アンプラグドを活用した公開鍵暗号学習プログラムの情報科教育への適用

間辺広樹[†1]　兼宗進[†2]　並木美太郎[†3]

本稿では、パズルを用いた公開鍵暗号方式の学習活動と、高校の情報科教育における授業実践について報告する。遠隔地間での暗号化通信を実現した公開鍵暗号方式は、今や情報社会の基盤を支える重要な技術の一つである。しかし、その原理は、二つの特異な概念を使ったシステムであるために、高校生が直感的な理解を得ることは容易ではない。その一つが、関数の「一方向性」であり、もう一つが、公開鍵と秘密鍵という「二つの鍵」である。そこで、我々は、コンピュータ・サイエンス・アンプラグドの学習活動であるツーリストタウンとキッドクリプトに着目した。これらは、視覚的なパズルを用いて「一方向性」と「二つの鍵」の概念を体験的に学ぶ事を可能にしている。この学習活動に独自の工夫を施しながら、高校で授業実践した結果、公開鍵暗号方式の概念を直感的な理解を促し、情報科教育のカリキュラムに組み込める効果的な学習活動になることがわかった。

A Learning Program of Public-key Encryption for Informatics Education

Hiroki Manabe,[†1] Susumu Kanemune[†2]
and Mitarou Namiki[†3]

This paper describes a learning program of public-key encryption for informatics education in high school. In this lesson, we used the computer science unplugged activities. Public-key encryption is an important technology in IT society today. However, it is not easy for high school students to understand it. Because it has two kinds of difficulties:one-way function and two different keys. So we used 'Tourits Town' and 'Kid Krypto' activities from CS unplugged. The students could understand encryption easily by using graphical puzzle games in the activities. We added some original improvement to the activities. From our experiment lessons, we confirmed the positive effects of CS unplugged activities in high-school informatics education.

1. はじめに

情報化社会の進展に伴ない、情報セキュリティについて学ぶことの意味は、年々大きくなっている。その中で、核となるのが、「情報の暗号化」に関する知識・技術である。

暗号技術は、情報社会の基盤を支える影の主役として大きな役割を担っている。平成22年1月に公示された新学習指導要領においても、教科「情報」の改善の基本方針に「情報安全等に対する実践的な態度をはぐくむ指導を重視する」と記され、情報セキュリティ教育の大切さが見直された。新たに設けられる科目「情報の科学」の「内容とその取り扱い」については、「情報セキュリティについては、情報セキュリティを確保するために情報通信ネットワークの中で個人認証や情報の暗号化などの技術が必要となることを理解させ、それらの技術ではどのような工夫がされているかを理解させる」と明確に、暗号技術を理解させることの必要性が、説かれている。

しかし、暗号の技術や仕組みの背景には、複雑な数学的課題が潜在していることが多く、学習者の意欲を維持しながら原理の理解を促すための授業を進めていくことは難しかった。中でも、公開鍵暗号方式（以下、公開鍵方式と記す）は、一方向性関数や、状況に応じた鍵の使い分けなど、特殊な概念を組合わせて成り立つ技術であることから、実感を伴った教材の開発や、学習者の意欲を惹き出す実習を行うことは難しかった。

そこで、授業の中に体験型学習法であるコンピュータ・サイエンス・アンプラグド[1)2)]（以下、アンプラグドと記す）を取り入れて、これらの問題の解決を目指す学習プログラムを検討することとした。

本稿では、平成25年度より科目「情報の科学」へ移行することになる科目「情報B」の中で実践した、公開鍵暗号の学習プログラムの経過と効果について報告する。

2. 情報科教育における暗号の学習

本章では、高校の情報科教育で扱うべき内容と、学習上の課題についての検討結果を記す。

†1 秦野総合高校 Hadano Sogo High School
†2 大阪電気通信大学 Osaka Electro-Communication University
†3 東京農工大学 Tokyo University of Agriculture and Technology

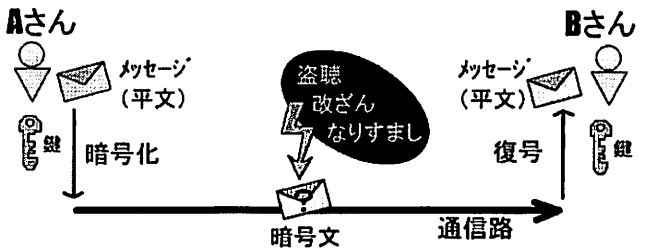

図 1　暗号の基本方式

2.1　暗号化方式の学習について

2.1.1　暗号化の重要性

暗号は、「情報を第三者から守る」ことと「その情報を盗む」ことのせめぎ合いから発達してきた技術である。その必然性を踏まえて指導することは、現代の暗号技術を理解することに繋がる。また、「送信者が鍵を使って情報を暗号化して通信路に流し、受信者が鍵を使って復号する」という基本的な方式 (図 1) は、昔も今も変わってはいない。まずは、この基本方式とそれを説明するための用語（「平文」「復号」など）の理解は定着させたい。

また、携帯電話の通話やメール、インターネットでの買物など、身近なところに暗号化通信があるにもかかわらず、多くの高校生が、自分の生活と関わりがある、という認識を持ってはいない。

したがって、まずは、暗号とは何か、何故暗号が必要なのか、ということを、日常的な素材を提示しながら、理解させることが重要である。

2.1.2　共通鍵暗号方式と公開鍵暗号方式の原理

現在、使われている暗号技術は、送信者と受信者の「鍵」の使い方によって、共通鍵暗号方式（以下、共通鍵方式と記す）と公開鍵方式に分けられる。

あらかじめ送信者と受信者の間で共通の鍵を作っておいて暗号化と復号にその鍵を使うのが共通鍵方式であり、事前の鍵の交換はせずに暗号化と復号に別々の鍵を使うのが公開鍵方式である。これらの方式が、用途や状況に応じて使い分けられたり、組み合わされて（ハイブリッド方式）使われる。

従って、実際に使われている暗号技術を理解するためには、共通鍵・公開鍵両方式の原理

1	2 つの素数 p,q を選び、n = p × q を求める
2	f = (p - 1) × (q - 1) を求める
3	f と互いにその数 b を選ぶ
4	a × b を f で割った時の余りが 1 となる数 a を選ぶ
5	n と a を公開鍵とする
6	平文をコード化した数 M から、M の a 乗を n で割った余り C を求める
7	暗号文として C を送信する
8	受信した暗号 C から、C の a 乗を n で割った余りとして M が得られる

表 1　RSA 暗号の基本的な手順

や鍵の使い方、メリット・デメリットを理解しておく事が必要となる。

2.2　学習上の課題

学習内容の分析から、各暗号方式の「原理」を学ぶことが、暗号化を学習する上で、重要であることがわかった。しかしながら、公開鍵方式においては、その原理が理解しにくい。理由としては、公開鍵方式が、日常的とは言えない、二つの概念を組合わせて成り立つ技術だからである。

その一つの概念が、関数の「一方向性」である。一方向性とは、「A → B は簡単であるが、B → A は困難である」という性質を言う。実装されている技術には、素因数分解や離散対数問題など代数学の難問が利用されている。そのため、B → A が困難であることの理由や度合いを、簡単に説明することができなかった。

もう一つの概念が、用途によって使い分ける「二つの鍵」である。共通鍵方式は、開ける鍵と閉める鍵は同じであり、日常的な鍵の使い方と対応させて、その概念はわかりやすい。しかし、公開鍵方式では開ける鍵と閉める鍵が異なる。この、非日常とも言える鍵の使い方や手順は、多くの学習者を戸惑わせてきた。

これまで一般的に行われてきた学習法は、主に RSA 暗号を扱った実習であった。RSA 暗号は、「桁数の大きな合成数を素数に分解する」ことの困難さを理由に、信頼度を確保して成り立っている暗号である。従って、その実習には、素数や素因数分解、剰余など数学的な話題を避けて通ることはできない。結果として、表 1 のような計算手順を追いかけることになり、学習者の意欲を継続させることが難しかった。

2.3　本研究の目標

本研究は、アンプラグドを活用した通信の体験実習を通して、公開鍵方式を支える「一方向性」「二つの鍵」の概念を獲得する学習プログラムの開発を目指すものである。

3. アンプラグドとキッドクリプト

本章では、アンプラグドの有効性と実験授業に活用した章についての詳細を述べる。

3.1 アンプラグドとは

アンプラグドとは、ニュージーランドのTim Bell博士らが開発したコンピュータ科学を学ぶための手法である。その特徴は、カードゲームやグループ学習など体験的な活動を通して、10歳程度の子供でもコンピュータ科学を学べるように工夫されている点にある。アンプラグドは、世界各国の言語に翻訳されている。日本語版は兼宗らによって1章から12章の12項目が「コンピュータを使わない情報教育[3]」として書籍化されている。

アンプラグドの扱っている題材は、2進数など基本的なものから、最小全域木や状態遷移など大学の授業で学ぶような題材まで幅広い。先生が教え込む、というより、学習者がゲーム性の高い活動を通して、その活動に内在するコンピュータ科学の本質を感じ取れるような流れがある。そういった形で獲得した理解は、強い印象を伴って、学習者に定着する[5][6]。本章で紹介する「ツーリストタウン」と「キッドクリプト」もまた、その特徴を持った活動のデザインパターン[4]を有している。

ツーリストタウンで、一方向性の重要性と強度を学び、キッドクリプトで暗号化と復号について体験的に学ぶ学習プログラムとなっている。

3.2 14章「ツーリストタウン」

アンプラグドの第14章である「ツーリストタウン」について記す。この章では、「最小支配集合問題」を扱っている。アンプラグドでは、最小支配集合問題について、次の例え話で記されている。

『街の交差点にアイスクリーム販売のバン(車)をいくつか置いて、商売をする。その際、他の交差点にいる客も道を1本歩けばアイスクリームを手に入れられるように、バンを置きたい。この条件を満たすための必要最低限のバンの台数と、それ設置する交差点を求めよ。』

この例え話を、図式化したものを、図2に示す。人々は、わざわざ次の交差点を超えてまでアイスクリームを買いに行きたくはない。しかし、バンをたくさん配置してはコストが掛かる。経営者としては、必要最低限の投資で、出来るだけの収益を上げたい。では、どうしたら良いか、という問題である。

例に示したレベルの「街」の大きさであっても、解決には数分あるいは、数十分を要するであろう。では、コンピュータを使えばすぐに解けるかというと、そうではない。これは、

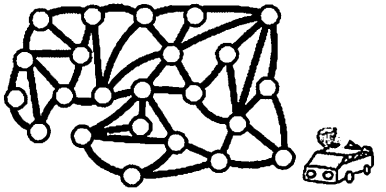

図2 最小支配集合(ツーリストタウン)の問題例

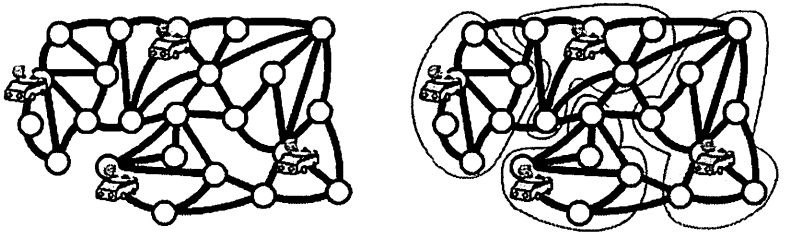

図3 最小支配集合の解(左)とバンが「支配」している様子(右)

グラフ理論においてのNP困難に分類される問題である。したがって、即座に解決に導くための決定的なアルゴリズムは存在せず、最適解を求めるには「総当たり攻撃」を行うのが基本となる。

例題となったこの問題の解を図3に示す。それぞれのバンが他の交差点を「支配」している様子(図3右)から、これが最適解であることがわかる。

しかし、解を求める事に反して、問題を作ることは難しくない(図4)。

まず、解となる「バンを置く交差点」とそこから伸びる道及び「バンを置かない交差点」を決める(図4左)。次に「バンを置かない交差点」同士を連結させる(図4中央)。最後に「バンを置く交差点」と「バンを置かない交差点」の区別をなくす(図4右)。これで、完成である。

一旦、交差点の区別をなくしてしまうと、バンを配置していた交差点がどこかの判断はつかなくなる。作った本人でさえ、解がわからなくなることもある。このように、問題を作る

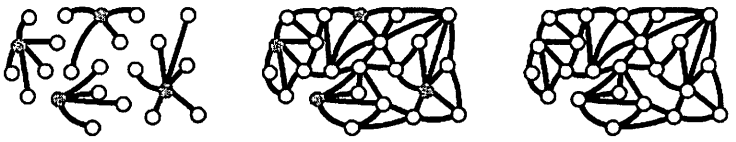

図 4　鍵の作り方 (左 → 中央 → 右)

のは優しいが、解くのは難しい、という「一方向性」を、視覚的な問題として提供している。

更に、街が大きくなって、交差点の数が、100,200,300,…と増えていくとどうなるか。学習者は、自分が問題を解いた経験から、常識的な時間では解決出来ないことを、直感的に感じ取ることが出来る。

アンプラグドでは、この一方向性の性質を公開鍵暗号方式に利用している。図 2 が公開鍵、図 3 が秘密鍵の役割を果たす。実際の授業では、生徒一人一人が、鍵セットを作成し、公開鍵のみを生徒間で交換することで、秘密鍵探しのゲームになる。それは同時に、「一方向性」の概念を、身を持って知ることでもある。

3.3　18 章「キッドクリプト」

アンプラグドの第 18 章である「キッドクリプト」について記す。この章では、14 章で作った鍵セットを使って、公開鍵暗号方式の通信を体験することができる。その方法は、単純な足し算を用いるが、間違えると意味をなくすので、慎重さが求められる。まずは、例として、メッセージ「24」を暗号化した状態の一例を図 5 に記す。

次に、これを作成した手順を図 6 に記す。

【手順 1】暗号化する数を、

24 = 1+1+1+3+1+2+0+0+0+1+1+0+1+2+2+1+0+1+0+3+2+0+1

のように、交差点の数と同じ項数の和となるようにランダムに展開する。そして、それらの数値を各交差点にセットする (図 6 左)。

【手順 2】すべての交差点に対し、「その交差点と隣接する交差点にセットされた数の合計」を計算する。右上の点のは、3+1+0+0+2+3 として 9 が得られる (図 6 右)。

【手順 3】この合計値のみを表示したものが、図 5 の「暗号文」となる。

「暗号文」を作成したら、それを受信者に送る。受信者は、暗号文を受け取ったら、この暗号化通信の元になった、ツーリストタウンの解 (図 3) の交差点に表示された数値を合計

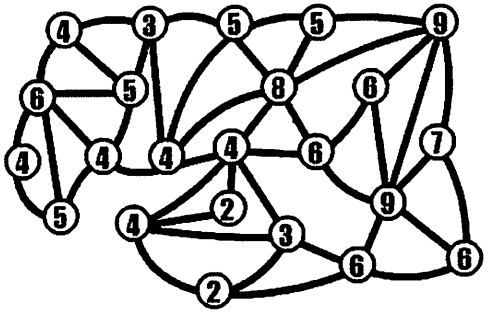

図 5　メッセージ「24」の暗号

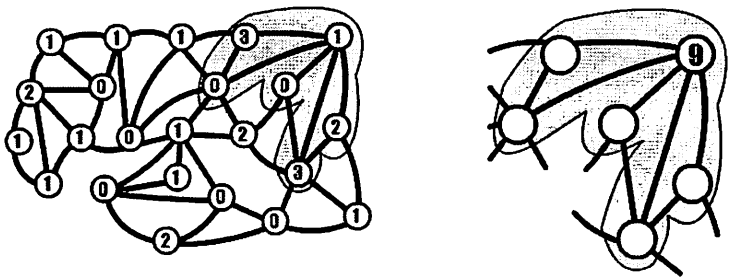

図 6　暗号を作成する手順

する。この合計値 5+6+4+9 こそが、元のメッセージ「24」である (図 7)。解となった交差点の「支配」(図 3 右) は、入力された数値を過不足なく数え上げたことになるからである。

これによって、「暗号文」が「復号」されたことになり、暗号化通信が成立する。

このように、キッドクリプトでは、ツーリストタウンの内容を受け継いで、暗号化通信を体験的に学ぶ事を可能にしている。

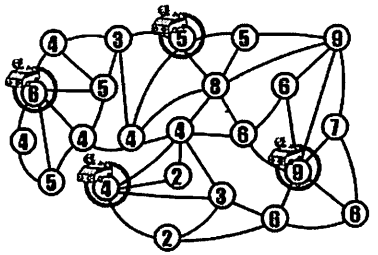

図 7　キッドクリプトの「復号」

4. 実験授業

本章では、本学習プログラムを使い、高校で行った実験授業の様子について記す。

4.1 対　　象

実験授業は、秦野総合高校の選択科目「情報 B」(生徒 29 名－2 年 8 名・3 年 21 名) の 2 コマ (1 コマ 90 分× 2) を使って実施した。生徒は既に「情報 A」を受講済みであり、2 進数や情報のディジタル化については、学習済みであった。

4.2 事前アンケート

本学習に先駆けて、生徒 29 名を対象に、暗号に対してどのような知識やイメージを有しているか、アンケート調査を行い、学習プログラムを具体化させることとした。アンケート項目は、「暗号」や「暗号技術」に対して、知っていることを自由記述で書いてもらった。

【質問】「暗号」や「暗号技術」に対し、どのような「知識」を持っていますか。

知らない・わからない　15 名 (51.7 %)

モールス符号に関わる記述　4 名

秘密のやりとり, 戦争に関する記述　各 2 名

船のライトでの会話, 携帯電話に使われている　各 1 名

SSL 通信,Web の接続　各 1 名

この結果、「知らない・わからない」が 15 名と半数を超えた。モールス符号をあげた生徒が数名いるが、前年度の授業 (「情報 A」) でその内容を取り上げたことが影響していると思われる。ディジタル技術との関連については、「携帯電話に使われている」「SSL 通信」「Web の接続」をそれぞれ 1 名の計 3 名が回答したのみに留まっている。

従って、ほとんどの生徒が、暗号の知識を有してなく、暗号技術と日常生活との関わり合いについての意識も低いことがわかる。そこで、暗号の基本から丁寧に理解させていく必要があった。

4.3 授業計画

本学習内容は、難度が高いため、メンバー同士でアイデアを出し合うことで、個人の考察では得られない知識の構築を期待し、クラス全体をそれぞれ 5 人程度になるようグループ分けした活動を多く取り入れることとした。

4.3.1 一日目の授業

『暗号の説明－共通鍵方式の説明－ツーリストタウンの活動』という流れを作った。

(1) 暗号についての説明
(2) 共通鍵方式についての説明と通信体験
(3) 開発したディジタル教材で手品を披露
(4) 最小支配集合についての説明
(5) 例題をグループ単位で解読
(6) ツーリストタウンの作り方の説明
(7) 各自オリジナルのツーリストタウンを作成
(8) 作成したツーリストタウンを生徒間で交換し相互に解読

4.3.2 二日目の授業

『公開鍵方式によるメッセージの送受信体験－公開鍵方式の説明－実装されている暗号技術の説明』という流れを作った。通信実習には、他の生徒が「解読しようとする」ことが考えられることから、暗号強度テストと位置付けた。

(1) 生徒作品によるディジタル教材で暗号通信実験
(2) キッドクリプト暗号の仕組み・作り方を説明
(3) 公開鍵方式の公開鍵と秘密鍵について説明
(4) 「なぜ鍵を公開しても大丈夫なのか」をテーマにグループ討論
(5) 公開鍵方式の実装例として RSA 暗号と SSL を紹介
(6) SSL を WEB ブラウザで確認
(7) 【まとめ】暗号について教科書で確認

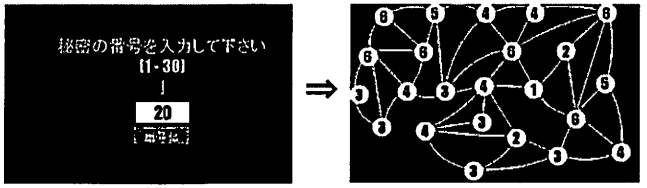

図 8　手品に使えるディジタル教材

図 9　授業の様子・最小支配集合の解説 (左)・例を見ながらオリジナルのツーリストタウンを作成 (右)

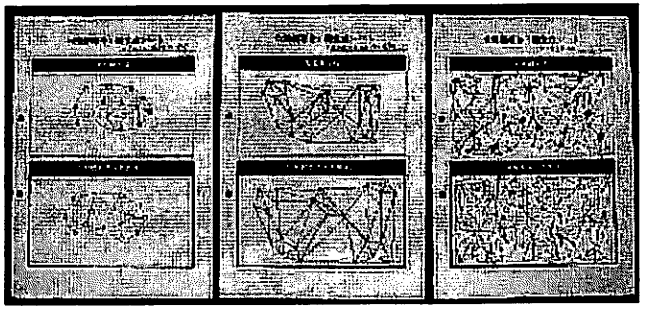

図 10　生徒によるオリジナルのツーリストタウン

4.4 用意した教具

本学習に際して、公開鍵方式の通信を疑似体験するためにディジタル教材を開発した。これは、テキストボックスから数値を入力した (図 8 左) 後、「暗号化」ボタンを押すと、「暗号文」、すなわち暗号化した状態が画面に表示される (図 8 右)、というものである。この過程を手計算で行うことも可能であるが、時間が掛かることと、ミスが生じることもあり得るため、あらかじめディジタル教材を作成しておくことで、時間の節約と確実な暗号化通信のデモンストレーションが出来ると考えた。更に、瞬時に暗号文を作成出来ることから、「手品」として暗号化通信を演出し、その種を見つけるというシナリオで授業の流れを作ることもできると考えた。このディジタル教材の画面は印刷し、グループ討論にも利用することとした。

また、一日目で作成した生徒の作品から、完成度や問題としての難易度を考慮して数点を選んでディジタル化し、二日目の教材として活用することとした。

4.5 授業結果

4.5.1 一日目の結果

暗号の基本的な概念 (図 1) を説明と、共通鍵方式による簡単な通信体験を行った後、開発したディジタル教材で手品を披露した。手品は、生徒が入力した数値を、後ろを向いていた授業者が当てる、という手品を数回実演した (図 8)。「何で、わかるの?」、と興味を持った生徒が多かった。

簡単な例でツーリストタウンの解き方を説明した後、手品につかったツーリストタウンの解を見つけるよう指示した。生徒はパズルゲームを解くように解を見つけようとした。解けて喜ぶ生徒、解けなくて残念がる生徒がいて、教室が活気に溢れた (図 9 左)。解けない生徒のために少しずつヒントを与えたが、なるべく自力で解を見つけられるように促した。

解を提示した後は、ツーリストタウンの作り方 (図 4) を説明し、問題を自作させた (図 9 右)。プリントは上下に分けて、上段に解・下段に問題を書いた。生徒が作った問題は、グループ内で交換して、相互に解き合った。作成したツーリストタウンのプリントは、授業終了時に提出させた (図 10)。この中から、次回の授業で使うために、数点を選び、教材としてディジタル化することとした。

授業時間全体を通して意見交換が行われた。中でも、手品の実演とツーリストタウンの解読において、生徒の活発さが際立った。生徒の感想からは、「問題を作るのは簡単なのに、解くのが難しい」という「一方向性」を感じ取った主旨の記述が多く見られた。

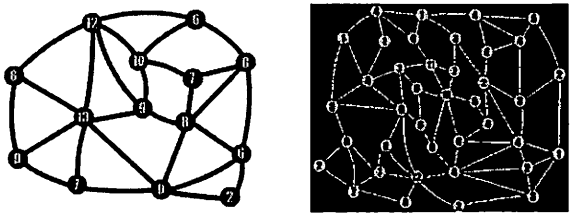

図 11　一日目の生徒作品から作成したディジタル教材

4.5.2　二日目の結果

授業の最初に、生徒全員に復号の手順（図 7）を伝えた。その後、教員用のコンピュータ画面を教室全体に提示して、一日目の生徒作品をディジタル化した二つの教材 (図 11) を提示した。実験に使った作品の作者二人とも、ディジタル化された自分の作品を見て驚いた。暗号化通信実験は、授業者がメッセージを入力し、作品を作った（唯一秘密鍵を知る）本人のみが解読するという状況を想定して行った。この実験で、通信自体は成り立ったが、想定していたキャッチボールのような小気味の良いやり取りにはならず、「秘密鍵を知る者だけが解読できる」といった状況は作れなかった。

キッドクリプト暗号の仕組みと作り方を説明し、ツーリストタウンの解と問題とが、秘密鍵と公開鍵になって、公開鍵方式となることの説明をした。

グループ討議の題材として、「インターネットで買い物ができるが、なぜ、鍵を公開しても大丈夫なのか」をテーマに、グループで話し合いをさせた。5 グループのうち、あるグループから「個人情報を会社に送信しても、その際の暗号が非常に複雑なので、解くことが容易ではない。」とまとめた。他 2 つのグループが、「他の人には解読できないから」という主旨のまとめをした。他のグループからは、まとめが出てこなかった。

公開鍵方式の実装例として RSA 暗号を取り上げ、合成数の素因数分解が使われていることに言及した。また、身近な例として、SSL 通信の様子をショッピングサイトの URL や Web ブラウザの鍵マークで確認し、Web ブラウザと Web サーバとの間で、公開鍵方式による暗号化通信が行われていることを説明した。

最後は、教科書を使い、暗号についてまとめられたページの内容を確認した。

授業の様子としてグループ討議は、意見交換が盛んなグループと、そうではないグループとに別れた。生徒の感想には、「内容が難しい」という記述が多く見られた。

5.　評価と考察

5.1　事後アンケートによる調査

本学習プログラム終了後に、以下の四項目について、アンケート調査した。

（1）　授業は難しかったですか？
- A. 強くそう思う…14 名（48.3 %）
- B. そう思う…13 名（44.8 %）
- C. どちらとも言えない…1 名（3.4 %）
- D. あまり思わない…1 名（3.4 %）

（2）　授業は楽しかったですか？
- A. 強くそう思う…17 名（58.6 %）
- B. そう思う…11 名（37.9 %）
- C. どちらとも言えない…1 名（3.4 %）
- D. あまり思わない…0 名（0.0 %）

（3）　次の項目で、「理解出来た」と思う事に、○を付けて下さい。
- A. 情報を暗号化することの必要性…25 名（86.2 %）
- B. 暗号についての基本的な仕組み…22 名（75.9 %）
- C. 共通鍵暗号方式の大まかな仕組み…12 名（41.4 %）
- D. 公開鍵暗号方式の大まかな仕組み…11 名（34.5 %）

（4）　授業を受けて、「気付いた事」を自由に書いて下さい。
- 街を作るのは簡単だったけど、解くのは難しかった、という主旨の記述…13 名
- 暗号化には色々な方法がある、という主旨の記述…10 名
- 身の回りにたくさんの暗号技術がある、という主旨の記述…7 名

5.2　事後アンケートの結果から

質問（1）（2）の結果から、多くの生徒が「難しい」としながらも、「楽しい」と感じていることがわかる。生徒は、パズルを解く楽しみを味わいながら、緊張感を保って授業を受けたていた。

質問（3）の結果から、暗号化の必要性と基本的な仕組みについては、理解出来たと感じている生徒が多いことがわかる。しかし、共通鍵方式と公開鍵方式を理解したと感じる生徒は少ない。本学習プログラムが公開鍵方式を理解させるものであったことから、この結果を

真摯に受け止める必要がある。考えられる要因としては、「体験的な活動後の説明やプリント教材などが不十分であったこと」「鍵の概念を十分に理解させないまま、難しい概念に進んだこと」などが考えられる。今後、検討をおこない、問題点を明らかにする必要がある。

ところが、質問（4）では、多くの生徒が、記述の中で「一方向性」を取り上げていることから、その感覚的な理解は出来ているものと思われる。これが、「どのように暗号技術と結びついているのか」や「なぜ信頼性を保証し得るのか」の部分を生徒に気付かせたり、伝えるための工夫が、今後の授業改善に有効であろうと推察できる。

5.3 授業の様子から

学習プログラムを通して、生徒は積極的な態度で学習した。授業中の発言などからも、当初、暗号の知識を持っていなかった生徒が、身近な問題として意識を高めていく過程が感じ取れた。本学習プログラムが、情報科教育の内容として妥当であったと考えている。しかし、「難しすぎた」と感じる生徒も数名いることから、説明等を工夫する余地はある。

二日目の「なぜ、鍵を公開しても大丈夫なのか？」に対するグループ討論では、「交差点の数が増えれば作った人以外は解けない」「コンピュータを使えば解けるのではないか」と言った疑問の投げかけや議論の展開を期待したが、残念ながら活発な意見交換は行われなかった。ここは、授業者が教えるのではなく、生徒自身に気付いて欲しい重要なポイントである。今後、実感を伴った理解を得る学習プログラムにするために、その関連付けへの検討が、重要な課題である。

本学習プログラムのような体験的な学習法は、生徒の興味関心を引き付けることは、明らかであるが、「楽しかった、けれど、何を学んだのかよくわからない」という状況に陥るリスクを抱えている。実験授業を通して、暗号について情報科として学ばせる内容と目標到達に向けて必要な体験的な活動の検討をすることの重要性を実感した。

6. ま と め

公開鍵暗号の学習プログラムを検討し、高校の「情報B」の授業で実践した。「ツーリストタウン」と「キッズクリプト」を活用することで、数学的な問題に立入ることなく、視覚的かつパズル的な問題から、公開鍵方式の背景にある「一方向性」と「二つの鍵」を体験する公開鍵暗号の通信実習を行うことが出来た。ゲーム性の高い活動は、生徒の活発な学びの姿勢を引き出した。公開鍵暗号の本質に気付いたグループもあった。実験を通して、本学習プログラムを改善していくことで、新科目「情報の科学」での情報セキュリティ教育に適用させられることがわかった。

本稿で紹介した授業は、暗号化のアルゴリズムに立ち入るのではなく、複数の公開鍵を用意して、それらを解いていくことで鍵方式の理解を進める流れにすることで、「情報B」や「情報の科学」だけでなく、「情報A」「情報C」「社会と情報」の教科でも扱うことが可能である。今後は、各教科における暗号化の学習目標を明確にし、活動内容を精査すると共に、学習法の開発・改善をおこなっていきたい。

参 考 文 献

1) Tim Bell, Ian H. Witten, Mike Fellows: Computer Science Unplugged - An enrichment and extension programme for primary-aged children,2005.
2) Michael Fellows,Neal Koblitz: Kid Krypto - Advances in Cryptology - CRYPTO' 92（1993 P.371-389）
3) 兼宗進監訳『コンピュータを使わない情報教育〜アンプラグド・コンピュータ・サイエンス』イーテキスト研究所, 2007.
4) Tomohiro Nishida, Susumu Kanemune, Yukio Idosaka, Mitaro Namiki, Tim Bell, Yasushi Kuno A CS unplugged design pattern ISSEP 2008 Proceedings, LNCS 5090, Springer, pp.241?252, 2008.
5) 井戸坂幸男，青木浩，兼宗進，久野靖:「コンピュータサイエンスアンプラグドの小学生向け実践の取り組み」.
6) 保福やよい，井戸坂幸男，兼宗進，久野靖:「高校情報BにおけるCSアンプラグドの活用」.
7) 間辺広樹，兼宗進，並木美太郎:「高校の文化祭におけるCSアンプラグド企画実施の報告と課題」.