，一組の関係として説明されている．

個人で読み，手順をトレースし，他者へ説明し，実際に動かし，もう一度言語活動へ戻る．この往復によって，生徒は「閉める鍵」と「開ける鍵」を，2 つの用語ではなく，情報通信における役割の関係として捉え始める．冒頭に挙げた発信する力と実践する力も，操作の回数ではなく，こうした説明の場面で育つと考えている．情報科の実習では，操作の成功をゴールにせず，操作で起きたことを説明し直す時間までを 1 つの学習過程として設計したい．

参考文献

1) 阿南統久：教科「情報」における言語活動を取り入れた授業実践報告（2014），https://www.sky-school-ict.net/ite/information/kyouka_info/20140530.html（参照 2026-08-01）．
2) 文部科学省：高等学校学習指導要領（平成 30 年告示）解説 情報編（2018），https://www.mext.go.jp/content/1407073_11_1_2.pdf（参照 2026-08-01）．
3) 大石智広：暗号を解読せよ～プログラミングで学ぶ公開鍵暗号（2017），https://www.wakuwaku-catch.net/jirei1762/（参照 2026-08-01）．
4) Rivest, R. L., Shamir, A. and Adleman, L. : A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, Communications of the ACM, Vol.21, No.2, pp.120-126 (1978), https://doi.org/10.1145/359340.359342
5) 伊藤大貴：easyRSA―RSA 暗号体験 Web アプリケーション，https://itou-daiki.github.io/easy_RSA/，https://github.com/itou-daiki/easy_RSA（参照 2026-08-02）．
6) Moriarty, K. et al. : PKCS #1: RSA Cryptography Specifications Version 2.2, RFC 8017 (2016), https://www.rfc-editor.org/rfc/rfc8017（参照 2026-08-01）．

（2026 年 8 月 29 日受付）



伊藤大貴（正会員）
itou-daiki@oen.ed.jp

大分県立日田高等学校 情報科教諭．大分大学大学院教育学研究科修了後，大分県内の公立学校に勤務．情報科教育，データサイエンス教育，教材・Web アプリケーション開発に取り組む．