ＣＳアンプラグドを目指した公開鍵暗号の授業

野部緑[†]

教科「情報」の情報セキュリティ分野の内容のひとつとして、情報の暗号化がある。南京錠を利用し、理解しにくい公開鍵や秘密鍵について授業を行った。

1. はじめに

本校では、単位制であり情報Ａ、情報Ｂ、情報Ｃの全ての科目を設置している。どれかを選択という形ではなく、すべての科目を選択することが可能である。そのため、差別化を図り、情報Ｂでは情報の科学的理解について、ＣＳアンプラグドを利用した実践を行ってきた。

今回は、このＣＳアンプラグドの考え方を生かして、公開鍵暗号方式について、アンプラグド風に教具を利用して授業をおこなった。

その授業について報告する。

2. 授業実践の内容

2.1 目的

高等学校の情報では、さまざまな分野を取り扱っている。情報モラル等という名称でくくられているが、情報セキュリティに関する内容も多い。

携帯電話の利用で、電子メールやWebの利用については以前より身近になっている。が、しかし、情報のセキュリティについては、自分とは関係がないと考えている生徒が多い。教科書で扱っている内容は多岐にわたっているが、そのなかで「暗号化の技術」における暗号と、共通鍵暗号方式、公開鍵暗号方式についての理解を深めるのが本授業の目的である。

なお、仕組みの理解が目的であるので、実際の方式であるとか数字の生成といったところまでは触れていない。

2.2 準備

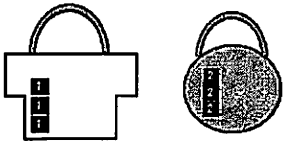
授業において利用したものは、以下教具である。

・鍵であける方式の南京錠（【共通鍵暗号方式用】

ただし、今回の発表においては、改良型としてダイヤル式南京錠を使用する。この南京錠は、設定した数字の組み合わせでなければ錠をかけることができないタイプである。（本文では、南京錠１とする）

・ダイヤル式南京錠（公開鍵暗号方式用）

設定した番号以外でも、錠をかけることができる。これを公開鍵とする。（本文では南京錠２とする）



秘密鍵は、設定した鍵の番号がかかれた用紙。

２人分（仮にＡさん、Ｂさん）の公開鍵（数個）と秘密鍵を用意する。

・暗号化するイメージで鍵をかけてメールをいれる箱（キャンディーポット）など。

2.3 授業の構成

「情報の暗号化」についての授業は２時間（50分×2）、そのうち、最初の時間は暗号そのものについての授業を行った。この内容は、何のために暗号にするかという話を、シーザー暗号、換字暗号、転置暗号などの紹介である。

教具を用いた授業は２限目に実際に利用されている例として、共通鍵暗号方式と公開鍵についての授業を行った。

使用した教科書は、日本文教出版の「情報Ｂ」[(1)]である。公開鍵の仕組みについては、「最新情報トピック集　第２版」[(2)]を参考にした。

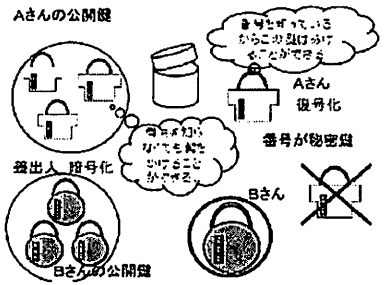
(1) 共通鍵暗号方式

① 生徒から、送信者と受信者を選ぶ
② 送信者の生徒は、何か文字の書かれた紙を箱にいれて、南京錠１で施錠する。このとき、送信者は鍵の番号を知っている。
③ 受信者やそのほかの生徒にこの箱を渡し、あけることを試みる。
④ 番号（鍵）がわからないと開けることができない、ということから、秘密はまもられるが、受信者に番号を教える必要があることを気づかせる。
⑤ 実際に、受け渡しをおこなう。このとき、途中で他の生徒がこの番号を見て、箱を開けることで、共通鍵暗号方式の問題点に気づかせる
⑥ さらに、別の受信者におくるためには、同じ鍵で送ることができないこと、取引が多いと、多くの鍵が必要になることも気付かせる、

† 大阪府立桃谷高等学校

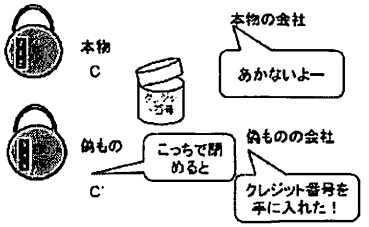
(2) 公開鍵暗号方式

① 送信者と受信者Aを選ぶ。受信者Aは自分の秘密鍵（番号のカード）を持っている。また、自分の公開鍵をインターネット上（授業では公開鍵の場所をつくっておく）に置いておく。
② 送信者の生徒は、何か文字の書かれた紙を箱にいれて、Aさんの南京錠2で施錠する。このとき、送信者は鍵の番号を知らなくてもよい。
③ 受信者Aやその他の生徒に箱をわたし、あけることを試みる。
Aさん以外はあけることができず、Aさんは箱をあけることができることを確認。
④ さらに、別の送信者がAさんに手紙をおくる。
⑤ 受信者Aさんと送信者の間は、番号（秘密鍵）のやりとりをしなくてもよいことに気付かせる
⑥ 受信者Bさんを選び、同じことを行う。このとき、Aさんもこれをあけることができないことを確認する。
⑦ これらから、共通鍵暗号方式と公開鍵暗号方式についての違いを考えさせる。



(3) 公開鍵暗号方式の発展。(認証機関)

⑧ 受信者Cを会社として、クレジット番号を送信するケースを考える。
⑨ 公開鍵として、本物Cと偽物C'を用意して、間違えてC‘を使うとどうなるかを考えさせる。



3. まとめ

3.1 生徒の感想

授業に参加した生徒が少ないのと、2 時間連続での感想のため、この授業についての感想そのものは少ないが、以下に列挙する。

・セキュリティって大事ですね。
・暗号っていろいろ考えられていますね
・難しかった、もう少し時間が欲しかった
・教科書だと全然わからんかったけれどこれやったらわかった
（シスアドの勉強をしていた生徒）

3.2 理解度

シスアドの勉強をしていた生徒が、これでわかったという感想があったように、「公開鍵」「秘密鍵」という単語をしっている生徒にとっては、理解が深まったと考えられる。

しかし、授業においては、公開鍵や秘密鍵をいう単語は口頭で伝えただけであったので、まず、単語が理解できていない生徒もおり、そこが難しいという感想につながったと考えられる。

また、認証機関の大切さというのは、伝わったと考えてもよいだろう。

3.3 今後の改良点について

・「公開鍵」「秘密鍵」という単語を伝えるために、番号を書いた紙の表や、南京錠に工夫をする。
・教室の中での授業であると、電子メールは離れた場所に送ることが伝わりにくい。ルーターの役目をする生徒を作るなどの工夫をしてもよいかもしれない。

参考文献

(1) 水越敏行，村井純，ほか25 名：新・情報B 探求する楽しさ，日本文教出版，平成18 年
(2) 久野靖，辰己丈夫，佐藤義弘，他：情報最新トピック集　第2版　高校版，p89，日経BP社，2008 年12 月