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

吉本　健司　　中西　通雄
Kenji YOSHIMOTO　　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、暗号化通信が学習項目に含まれているが、教科書での扱いはせいぜい 4 ページほどである。そこで、本研究では、学習者がコンピュータ上で実際に暗号化および復号をためしたり、公開鍵の長さによって秘密鍵を見つけるのにどの程度時間がかかるかを体験できるように、教材を作成した。この教材は JavaScript で作成してあるため、Web ブラウザ環境があれば使うことができる。
キーワード：暗号化，RSA 暗号，復号，Web 教材

1.　はじめに

高校の情報の科目「情報の科学」には、暗号化通信が学習項目に含まれているが、教科書での扱いは共通鍵暗号と公開鍵暗号をあわせてもせいぜい 4 ページ程度である(1)。本研究では、学習者がコンピュータ上で実際に暗号化および復号をためしたり、公開鍵の長さによって秘密鍵を見つけるのにどの程度時間がかかるかを体験できるように、教材を作成した。この教材は JavaScript で作成してあるため、自分の PC に置くことで Web ブラウザから使うことができる。また、本教材で扱う公開鍵暗号はすべて RSA 暗号を使用している。

2.　本 Web 教材について

本教材は、体験ページと学習ページで構成している。高校の情報の科目「情報の科学」を受講している高校生を対象としている。

2.1　学習ページ

学習ページは、暗号化通信の教材として使用するため、暗号化通信について図や文章を使用して解説を行っている。

2.2　体験ページ

体験ページには、「共通鍵暗号体験」「公開鍵暗号体験」「ディジタル署名体験」「公開鍵暗号解読」の 4 つのページがある。

「共通鍵暗号体験」「公開鍵暗号体験」ページでは、それぞれ暗号化と復号の体験を行う。「共通鍵暗号体験」では、シーザー暗号方式を使用した暗号化と復号を行う。図 1 は、暗号化した状態の共通鍵暗号体験のページである。

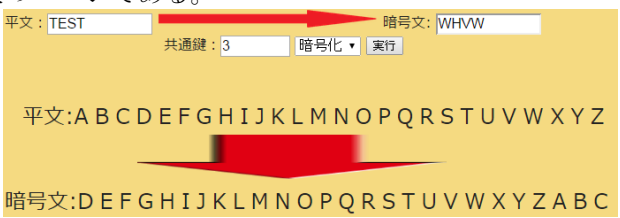

図 1　共通鍵暗号体験画面

「公開鍵暗号体験」では、平文を入力して暗号化と復号を行う。図 2 は、公開鍵暗号体験のページである。一文字ずつ暗号化と復号の計算過程と、平文と暗号文の関係を表に示している。また、図 2 に示すように、計算式や表では、平文は橙色、暗号文は水色、公開鍵の指数は黄色、公開鍵の係数と秘密鍵の係数は緑、秘密鍵の指数は紫というように表示色を統一しており、色で種類を見分けやすくしている。

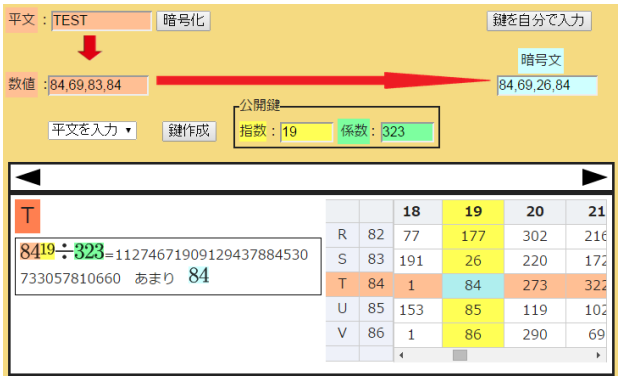

図 2　公開鍵暗号体験画面

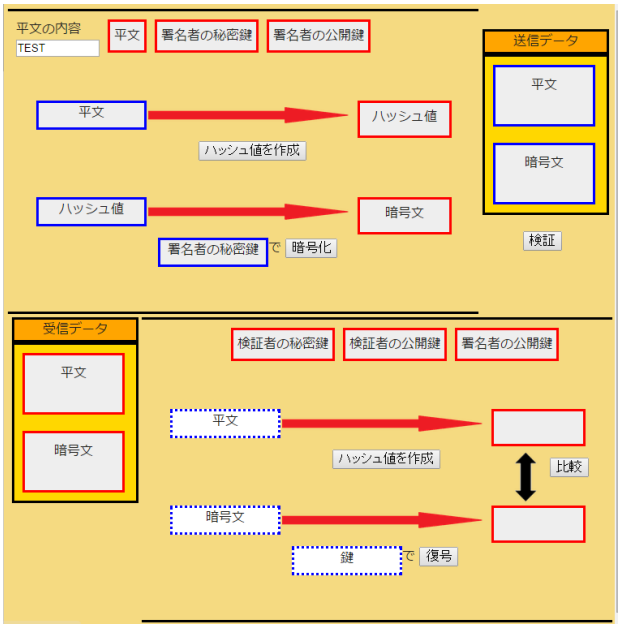

図 3 ディジタル署名体験画面

「ディジタル署名体験」では、ハッシュ化と暗号化を利用し、証明者が送信するデータの作成を行い、

またはハッシュ化と復号を利用して、受信したデータの検証を行う。実際にハッシュ化や暗号化を行うことができ、平文の値の違いによってハッシュ値や暗号文がどのように変化するのかを体験することができる。

「公開鍵暗号解読」では、2 から順に公開鍵の係数を素数で割っていき二つの素数を見つけ、見つけ出した素数と公開鍵の指数から秘密鍵を割り出す。公開鍵の係数の長さによって計算量が増えて解読にかかる時間が変化することを､学習者は体験できる。公開鍵の長さを 8～14 桁の中から選択、または手動で公開鍵を入力することができる。

3. 評価

本学部 1 年生 2 名と 4 年生 3 名に、本教材の学習ページで暗号化通信を学習してもらった後、理解度テストを実施した。結果を図 4 に示す。

理解度テストの問題は、図 4 に示したそれぞれの項目の仕組みについて、正しく説明しているものを 4 つの選択肢から選ぶものである。全部で 6 問であるが、ここではそのうち 2 つを表 1 に示す。

表 1　理解度テスト問題

問：公開鍵暗号について説明しているものを選択してください。 ・鍵をすべて公開している ・鍵をすべて誰にも知られないように保管する。 ・暗号化した鍵で復号もすることができる。 ・暗号化と復号で違う鍵を使用する。
問：PKI について説明しているものを選択してください。 ・公開鍵の本人性を保証する技術である。 ・認証局が発行した証明書には秘密鍵が含まれている ・公開鍵を作成する技術である。 ・公開鍵を安全に相手へ送信する技術である。

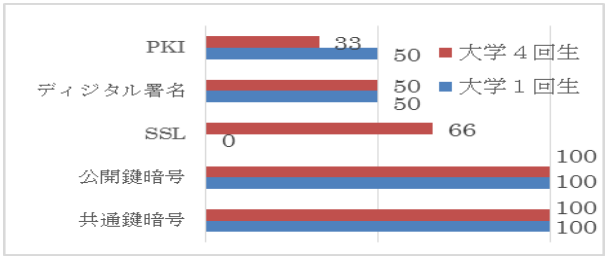

図 4　理解度テスト結果

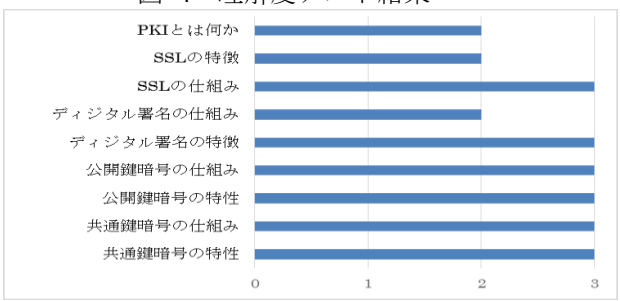

図 5　アンケート結果（4 回生）

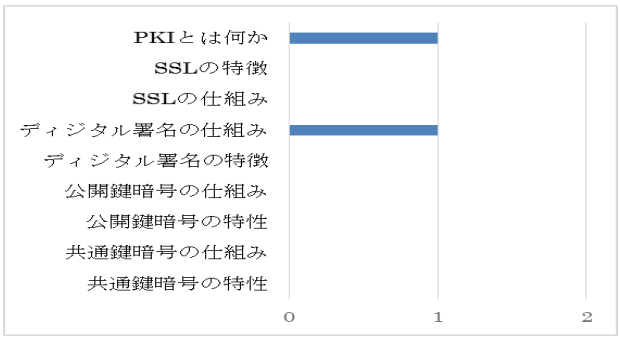

図 6　アンケート結果（1 回生）

図 4 に理解度テスト結果を正解率（パーセント）を、図 5 と 6 に各項目ごとに理解できたと感じたと答えた人数を示す。

図 4 より、体験ページを作成した項目と作成しなかった項目では、全体の正解率では体験ページを作成した項目のほうが高かった。4 回生は体験ページを作成した項目（共通鍵暗号，公開鍵暗号，ディジタル署名）に関してはすべて理解できたと回答していたが、1 回生が理解できたと回答した項目は、ディジタル署名の仕組みのみであった。

また、共通鍵や公開鍵の体験ページでは、興味をもって体験ページを利用する学習者が少ない結果となった。ディジタル署名の体験ページでは、全員が一度は署名作成に失敗してから、教材を確認していた。つまり学習ページ部分をあまり読まずに先に進むことを急いだ結果と考えられる。1 回生 2 人のうち 1 人はディジタル署名の仕組みを理解できたと回答したが、公開鍵を解読するページでも、1 回生に関心を寄せる結果とはならなかった。しかし、公開鍵の解読時間については、パソコンのスペックの違い、ブラウザの種類によって大きな差がうまれる点に興味を抱く学習者もいた。

4. 今後の課題

理解度テストの結果では体験ページがある項目のほうが正解率が高かったため、PKI や SSL の体験ページの作成が必要である。また、学習者の反応の中にディジタル署名体験ページを利用する際に学習ページに立ち戻る動きがあったことから、共通鍵や公開鍵など各項目に、ディジタル署名体験ページのような問題形式のページを作成する必要がある。また、教材として利用した学習ページでは、それぞれの内容を 1 ページにまとめていたが、体験ページと同じ項目で学習ページを作成してほしいとの意見もあり、検討する必要がある。

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,平成 26 年 1 月 25 日発行
(2) 齋藤孝道：「マスタリング TCP/IP 情報セキュリティ編」平成 25 年 9 月 1 日発行