暗号を解読せよ

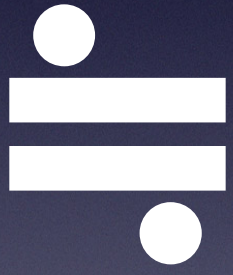
プログラミングで学ぶ公開鍵暗号

神奈川県立生田東高校
大石智広

授業の狙いと背景

背景にある考え

問題解決に
必要な力



プログラミン
グを通して
学べる力

プログラミングを通して学べること

- 手順に分けて考える
- 上手く行っているか確かめる

問題解決力の中身

- 手順化
- 検証

手順化とは

問題解決への道のりを、細かいステップに分けること

手順化とは

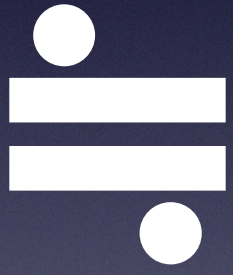
- 問題解決への道のりを、細かいステップに分けること
- プログラムを書く能力のコアスキル

検証とは

- 手順が実際に問題解決に向かっているか、確かめること
- いつ、どうやって確かめたら良いか？を考える

背景にある考え

問題解決に
必要な力



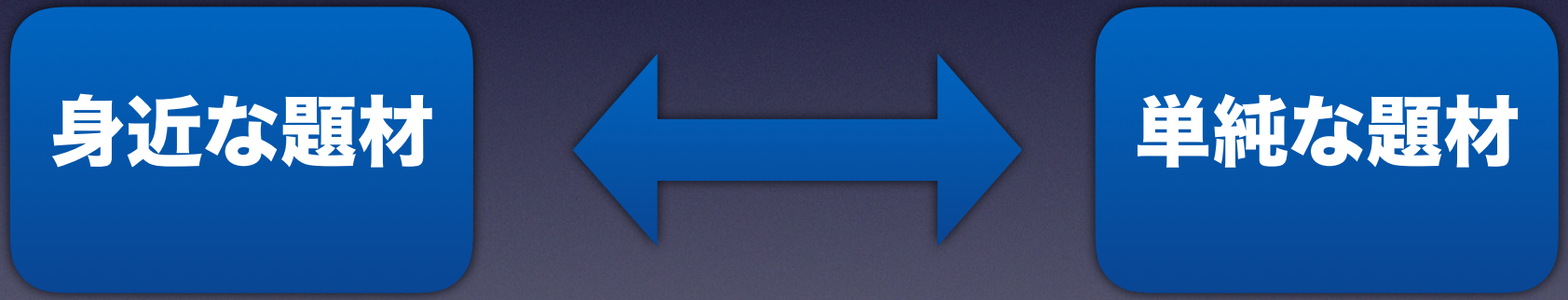
プログラミン
グを通して
学べる力

今回の授業のイメージ

1. 問題解決の手順を考える
2. 手順をプログラムで表現する
3. プログラムを実行しながら、手順を検証する

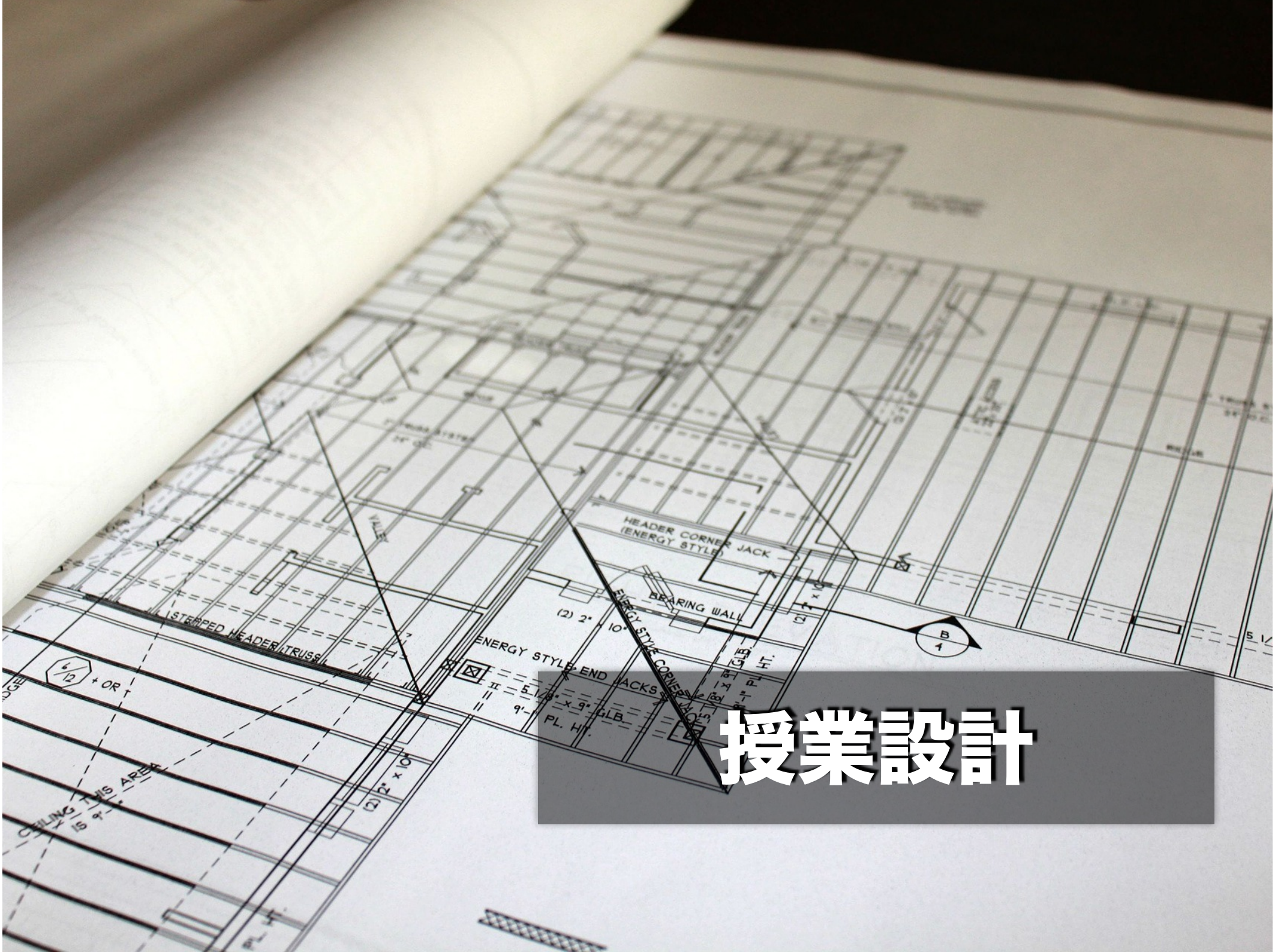

題材の選定

トレードオフ



公開鍵暗号の解読困難性を学ぶ

- 公開鍵の手順がシンプルだが革命的
- 素因数分解の手順がシンプルかつ、コンピューター利用のメリットを感じ易い
- 暗号化は身近ではないが、日常である

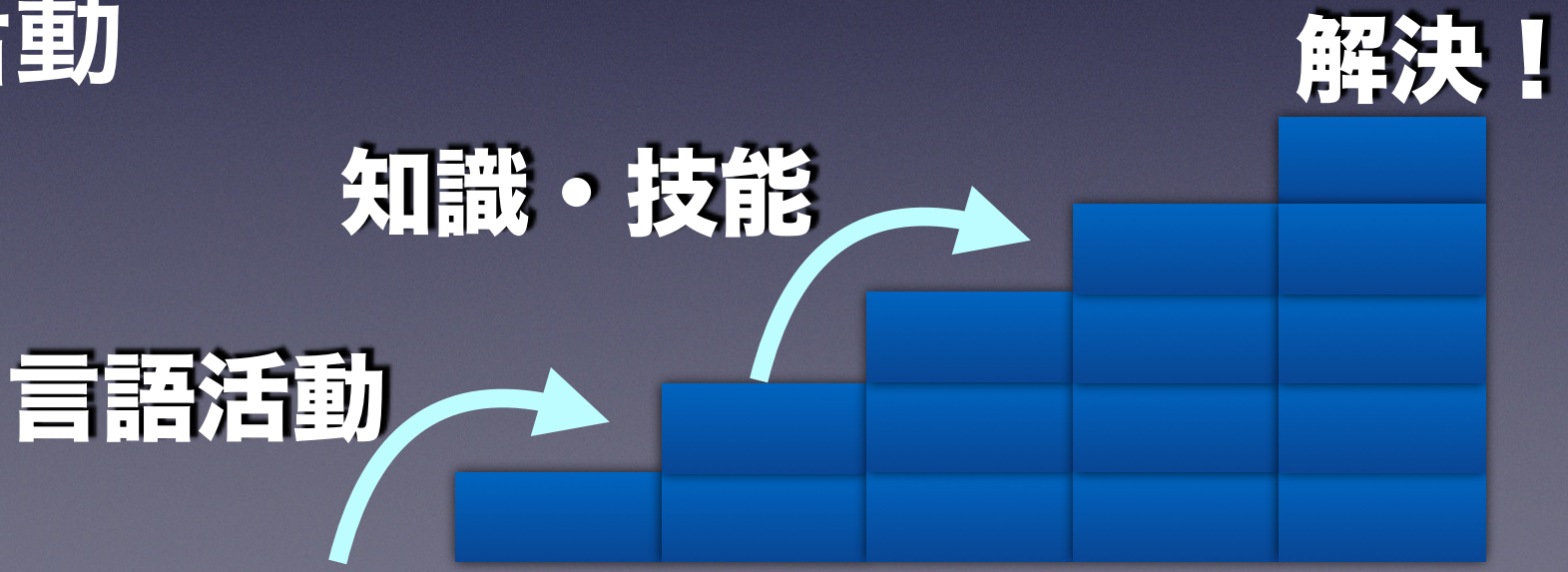

授業設計

授業のねらい

- 公開鍵暗号方式の手順と解読困難性を理解する
- 問題解決に必要な手順化と検証を行う
- プログラムに表現することの利点と、検証の必要性を学ぶ

授業設計のキーワード

- 問題解決型の授業
- スモールステップ
- 言語活動



授業計画

1	公開鍵暗号方式の手順を生徒に発明させる
2	素因数分解の手順を生徒に考案させる
3	コンピュータに素因数分解させ、秘密鍵を作成する

授業の実際

授業計画

1	公開鍵暗号方式の手順を生徒に発明させる
2	素因数分解の手順を生徒に考案させる
3	コンピュータに素因数分解させ、秘密鍵を作成する

公開鍵暗号方式の手順を生徒に発明させる

No	内容	分類
1-1	暗号化に必要な 鍵と手順について理解させる	
1-2	グループで公開鍵方式の手順を 発明させる	手順化
1-3	見つけた手順を文章で表現する	手順化

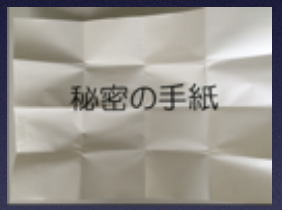
人類が2000年間発明できなかった
難問を５分で発明

鍵を送らなくても良い暗号を
発明しよう

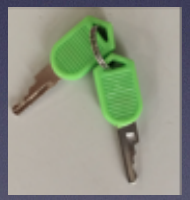
公開鍵暗号方式の手順を生徒に発明させる

ボブ　　イブ　　アリス

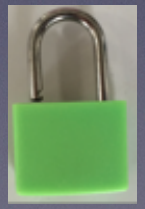
南京錠のかかるケース



秘密の手紙



南京錠の鍵



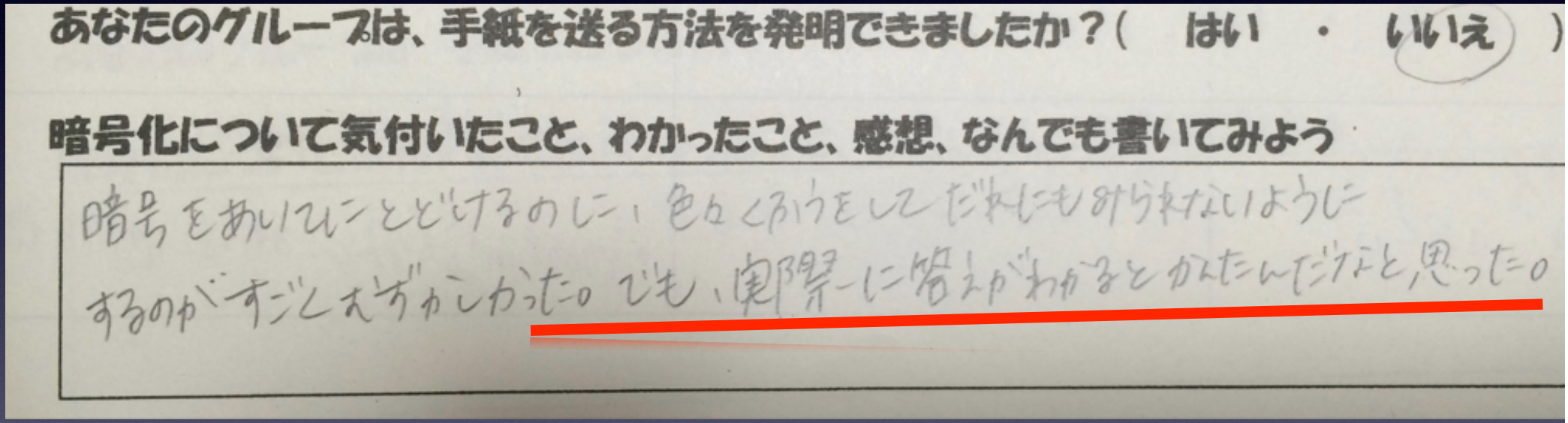
南京錠

イブに見られないで、アリスからボブに手紙を送る手順を見つける

公開鍵暗号方式の手順を生徒に発明させる

- 南京錠や手紙を実際に送りあって、手順を見つける
- 何かを送るときは、必ず一旦イブを経由する
- 最初に見つけた班が優勝！

生徒の反応

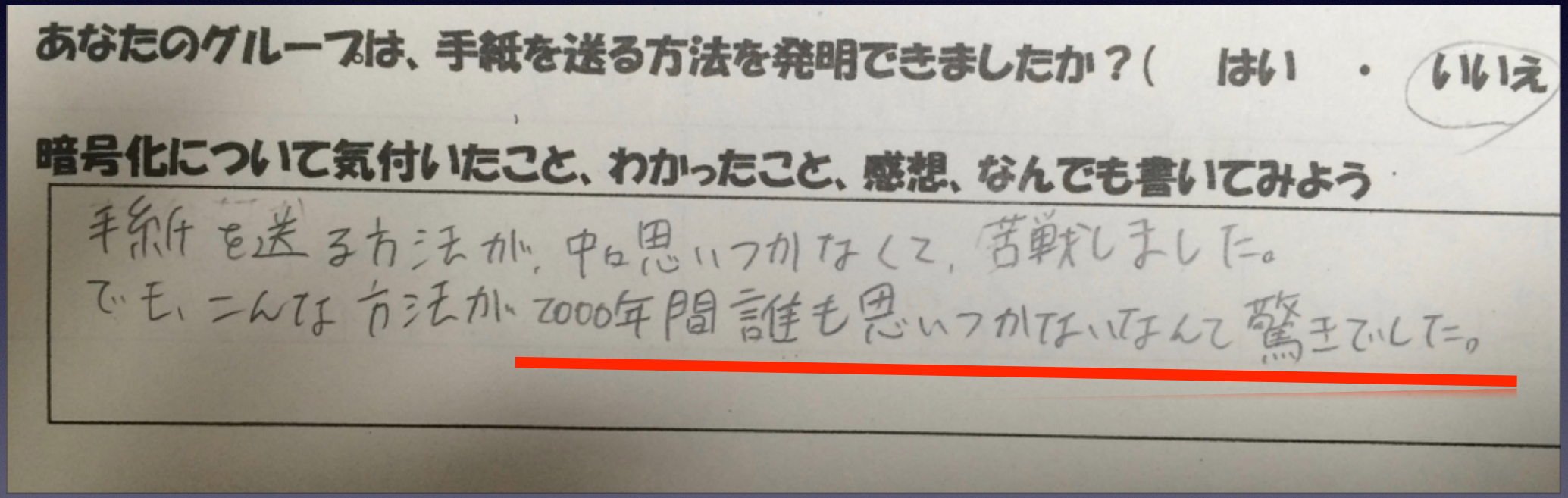


あなたのグループは、手紙を送る方法を発明できましたか？（　はい　・　いいえ　）

暗号化について気付いたこと、わかったこと、感想、なんでも書いてみよう

暗号をあいてにとどけるのに、色々くふうをしてだれにも分られないように
するのがすごくむずかしかった。でも、実際に答えがわかるとかんたんだなと思った。

生徒の反応

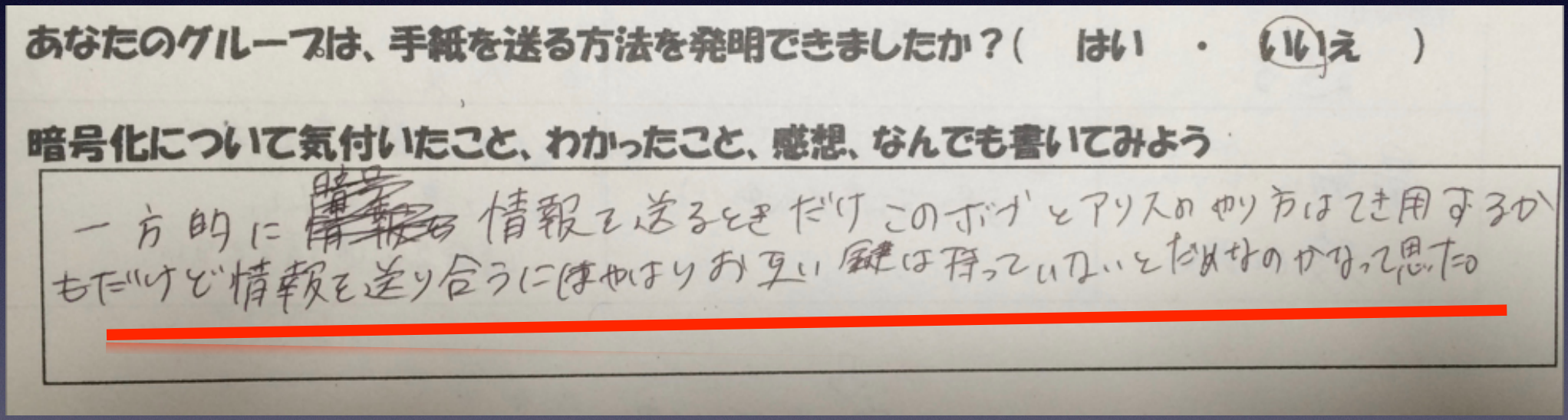


あなたのグループは、手紙を送る方法を発明できましたか？（　はい　・　いいえ）

暗号化について気付いたこと、わかったこと、感想、なんでも書いてみよう

手紙を送る方法が、中々思いつかなくて、苦戦しました。
でも、こんな方法が2000年間誰も思いつかないなんて驚きでした。

生徒の反応



あなたのグループは、手紙を送る方法を発明できましたか？（　はい　・　いいえ　）

暗号化について気付いたこと、わかったこと、感想、なんでも書いてみよう

一方的に暗号情報を送るときだけこのボブとアリスのやり方は使用するかもだけど情報を送り合うにはやはりお互い鍵は持っていないとだめなのかなって思った。

授業計画

1	公開鍵暗号方式の手順を生徒に発明させる
2	素因数分解の手順を生徒に考案させる
3	コンピュータに素因数分解させ、秘密鍵を作成する

素因数分解の手順を生徒に考案させる

No	内容	分類
2-1	公開鍵が素因数分解出来れば、秘密鍵が解読できることを説明	
2-2	個人で素因数分解の手順を考案させる	手順化
2-3	グループでどの手順が優れているか議論させる	手順化
2-4	手順が正しく素因数分解を行えるか検証	検証

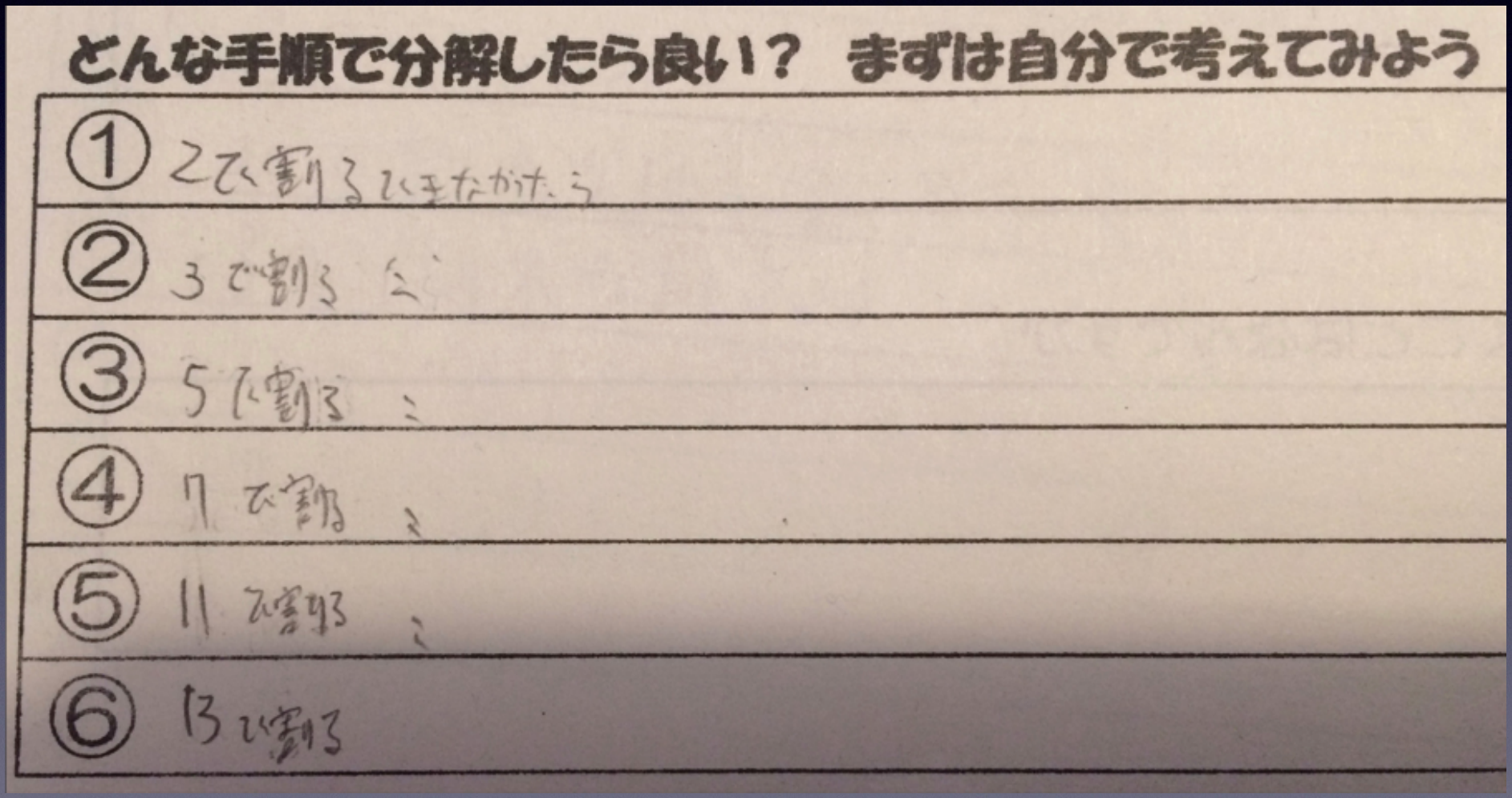
公開鍵が素因数分解出来れば、秘密鍵が解読できることを説明

- 公開鍵＝秘密鍵❌別な素数
- 公開鍵を素因数分解すれば、秘密鍵を入手できる

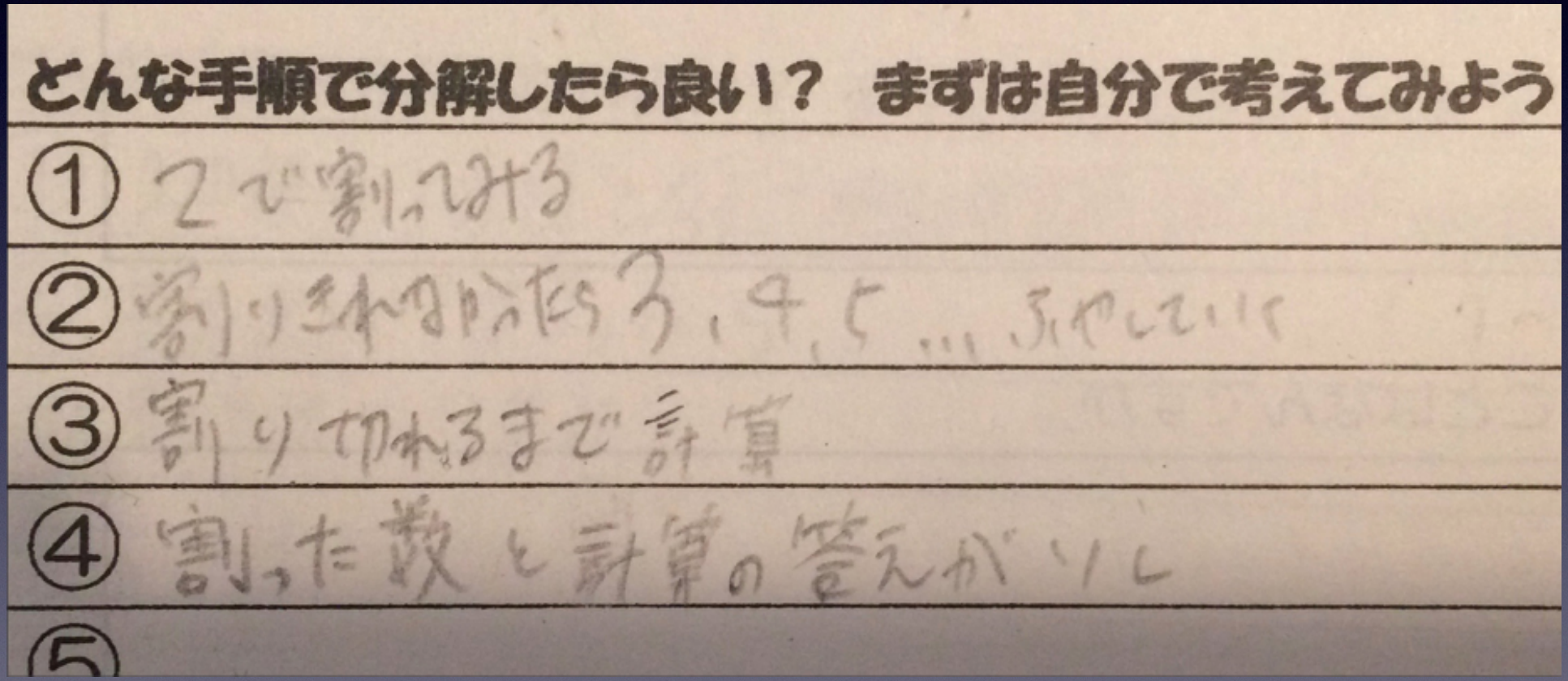
個人で素因数分解の手順を考案させる

- 素因数分解という言葉を使わない
- 時間とともに、ヒントを表示
- 個人で出来なくても、この後のグループ活動でフォロー

個人で素因数分解の手順を考案させる



個人で素因数分解の手順を考案させる


どんな手順で分解したら良い？　まずは自分で考えてみよう

① 2で割ってみる

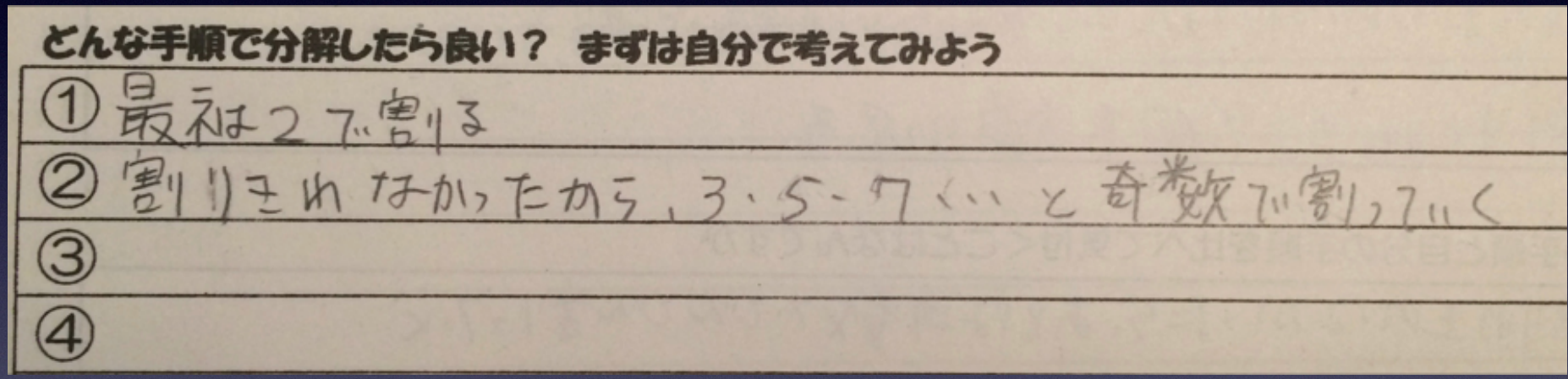
② 割りきれる分だけ3，4，5…ふやしていく

③ 割り切れるまで計算

④ 割った数と計算の答えがソレ

⑤

個人で素因数分解の手順を考案させる


どんな手順で分解したら良い？　まずは自分で考えてみよう

① 最初は2で割る

② 割りきれなかったから，3・5・7くらいと奇数で割っていく

③

④

手順が正しく
素因数分解を行えるか検証

- あらかじめテスト用の数字を用意
  - 703,551,731,667
- 電卓を使いながら、手順を実行

授業計画

1	公開鍵暗号方式の手順を生徒に発明させる
2	素因数分解の手順を生徒に考案させる
3	コンピュータに素因数分解させ、秘密鍵を作成する

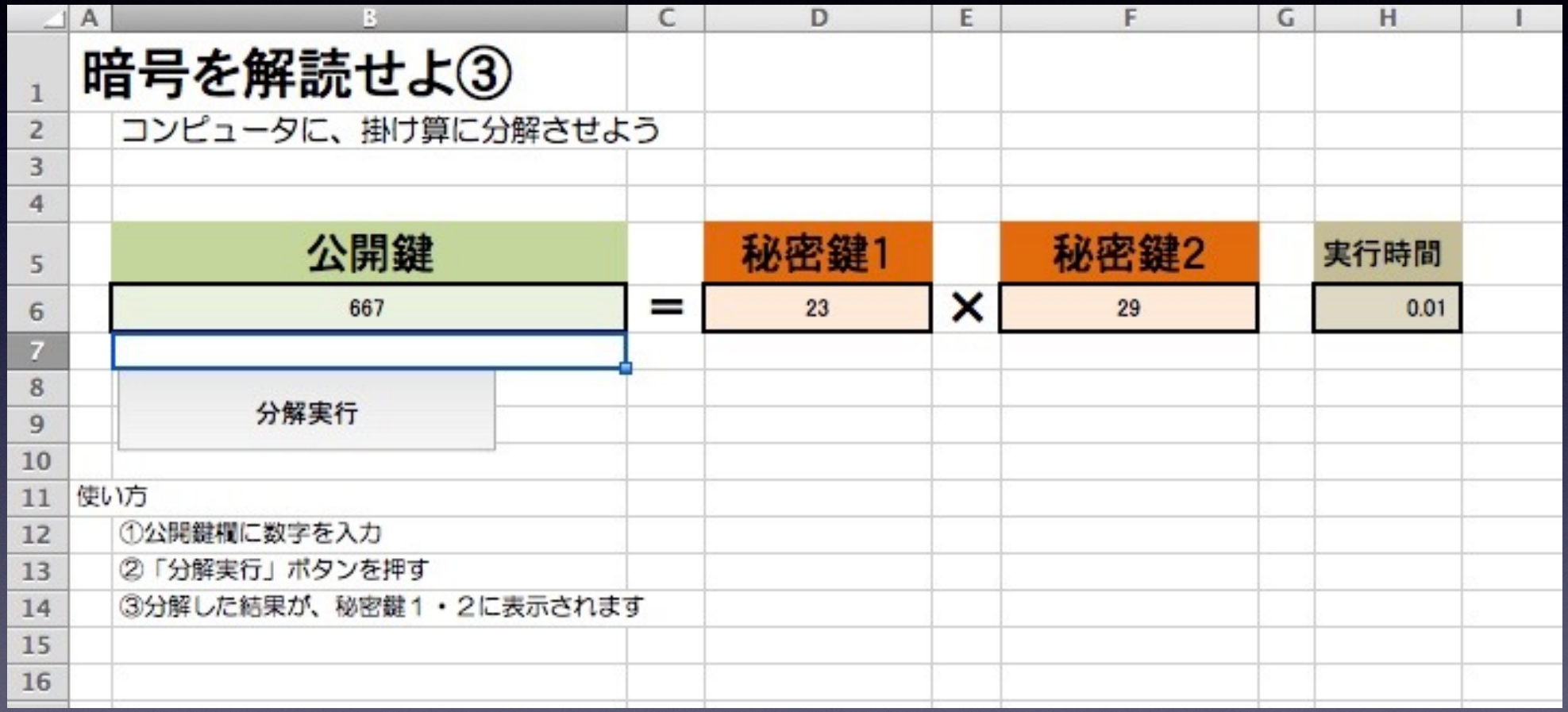
コンピュータに素因数分解させ、秘密鍵を作成する

No	内容	分類
3-1	コンピューターは手順を素早く正確に実行できることを理解させる	
3-2	素因数分解を行うプログラムをテストする方法を考えさせる	検証
3-3	テストを実行させる	検証
3-4	プログラムを実行し公開鍵から秘密鍵を作らせる	

用意したプログラム

- プログラムは事前に教員が用意
- EXCEL VBAを使用
  - どんな学校にも必ずある
  - 入力画面や、データを簡単に用意できる
- 分かりやすい画面を用意

用意した画面



暗号を解読せよ③

コンピュータに、掛け算に分解させよう

公開鍵		秘密鍵1		秘密鍵2	実行時間
667	=	23	×	29	0.01

分解実行

使い方

①公開鍵欄に数字を入力

②「分解実行」ボタンを押す

③分解した結果が、秘密鍵１・２に表示されます

ソース

```
Sub main()
    Dim key As Double
    Dim q, r As Double
    Dim i As Double
    Dim flag As Boolean

    Dim starttime, stoptime, timediff As Variant


    flag = True

    key = Cells(6, 2).Value
    Cells(6, 4).Value = "計算中"
    Cells(6, 6).Value = "計算中"

    i = 1                   '1からスタート'

    starttime = Timer
    While flag
        i = i + 1           'iに1を足す'
        q = key / i          '公開鍵をiで割る'
        r = key - Int(q) * i   '余りを求める'
        If r = 0 Then        'もし余りがゼロつまり割り切れていたら'

            Cells(6, 4).Value = i '割った数と、割り算の答えを表示'
            Cells(6, 6).Value = q

            flag = False       '割り切れるまで繰り返し'
        End If
    Wend
    stoptime = Timer
    timediff = stoptime - starttime

    Cells(6, 8).Value = timediff

End Sub
```

プログラムが正しく動くか テストさせる

- 素数を２つ掛けて、テスト用の数字を作らせる
- プログラムで分解し、元どおりになるかを検証

プログラムに公開鍵を分解させる

- 866421697541683
  - ５秒ほどで分解
- 実際の公開鍵の桁数10^{600}を説明

生徒の反応

暗号について気付いたこと、学んだこと、を何でも書いてください

かんたんな暗号ではなく人間では
考えられないくらいの数字でかかれていて
インターネットってすごいんだなと思いました。
暗号はとけてしまうならいみがなくて、解けないかぎり
暗号だなと思いました。

生徒の反応

暗号について気付いたこと、学んだこと、を何でも書いてください

色々な手順で暗号が解読されたりと，1人一人違うやり方で解読していたのですごいと思った。グループで分解の手順を発表しあった時にすごい発見があったりととても勉強になりました。

コンピュータプログラムについて、気付いたこと、学んだこと、を何でも書いてください

コンピューターで、暗号解読すると5秒もかからずに解読されていて手順で普通にやると，時間がかかり大変だったのでコンピューターでやったほうが普通に速いから楽にできると思った。

生徒の反応

暗号について気付いたこと、学んだこと、を何でも書いてください

暗号はそうそう簡単にできていないが、人間よりすぐれてるPCでも解くのに
時間がかかるというのはそうとうだなと思った。
これだけ守られているなら安全だと思った。でも実際時間もかかるしめんどくさいから
暗号を解こうとはなかなか思えない。

コンピュータプログラムについて、気付いたこと、学んだこと、を何でも書いてください

プログラムを作るときが一番大事だと思った。そこで間違えたり
いくらコンピューターでも全て正しくなければできないんだなと思った。


UPDATE

バグを発見させる

- プログラムが暴走するケースを用意しておく
  - 「1」「整数ではない数」
- 発見を競争させる
- 修正させるか、修正してみせる
  - 作ったら終わりではない、ことを示せる

重視する点に合わせて バリエーションを作る

- 公開鍵の手順の発見まで
- ネットワークを重視
  - コンピュータ同士での鍵のやりとりを解説
  - 実際にやりとりしている鍵を見る
- プログラムを重視
  - 実際にプログラムを作成する
- 大学数学への招待　リーマン予想

素因数分解を行うプログラムを生徒に作らせる

- 簡単に記述できる
- 変数型について学ぶ良い課題
  - int型では桁あふれしたり、mod関数が桁あふれしたり
- 繰り返しの終了条件について学ぶ良い課題

最後に

暗号について気付いたこと、学んだこと、を何でも書いてください

コンピュータプログラムについて、気付いたこと、学んだこと、を何でも書いてください

授業全体の感想を何でも書いてください

楽しかった。

授業全体の感想を何でも書いてください

2時間授業をやってみて、あっという間に終わってしまいとても学んだ事が
多かったし楽しい授業でした。
コンピューターは、色々な事に役立ったりすることが改めて分かったのでよかったです。

今回の授業

公開鍵暗号方式を学ぶ

コンピュータプログラムについて、気付いたこと、学んだこと、を何でも書いて

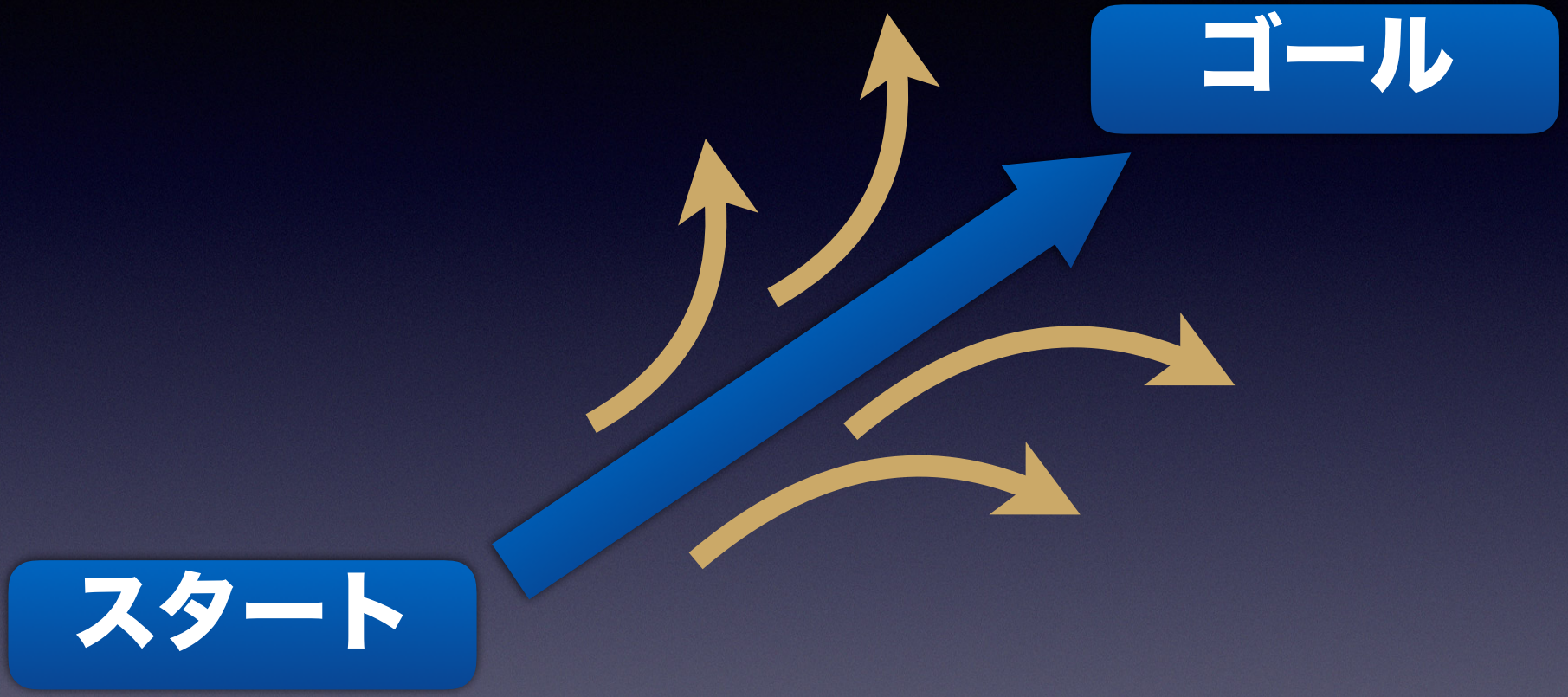
短時間で計算できちゃうのですごいおどろきました。

授業全体の感想を何でも書いてください

いつもより楽しい授業でした!

Appendix

手順化と検証の関係



- 手順化：ゴールまでの真っ直ぐな進み方を見出す
- 検証：ゴールに向かわない道を見出す