通信の暗号化・復号および公開鍵暗号基盤の Web 学習教材の改良と評価

田中 凌　　中西 通雄
Ryo TANAKA　　Michio NAKANISHI
大阪工業大学情報科学部コンピュータ科学科
Department of Computer Science, Faculty of Information Science and Technology
Osaka Institute of Technology
Email: naka@is.oit.ac.jp

あらまし：高校の情報の科目「情報の科学」には，暗号化通信の学習項目が含まれている．しかし，教科書での扱いは 4 ページ程度であり，暗号化通信は目に見えにくいので，図や解説だけでは学習者にとって理解しづらい．本研究室では，昨年度に初学者向けの暗号化通信の Web 教材が開発された．本研究では，昨年度の研究の問題点を解決し，PKI 体験ページと RSA 暗号の鍵ペア生成体験ページの追加と，インタフェースの改良を行った．

キーワード：暗号化，復号，PKI，Web 教材

1. はじめに

高等学校の情報科目「情報の科学」には暗号化通信の学習項目が含まれている．しかし，教科書の扱いは 4 ページ程度と少なく[1]，暗号化通信はコンピュータ内部の処理であるので人間の目では見えにくい．よって，初学者にとって図や解説だけでは暗号化通信の過程を理解しづらい．本研究室では，2014 年度に初学者向けの暗号化通信の Web 教材が開発され[2]，さらに 2015 年度にアニメーションと SSL/TLS の項目の追加などの改良が行われた[3]．

しかし，2015 年度の教材では，PKI の体験は SSL/TLS 体験ページでまとめられたため，どの部分が PKI かわかりにくかった．また，操作方法を見る場合，別ウィンドウで開く必要があるので不便であった．したがって，今年度の研究では，これらの問題点を改善することを目標とした．昨年度の研究との違いは，次の 5 点である．

(a) PKI 体験ページと HTTPS 学習ページ追加
(b) RSA 暗号（鍵ペア生成）体験ページ追加
(c) 各体験ページに操作手順の説明文追加
(d) Bootstrap の実装とインタフェースの改良

2. 利用者インタフェース

開発言語は HTML，JavaScript，CSS である．開発行数は，昨年度の研究で作成されたものから約 150 行程度の JavaScript を修正のうえ再利用し，新たに 2300 行程度追加して合計 2450 行程度である．本教材は Web ブラウザ上で動作し，インターネットの接続は不要である．

本教材は学習ページと体験ページから構成されている．暗号化通信の項目は「共通鍵暗号」，「公開鍵暗号」，「ディジタル署名」，「PKI」，「SSL/TLS」の 5 項目である．順番は学習ページから体験ページに進む．また，体験ページの操作すべき箇所の説明文を赤く表示するようにした．

2.1 学習ページ

学習ページでは，暗号化・復号の過程や各暗号化通信の役割について図や文章を用いて解説する．

2.2 体験ページ

体験ページでは，「共通鍵暗号」，「公開鍵暗号」，「RSA 暗号（鍵ペア生成）」，「ディジタル署名」，「PKI」，「SSL/TLS」の疑似的な体験をすることができる．「共通鍵暗号」と「公開鍵暗号」（図 1）は，共通鍵暗号および公開鍵暗号の暗号化・復号の過程を体験できる．公開鍵暗号体験ページでは，今年度から鍵入力において，受信者の公開鍵と秘密鍵の値を入力するようにした．

図 1　公開鍵体験ページ

「RSA 暗号（鍵ペア生成）」（図 2）は，RSA 暗号における公開鍵と秘密鍵の生成の過程を体験できる．RSA 暗号（鍵ペア生成）ページでは，素数を入力し，それぞれ計算することで公開鍵と秘密鍵の値と鍵アイコンを生成するようにした．

図 2　RSA 暗号（鍵ペア生成）体験ページ

「ディジタル署名」では，ディジタル署名におけるデータの改ざんの検知の過程を体験できる．今年度追加した「PKI」（図 3）では，公開鍵証明書を発行し，公開鍵は本人のものであるか証明する過程を体験できる．「SSL/TLS」（図 4）では，SSL/TLS を用いた HTTPS 通信の過程を体験できる．今年度から HTTPS 通信を再現するために，サーバ接続要求ボタンの追加を行った．

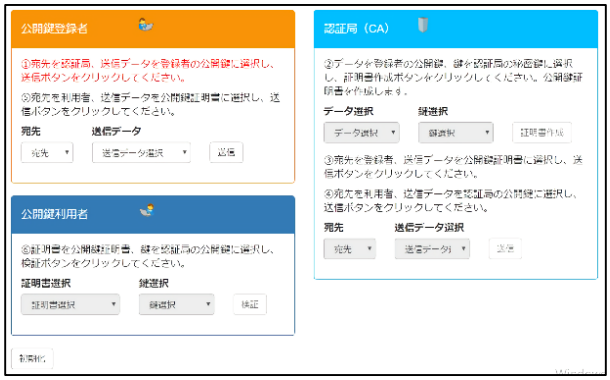

図 3　PKI 体験ページ

図 4　SSL/TLS 体験ページ

3.　評価

暗号化通信の知識がない文系大学生 5 人に評価を実施した．本教材使用前に全 8 問の理解度テスト，使用後に全 12 問の理解度テストとアンケート（4 段階評価と自由記述）を行った．

理解度テストは「共通鍵暗号」,「公開鍵暗号」,「ディジタル署名」,「PKI」,「SSL/TLS」に関する選択肢問題である．

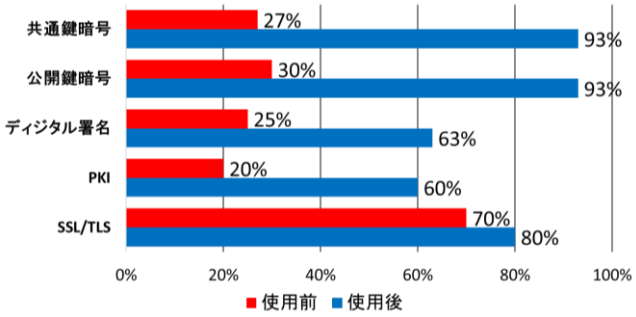

図 5　使用前と使用後の平均正答率

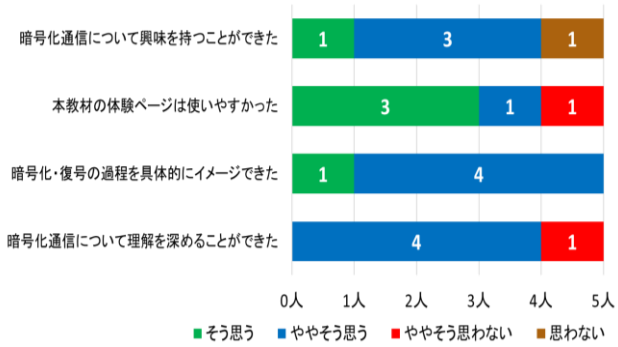

図 6　4 段階評価結果

図 5 に示した本教材の使用前と使用後の平均正答率を見ると，特に「共通鍵暗号」と「公開鍵暗号」では，使用後の平均正答率が 93%まで大きく伸びている．このことから，一定以上暗号化・復号の過程の理解を深める効果があったと考えられる．

図 6 に示した 4 段階評価の結果を見ると，特に「暗号化・復号の過程を具体的にイメージできた」の項目では，被験者全員「そう思う」,「ややそう思う」と答えた．このことから，本教材によって暗号化・復号の具体的なイメージをすることができたと考えられる．

また，自由記述では，良い点について「体験ページで操作できるので，理解が深まりやすい」,「パソコンで学べる」などの意見を得た．一方，改善してほしい点について「専門用語が難しい」という意見があった．これは，学習ページでは図と解説を見るだけなので，専門用語を理解できなかったことが考えられる．

4.　今後の課題

学習ページは解説と図を見るだけであるので，復習できるように，学習ページと体験ページの間に確認問題ページを追加する．確認問題ページでは，一定以上の点数を取れば体験ページに進めるようにする．これによって，専門用語の意味を理解した上で体験ページに進めると考えられる．

謝辞

本研究の一部は JSPS 科研費 JP26350327 の助成を受けた．

参考文献

(1) 岡本敏雄，山極隆，「最新情報の科学」，実教出版株式会社（2014）
(2) 吉本健司,「暗号化通信を学ぶための暗号化と復号の過程を可視化した Web 教材」，大阪工業大学情報科学部コンピュータ科学科，卒業論文（2014）
(3) 篤田直樹,「共通鍵と公開鍵の原理およびディジタル署名と公開鍵基盤のしくみの学習教材」，大阪工業大学情報科学部コンピュータ科学科，卒業論文（2015）