4G-03

高等学校における 暗号技術の効果的な学習のための教材開発と実践

山口　健二†　　桑名　杏奈‡　　加々美　勝久*
お茶の水女子大学附属高等学校†　　群馬大学電子情報部門‡　　お茶の水女子大学*

1. はじめに

筆者らは，中等教育における情報および数学に関する教材開発を行っている．その一つとして，暗号の教材開発を行っている．暗号技術は，数学と情報の両方の知識・技術に関係しており，教育題材として非常に興味深い内容である．本論文では，暗号の概要や教育現場での暗号技術に関する教育の現状を説明するとともに，開発中の教材の紹介と，それを高校の授業で実践した結果について紹介する．

2. 教材開発の背景・目的

高度情報化社会において，個人情報をはじめとする機密情報の安全性をいかに保つかが重要となっている．その際に使用されるのが，暗号技術である．暗号は共通鍵暗号と公開鍵暗号に分類される[1]．共通鍵暗号方式はシーザー暗号やバーナム暗号，公開鍵暗号方式は RSA 暗号[2]がある．実際これらは組み合わせて使用することもあり，例えば，インターネット上で買い物をするときに，クレジットカード番号や有効期限は，SSL 通信によって暗号化されている[3]．これらの暗号の構築や実装，解読手法，安全性証明には，数学と情報の知識・技術が大いに関係している．

これらは，高校の情報の授業で知識としては習うものの，なぜ，そのような方法で暗号化や復号ができるのか，というところまで授業で教えられていないことが大半である．特に，暗号の安全性となると，大学で習う数学理論が関係しており，なかなか授業で扱えないのが現状である．

したがって，本教育プログラムでは，暗号の安全性を保証している数学理論について，中高生でも分かりやすく説明し，情報科社会における暗号の重要性と，そこで活用されている数学についての理解を深めることを目的とする．Web 上での実際の暗号化や復号のステップについて，実際の数値を用いることで，興味を惹いてもらうようにする．

3. 開発する教材の教科上の位置付け

2022 年度から高校で始まる新学習指導要領では，「情報Ⅰ」が必修（2 単位）となり，さらに，選択科目として，「情報Ⅱ」が登場する．「情報Ⅱ」では，　情報システムにおける，情報の流れや処理の仕組み，情報セキュリティを確保する方法や技術について学ぶ．まず，2022 年度からの「情報Ⅰ」において使用可能な教材を開発することを目指す．

文部科学省のホームページにおいて，「情報Ⅰ」および「情報Ⅱ」教員研修用教材[4]が公開されているが，「情報Ⅰ」では，第 4 章の情報通信ネットワークとデータの活用において，情報セキュリティの要素の一つとして，暗号化の項目があるが，暗号化方式や暗号化アルゴリズムの名称について触れられているが，実際のアルゴリズムの数学的原理は省略されている．また，「情報Ⅱ」についても，RSA 暗号や楕円曲線暗号，SSL といった個別の暗号技術について触れられているものの，こちらも数学的原理は省略されている．この省略されている部分について，学習指導要領の発展的な内容として，教育プログラムを位置付ける．

4. 開発中の教材の紹介

単に数式に従って暗号化アルゴリズムを説明するではなく，まず初めにアプリケーション上で暗号を体験できるプログラムを開発することにした．共通鍵暗号方式のシーザー暗号や単換字暗号，バーナム暗号，公開鍵暗号方式の RSA 暗号について Excel で実装した．相手に送る場合の情報の流れを可視化するとともに，実際に送る数値や文字は，生徒が任意に選べるものとした．また合わせて，指導案も作成した（図 1-4）．

Development and Practice of Teaching Materials for Effective Learning of Cryptography in High Schools
†Kenji Yamaguchi, Ochanomizu University Senior High School
‡Anna Kuwana, Gunma University, Division of Electronics and Informatics
*Katsuhisa Kagami, Ochanomizu University

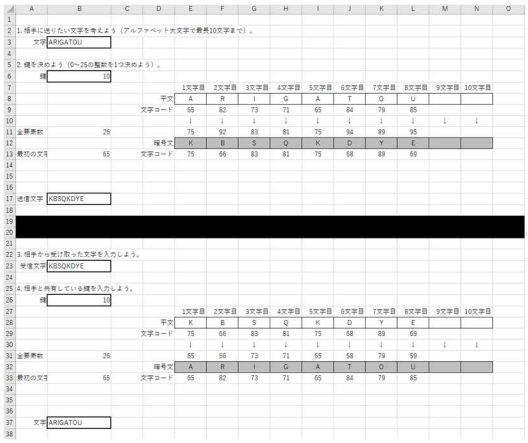


図 1：シーザー暗号の体験プログラム

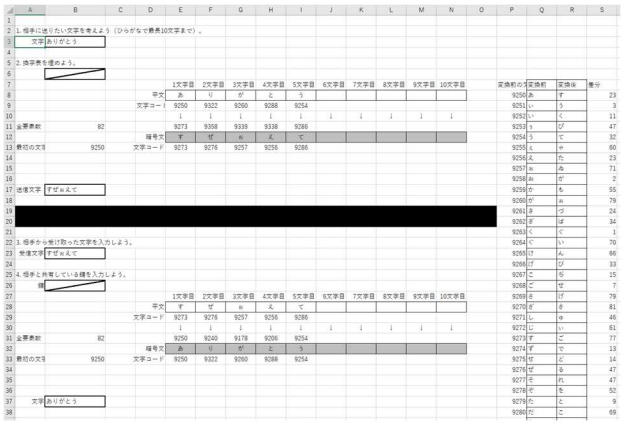


図 2：単換字暗号の体験プログラム

図 3：バーナム暗号の体験プログラム

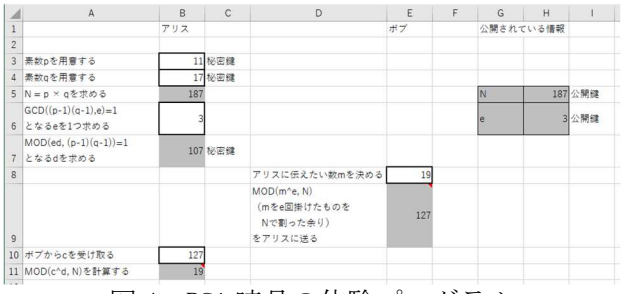
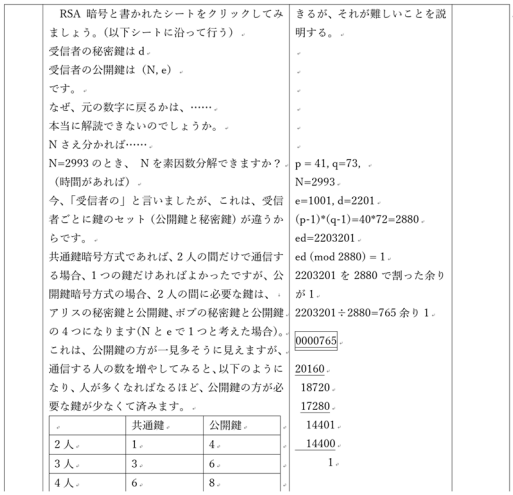


図 4：RSA 暗号の体験プログラム



RSA 暗号と書かれたシートをクリックしてみましょう。(以下シートに沿って行う)	きるが、それが難しいことを説明する。
受信者の秘密鍵は d。	
受信者の公開鍵は (N, e)	
です。	
なぜ、元の数字に戻るかは、……	
本当に解読できないのでしょうか。	
N さえ分かれば……	
N=2993 のとき、 N を素因数分解できますか？ (時間があれば)	p = 41, q=73,
	N=2993
今、「受信者の」と言いましたが、これは、受信者ごとに鍵のセット (公開鍵と秘密鍵) が違うからです。	e=1001, d=2201
	(p-1)*(q-1)=40*72=2880
	ed=2203201
共通鍵暗号方式であれば、2 人の間だけで通信する場合、1 つの鍵だけあればよかったですが、公開鍵暗号方式の場合、2 人の間に必要な鍵は、アリスの秘密鍵と公開鍵、ボブの秘密鍵と公開鍵の 4 つになります(N と e で 1 つと考えた場合)。	ed (mod 2880) = 1
	2203201 を 2880 で割った余りが 1
	2203201 ÷ 2880=765 余り 1
これは、公開鍵の方が一見多そうに見えますが、通信する人の数を増やしてみると、以下のようになり、人が多くなればなるほど、公開鍵の方が必要な鍵が少なくて済みます。	0000765
	20160
	18720
	17280
	14401
	14400
	1

	共通鍵	公開鍵
2 人	1	4
3 人	3	6
4 人	6	8

図 4：指導案

実際に，本教材を用いて，本学の附属高等学校で実践授業を行った．授業後のアンケートの結果，共通鍵暗号方式については，概ね理解が深まったが公開鍵暗号方式である RSA 暗号については，難しいといった感想が多かった．指導方法については，改善の必要性がある．

5. 今後の予定と課題

完成した本教材の指導案およびプログラムについては，サーバ上に公開し，多くの教育機関で利用できるようにする．また今後も活用しやすくするため，改良を続けていく予定である．

謝辞

本教材開発と実践にあたり，お茶の水女子大学理系女性教育開発共同機構の令和 2 年度お茶の水女子大学附属学校における理系女性育成のための新たな教育プログラム開発プロジェクトの支援を頂いた．

参考文献

[1] 神永正博，現代暗号入門，講談社，2017.
[2] R. L. Rivest, A. Shamir, L. M. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", MIT-LCSTM-082(1977).
[3] Internet Engineering Task Force (IETF), " The Transport Layer Security (TLS) Protocol Version 1.3, " RFC8446, https://tools.ietf.org/html/rfc8446, 2018
[4] 文部科学省，高等学校情報科（各学科に共通する教科），https://www.mext.go.jp/a_menu/shotou/zyouhou/detail/1416746.htm, 2020.