鍵暗号方式の理解を深めることを目的とした Web アプリケーションの実装

前田祐杜[1]　御家雄一[2]　伊藤一成[1]

1　青山学院大学社会情報学部 〒252-5258 相模原市中央区淵野辺 5-10-1
2　青山学院大学大学院社会情報学研究科 〒252-5258 相模原市中央区淵野辺 5-10-1

あらまし 令和 4 年度から年次進行で実施されている高等学校共通教科情報の必履修科目「情報Ⅰ」では，情報セキュリティについて言及され，すべての「情報Ⅰ」の検定教科書で鍵暗号化方式の解説が含まれる．しかし，文章や図を見るだけではなく，体験を通して学習することでより理解が深まると考えた．そこで，公開鍵暗号方式と共通鍵暗号方式を文章の受け渡しを通して，体験的に学習することができるアプリケーションを提案し，実装した．講義内で使用し，評価を行ったところ良好な評価を得ることができ，学生の鍵暗号方式に対する理解を促進する可能性があることがわかった．

キーワード アプリケーション，鍵暗号方式，ピクトグラム，情報教育

1. はじめに

鍵暗号方式とは，データのやり取りをする際に鍵を用いて暗号化を施し，通信経路で盗聴されても機密性を保持するための技術である．鍵暗号方式には大きく分けて 2 種類あり，ひとつは，暗号化と復号を同一の鍵で行う共通鍵暗号方式で，もう 1 つは，復号に使う秘密鍵から生成した公開鍵を配布し，その鍵で暗号化された暗号文を自身の持つ秘密鍵で復号する公開鍵暗号方式がある．

平成 25 年に閣議決定された「世界最先端 IT 国家創造宣言」（以下「創造宣言」）では，「初等･中等教育段階でのプログラミング，情報セキュリティを充実させる」ことが謳われている．さらに創造宣言では，「サイバーセキュリティの確保」や「IoT や AI の更なる進化により，実世界とサイバー空間が相互に連携する社会の実現」に向けて，セキュリティ技術の開発や，情報セキュリティ人材の育成が謳われており，鍵暗号化方式の概要は，全国民が理解すべき重要な項目となってきている．平成 22 年施行，令和 3 年度入学生まで実施される高等学校学習指導要領の共通教科情報の選択必履修科目である「社会と情報」と「情報の科学」の内容についての項目で情報セキュリティについて言及され，検定教科書では鍵暗号化方式についての記載がある．また令和 4 年度から年次進行で実施されている高等学校共通教科情報の必履修科目「情報Ⅰ」にも，情報セキュリティについて言及され，すべての「情報Ⅰ」の検定教科書で鍵暗号化方式の解説が含まれる．また，検定教科書や副読本では図を用いることで，鍵暗号方式の流れを視覚的に表現している．

しかし，体験を通して学習することで，文章や図だけでは理解し難い部分をより鮮明に理解することができると考える．「情報Ⅰ」では，特にプログラミングにおいては，様々な学習アプリケーションが用意されており，体験を通して学習することができる．鍵暗号方式においては，これまでも，CS アンプラグドの技法を用いたアクティビティの開発などの取り組みが行われており，これらを「情報Ⅰ」の教材として導入することは可能である[1][2].

しかし，CS アンプラグドを用いた体験学習には専用の機材などを用意する必要がある場合が多く，準備するためには時間やコストを要してしまう．そのため，特定の URL にアクセスするだけで，使用できる Web アプリケーションを用いて鍵暗号方式を体験的に学習することが望ましいと考えた．そこで，プログラミングの単元と同様に，コンピュータやスマートフォンを用いて，暗号化処理・複合処理を体験しながら鍵暗号方式を体験的に学習できるアプリケーションを提案し，プロトタイプを実装したので報告する．

以下 2 章で，実装したアプリケーションについて，解説する．3 章で本アプリケーションの考察を行い，4 章でまとめる．

2. 実装アプリケーション

2.1. 概要

他者とメッセージを交換する中で，送信する内容を暗号化し，受信する内容を復号するプロセスを通して暗号化の仕組みを体験できるアプリケーション「BOUCHO」を実装した．本章では，「BOUCHO」の実装方式及び使用方法について解説する．

2.2. アプリケーション

「BOUCHO」には次の 2 つのモードが存在する．

1. 共通鍵モード…文章を受け渡す送信者と，その文章を受取る受信者の間で通信を行う．共通鍵暗号方式を用いて，共通鍵で送信者の文章を暗号化することで，共通鍵のパスフレーズを知る受信者の

みが暗号文を復号でき送信者の文章を閲覧できる。一方で，共通鍵パスフレーズを知らない場合は解読困難な暗号文のまま表示する．

2. 公開鍵モード...質問文を公開する質問者と，その質問に回答する回答者の間で通信を行う．公開鍵暗号方式を用いて，回答者が文章を質問者の公開鍵で暗号化する．質問者は自身が設定した秘密鍵で暗号文を復号でき，回答者の文章を閲覧できる．

「BOUCHO」にアクセスしたとき，図 1 のメニュー画面を表示し，利用者が使用するモードを選びボタンを押下することでそれぞれのモードに遷移する．

図 1　メニュー画面

2.3. 共通鍵モード

共通鍵モードは，共通鍵暗号方式を使用する．共通鍵モードでは，発言内容を公開する送信者と，送信者の発言内容を受け取る受信者の２名で実施する．共通鍵暗号方式で暗号化するため，送信者は共通鍵となるパスフレーズを用意する．共通鍵暗号方式では，暗号化と復号に同一の鍵を使用するため，送信者が用意したパスフレーズを用いて発言内容を暗号化することで，パスフレーズを知る受信者のみに発言内容を公開することができる．

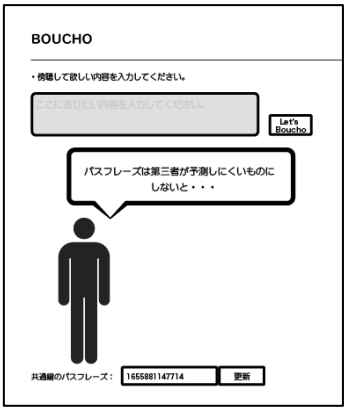
送信者と受信者それぞれの手順の概略を示す．

手順 1 送信者による文章の暗号化
手順 2 受信者による暗号文の復号

次に，それぞれの手順における詳細について 2.3.1, 2.3.2 項で解説する．

2.3.1. 送信者による文章の暗号化

送信者が共通鍵モードにアクセスしたときに表示される画面を図 2 の(1)に示す．



(1) 初期画面

(2) 暗号化完了画面

図 2　共通鍵モード送信者側のスクリーンショット

図 2 の(1)の画面上部にはテキストフィールド（以下，内容記述フィールドと記述）があり，ここに送信者が発言する内容を入力する．画面中央には，人型ピクトグラムを表示し，文章を暗号化する上での注意点を示している．図 2 の(1)の画面下部には，発言内容を暗号化する際に用いる共通鍵のパスフレーズを入力する欄（以下，パスフレーズ入力欄と記述）を表示する．初回アクセス時にはあらかじめランダムな値を自動入力し，Web ブラウザのローカルストレージに半永続的に保存する．利用者が任意のパスフレーズに変更する場合は，パスフレーズ入力欄に任意のフレーズを入力し，パスフレーズ入力欄の右にある更新ボタンを押すことで変更できる．内容記述フィールドの右に「Let's Boucho」と記したボタンを配置した．発言内容と共通鍵のパスフレーズを入力した後に「Let's Boucho」ボタンを押下すると次のような URL を生成する．

https://pictogramming.org/apps/boucho/?sent=XXXXXXXXXX

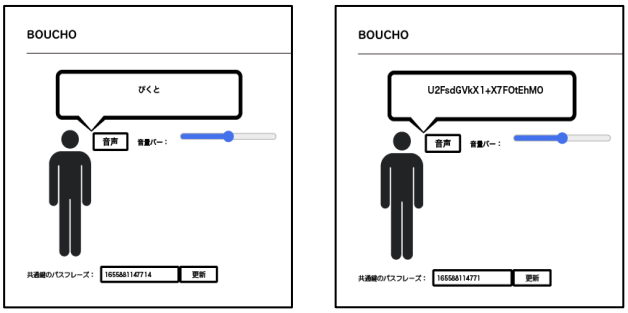
URL 中の XXXXXX は，暗号化通信を行うための JavaScript ライブラリである crypto-js に含まれるモジュールの 1 つで，共通鍵暗号通信を実現する AES 暗号のアルゴリズムを用いて暗号化した文字列を URI エンコードすることで生成したものである．すなわち送信者の発言内容を暗号化した文字列を，URL に乗せて受信者に共有する．これにより，URL を通して発言内容を送信できるが，URL を見ただけでは平文の内容を予測することができない．共通鍵パスフレーズを知らなければ，平文に復号することができないため，URL の盗聴によって発言内容の閲覧を防ぐことが可能になる．また生成した URL を元に QR コードを自動作成し，図 2 の(2)に示すように，画面中央に

表示する．この QR コードは他者が読み込むことで，URL を入力する手間を省く．以降 URL の共有は QR コードを使用することを前提とする．URL を受け渡しする際に，第三者が内容フィールド内の発言内容を盗み見する可能性があり，これを防ぐために「Let's Boucho」ボタンを押すと同時に内容記述フィールドを非表示にする．

2.3.2. 受信者による暗号文の復号

受信者が，送信者の QR コードを読み取りブラウザ上で「BOUCHO」のページにアクセスした際に表示する画面を図 3 に示す．

送信者と受信者の共通鍵が一致している場合は，図 3 の(1)のように画面中央部のピクトグラムの吹き出しに平文を表示するが，受信者の共通鍵が送信者の共通鍵と異なる場合は，図 3 の(2)のように暗号文が復号されずに暗号文のまま表示する．なお，暗号文を表示する際には画面レイアウトの都合上，全文を表示するのではなく，一部を切り取って表示している．一度目のアクセスで復号に失敗したとしても，正しい共通鍵パスフレーズを入力し直し，更新ボタンを押すことで，再度アクセスすることなく復号できる．以上より，共通鍵による暗号文の復号には，送信者から共通鍵を教えてもらう必要があることに加え，悪意のある第三者に共通鍵を知られてしまうと文章を盗聴される可能性がある．そのため，共通鍵モードでは共通鍵の仕組みだけでなく，鍵の配送問題も体験できる．



(1) 復号成功　　(2) 復号失敗

図 3　共通鍵モード受信者側のスクリーンショット

2.4. 公開鍵モード

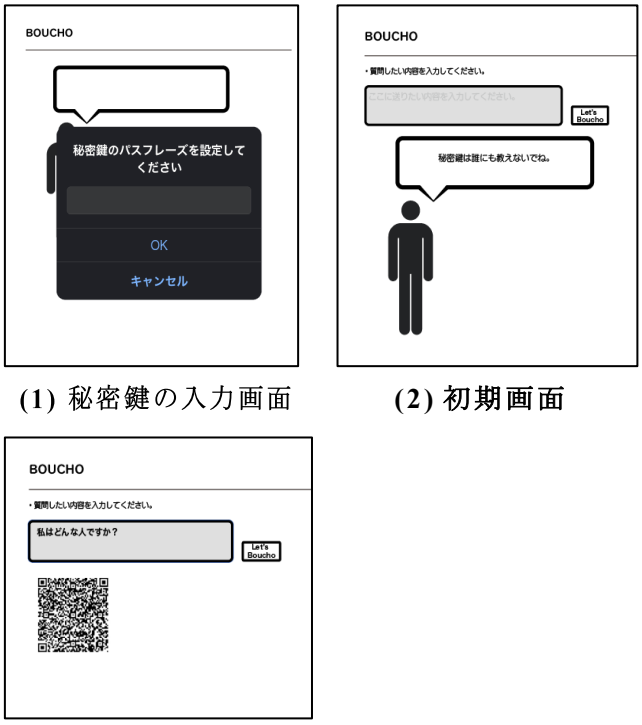
公開鍵モードは質問者が設定した秘密鍵パスフレーズにより生成された公開鍵を質問文に加えて回答者に配布し，回答者がその公開鍵で回答を暗号化する．公開鍵で暗号化した暗号分は秘密鍵以外では復号不可能であるため，秘密鍵を知る質問者のみが回答を閲覧できる機能である．

公開鍵モードは回答者に質問文を投げかける質問者とその質問に回答する回答者が必要である．質問者と回答者それぞれの手順の概略を示す．

手順 1 質問者による秘密鍵の設定及び質問文の作成
手順 2 回答者による回答文の暗号化
手順 3 質問者による暗号文の復号

次にそれぞれの手順における詳細について 2.4.1～2.4.3 項で解説する

2.4.1. 質問者による秘密鍵の設定及び質問文の作成



(1) 秘密鍵の入力画面　　(2) 初期画面

(3) 質問文受け渡し画面

図 4　公開鍵モード質問者側のスクリーンショットその 1

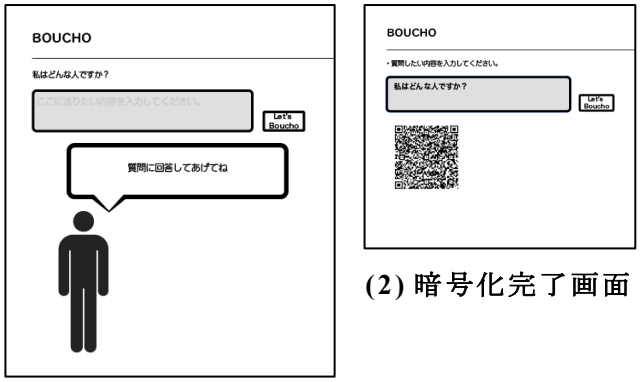
質問者は，公開鍵モードへの初回アクセス時には図 4 の(1)のように秘密鍵暗号のパスフレーズの入力を促すポップアップを表示する．入力された秘密鍵パスフレーズは共通鍵と同じく，Web ブラウザのローカルストレージに半永続的に保存する．質問者が秘密鍵パスフレーズを入力すると図 4 の(2)の画面を表示する．画面上部には共通鍵モードと同様に内容記述フィールドを配置しており，ここに質問文を入力する．画面中央部にはピクトグラムを配置し，秘密鍵の取り扱いに対する注意を述べている．秘密鍵を一度決定すると，秘密鍵の変更は原則不可能にしている．これは任意のタイミングで鍵を変更可能な共通鍵モードとは異なる点である．これは，共通鍵暗号方式では特定の

共通鍵を知る全ての人が暗号文を復号可能であるため，複数の相手に対して同じ共通鍵を用いるのではなく相手ごとに鍵を分けなければならないという性質があることに対して，公開鍵暗号方式における暗号文の復号は，秘密鍵を用いてのみ可能で，その秘密鍵は質問者以外に公開することは不要だからである．内容記述フィールドに文章を入力し，「Let's BOUCHO」ボタンを押下すると，次のようなURLを生成する．

http://pictogramming.org/apps/boucho/?mode=question&sent=XXXXXXXXXXX&openKey=XXXXXXXXXX

URL内のopenKey属性に与えられている文字列は，公開鍵暗号方式のうちのRSAアルゴリズムを用いて暗号化するために必要となる公開鍵であり，この公開鍵は質問者が入力した秘密鍵パラフレーズから生成したものである．このURLを元にQRコードを自動作成し，図4の(3)に示すように画面中央部に表示する．このQRコードを質問回答者に読み込ませることで，URLを取得させ，質問内容に加えて，回答内容を暗号化するための公開鍵を渡すことができる．

2.4.2. 回答者による回答分の暗号化



(1) 回答画面　　(2) 暗号化完了画面

図5　公開鍵モード回答者側のスクリーンショット

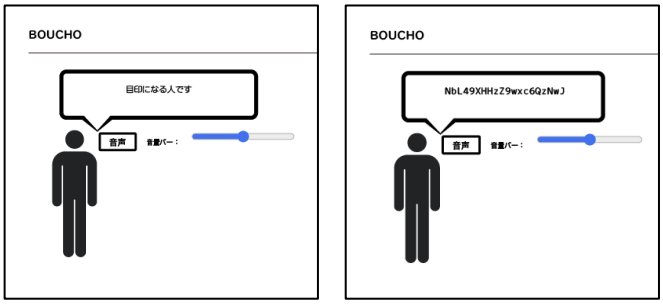
質問者が発行したQRコードを読みとると，端末は図5の(1)で示すようにブラウザ上で「BOUCHO」のページにアクセスする．内容記述フィールドの上部には質問者による質問内容が表示され，回答者はその質問に対する回答を内容記述フィールドに入力することになる．「Let's Boucho」のボタンを押すと，質問者から受け取ったクエリパラメータから抽出した質問者の公開鍵を用いて文章を暗号化し，以下のようなURLが生成される．

https://pictogramming.org/apps/boucho/?mode=rsaResult&sentence=XXXXXXXXXXXX

URLのsentence属性は，回答者の文章を質問者の公開鍵を用いて暗号化した暗号文である．このURLを元にQRコードが作成され，図5の(2)のように画面中央部に表示される．このQRコードを質問者に読み込ませることで，質問者に回答を渡すことができる．URLを受け渡しする際に，第三者が内容フィールドに記された発言内容を盗み見する可能性があり，これを防ぐため「Let's Boucho」ボタンを押すと同時に内容記述フィールド全体を非表示にする．

2.4.3. 質問者による暗号文の復号

回答者の画面に表示されたQRコードを読み取ると，図6の(1)のような形で「BOUCHO」のサイトにアクセスできる．質問文を作成した時と同じ端末でアクセスすると，秘密鍵がブラウザに保存されているため，回答の暗号文を復号した平文が画面中央のピクトグラムの発言として表示する．一方，質問文を作成した時とは異なる端末でアクセスし，暗号化時点とは異なる秘密鍵を設定すると，暗号文を復号できず，図6の(2)のように，暗号文のまま画面上のピクトグラムの発言として表示する．なお，暗号文を表示する際には画面レイアウトの都合上，全文を表示するのではなく，一部を切り取って表示している．



(1) 復号成功　　(2) 復号失敗

図6　公開鍵モード質問者側のスクリーンショットその2

3. 実践・評価

3.1. 概要

2022年7月8日（金曜日），青山学院大学社会情報学部の一年次における必履修科目である「情報科学概論」の受講者67名を対象に「BOUCHO」を用いた実習を行った．この講義は，受講者全体を3クラスに分けて実施されており，そのうちの1クラスで「BOUCHO」を用いた．67名は，「BOUCHO」を用

いた実習を行ったクラスに当日出席していた人数である．実習後に，鍵暗号方式に対する理解を図るためのアンケートを実施し，受講者からの回答を得た．

3.2. アプリケーションの実践

「BOUCHO」を用いた実習を実施した環境は，学生一人に対して一台の PC が配当されており，2 つの PC の間には，講師が使用する PC の画面を表示するモニタ（以下，中間モニタと記述）が配置されている PC 実習室である．講義時間は 90 分である．講師による共通鍵暗号方式と公開鍵暗号方式に関する導入講義を約 30 分間行った後に共通鍵モード，公開鍵モードの順に「BOUCHO」を使用した．次に，それぞれのモードにおける運用時の実習手順を説明する．

3.2.1. 共通鍵モードの使用

講義開始前までに，講師は 2.3.1 項に示した方法に沿って，共通鍵パスフレーズで文章の暗号化を行い，共通鍵モードの暗号化完了画面（図 2 の 2）にある QR コードを準備した．「BOUCHO」実習時に中間モニタに QR コードを表示した．学生が中間モニタの QR コードよりスマートフォンで「BOUCHO」にアクセスすると，画面上には復号失敗画面（図 3 の 2）を表示した．その後，講師が共通鍵パスフレーズを学生に共有し，学生が正しいパスフレーズを入力することで，復号成功画面（図 3 の 1）を表示した．次に，学生に教室の PC で共通鍵モード初期画面（図 2 の 1）にアクセスさせた．2.3.1 項の方法で文章の暗号化を行い，PC の画面に QR コードを表示させた．中間モニタを挟んだ隣の席の人の QR コードを，スマートフォンを用いて読み取らせ，互いに設定した共通鍵パスフレーズを教えさせた．2.3.2 項の方法で復号させた．

3.2.2. 公開鍵モードの使用

講義開始までに，講師は 2.4.1 項に示した方法に沿って，秘密鍵パスフレーズと，質問文を入力し，公開鍵モードの質問文受け渡し画面（図 4 の 3）の QR コードを準備した．「BOUCHO」実習時に中間モニタに QR コードを表示した．学生が中間モニタの QR コードよりスマートフォンで「BOUCH」O にアクセスすると，回答画面（図 5 の 1）を表示し，2.4.2 項の方法で回答を暗号化して QR コードを画面上に表示させた．講師が学生の画面に表示させた QR コードを読み取って周り，学生の回答を閲覧した．

3.3. アンケート評価

アンケートの質問項目は表 1 に示す 4 項目である．用意した質問は，いずれも単一回答選択肢を用意しており，選択肢の内容は「はい」,「いいえ」とした．66 名より回答があった．回答結果を表 2 に示す．

質問 1 のアンケート結果から，約 96%の履修者が，共通鍵モードで，相手から入手した共通鍵パスフレーズを用いて暗号文を復号できたと回答している．このことから，共通鍵暗号方式は，通信する二者間で同一の鍵を用いているということの理解を促す可能性が考えられる．

質問 2 のアンケート結果から，約 85%の履修者が，質問者の公開鍵で回答を暗号できたと回答した．この結果から，本アプリケーションを利用することで，公開鍵暗号方式では暗号文を受け取る側の公開鍵を用いて暗号化を行うということの理解を促す可能性が考えられる．

質問 3 のアンケート結果から，97%の履修者が，質問者の秘密鍵で回答者から受け取った暗号文を復号できたと回答した．この結果から，本アプリケーションを利用することで，公開鍵暗号方式では暗号文を受け取る側の秘密鍵を用いて復号を行うということの理解を促す可能性が考えられる．

質問 4 のアンケート結果では，質問の回答者全員が，「BOUCHO」が鍵暗号方式への理解の手助けになったと回答している．本稿の冒頭で記述したように，鍵暗号方式は講義形式で理解するのが難しいという特徴がある．一方で，質問 4 への回答から，「BOUCHO」は鍵暗号方式の理解を促進することが分かったため，鍵暗号方式における学習支援ツールとして使用できる可能性が考えられる．

表 1　アンケート内容

質問	内容	回答形式
1	共通鍵モードで，共通鍵パスフレーズを送信者より伝えられた後に，復号できた．	単一回答選択
2	公開鍵モードで，質問者の質問に対する回答を質問者の公開鍵で暗号化できた．	単一回答選択
3	公開鍵モードで，質問者の公開鍵を用いて暗号化した暗号文は，質問者の秘密鍵を用いることで復号できた．	単一回答選択
4	「BOUCHO」が，鍵暗号方式の理解の手助けとなった．	単一回答選択

表 2　アンケートの回答結果

質問	はい	いいえ
1	0.955	0.045
2	0.848	0.152
3	0.970	0.030
4	1.000	0.000

4. 終わりに

鍵暗号方式は情報セキュリティの分野において重要な項目である．しかし，難解な数学的要素が含まれているため，学習するのが難しい．そこで，本稿では，スマートデバイスを用いて，鍵暗号方式を体験的に学習できるアプリケーションの紹介と評価を行った．学生の「BOUCHO」に対する反応は好評であった．そのため，「BOUCHO」は学生が鍵暗号方式の理解を深めることに役立つ可能性があることがわかった．しかし，今回行ったアンケートでは，それぞれの項目に対して用意した選択肢が，二つであったため，評価が十分に厳密であったとは言えない．今後は，具体的な評価項目や，選択肢を用いたアンケートを実施することで，「BOUCHO」がどの程度，学生の鍵暗号方式に対する理解の促進に貢献したかをより厳密に評価したい．

謝辞

本研究は JSPS 科研費 21H03560 の助成を受けたものです．

参 考 文 献

[1] 田中一郎，鈴木二郎，“ウエブとデータベース”，DEWS 2008.

[2] I. Tanaka and J. Suzuki, “Web and Database Technologies”, Proc. of ACM SIGMOD, pp. 10-22, 2010.