付録Q

「ペルーのコイン投げー暗号プロトコル」の学習

1. 学習活動

- コイン投げをする。
- 離れたところでコイン投げをする。

2. 準備物

- コイン
- アルバイト情報誌（同じもので厚みがあるもの）２冊

3. 実習１ コイン投げ

1. 亜由美と一郎は近くにいる。亜由美がコイン投げをして、一郎が当てる。
2. 亜由美と一郎の距離は離れている。

一郎がコイン投げをして、亜由美が当てる。一郎はインチキをしているかもしれない。答えは信用できるか。電話でコイン投げは可能か。

4. 実習２ アルバイト情報誌でコイン投げ

1. アルバイト情報誌を亜由美と一郎がそれぞれ持ち、離れたところに立つ。[*1]
2. 一郎がアルバイト情報誌の中から求人先を１つ選び、電話番号を亜由美に伝える。
3. 亜由美は求人先が載っているページの番号が偶数であるか奇数であるかを予想し一郎に伝える。
4. 一郎はページ番号を亜由美に伝える。
5. 亜由美は伝えられたページに、求人先の電話番号があることを確認する。

5. フォローアップディスカッション

- 亜由美は正答を見破って返答することができるか．（見破るには「逆引き」をしなければならないから，一般には困難．でも，ちょっと頑張ればできるかもしれない．それを許さないためには，亜由美の返答に適切な時間制限を課せばよい．）
- 一郎はインチキをすることができるか，つまり，亜由美が返答した後に一郎が正答を変更することは可能か．（もし，同一業者が情報誌の２ヶ所に求人情報を載せていて，それがたまたま奇数ページと偶数ページで，さらに，その事実を一郎が事前に知っていれば，インチキが可能になる．つまり，インチキの可能

[*1] アルバイト情報誌は辞書や資料集などに置き換える。

性を厳格に排除するには，利用する一方向関数の単射性が必要.）

- 亜由美と一郎が同一のアルバイト情報誌を入手できない場合はどうすればよいか.（素因数分解を使ったプロトコルへの導入．素数や素因数分解という数学的原理は不変なので，事前に情報を共有しておく必要がない）