2018/07/03

阿部　希駿

卒業研究

1 緒言

文部科学省が発表した国際学力調査によると世界の中でも日本の学力は上位にある．しかし日本の学生の学力は二極化していると言われ，問題点は多い．二極化の下の山の学生は学習内容の一部がわからないのではなく，「何をしているのかがわからない」「どこがわからないのかもわからない」などという根本的な原因があると推測している．

また各塾の調査では中学，高校で学習する科目の中で数学と英語は苦手になりやすいと言われている．この 2 科目の共通点として既に学習した知識を使うことを前提として授業を行う積み上げ型教科という点がある．積み上げ型教科では単元の内容が複雑になるほど必要な前提知識が多くなり，どの単元の内容が使われているかがわかりにくくなる．そのためその単元の内容を理解をすることが難しくなることが問題点としてあげられる．

そこで「学習する単元を前提知識とする単元の概要をあらかじめ説明することで，内容の理解を促進することができる」という仮説を立てた．この仮説では特に複数の単元の学習内容を用いて学習を行う単元で，用いる単元の内容などの具体的なイメージがしづらい場合を対象にする．本研究では，講義にて学生を対象にして実験を行い，この仮説を検証することを目的とする．講義では「ブロックチェーン」を対象にする．学習の過程である「暗号」や「ハッシュ」の段階では計算などの学習がメインで目的がわかりづらいが，「ブロックチェーン」では

2 教科の特性

学校で学習する教科には独立型教科と積み上げ型教科に分かれ，それぞれ下図のように積み木のような図で表される．

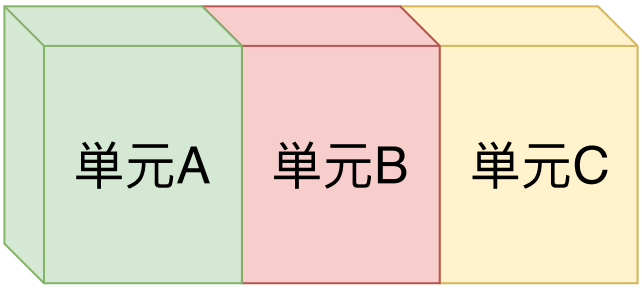

図 1　独立型教科の教育モデル

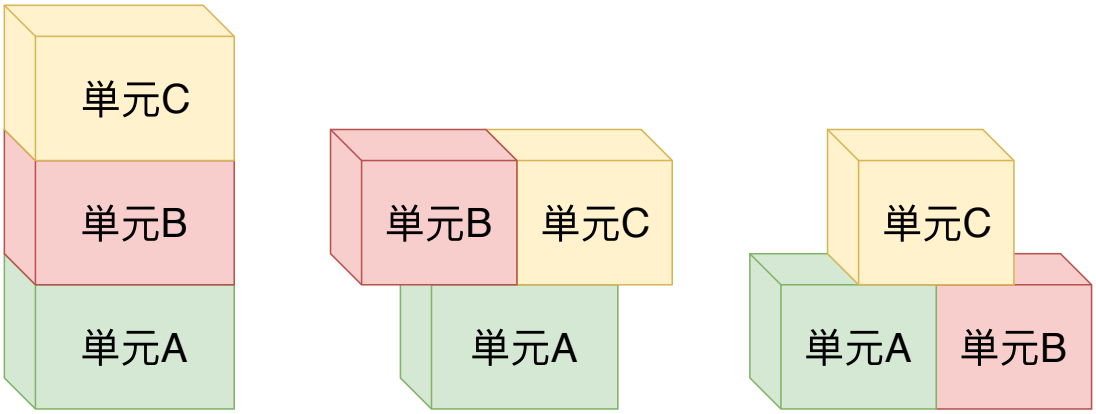

図 2　積み上げ型教科の教育モデル

2.1 独立型教科

独立型教科は国語や社会が該当する．独立型教科では図 3 のように各単元が独立していて関連性があまりないためどの単元から学習しても支障がない．

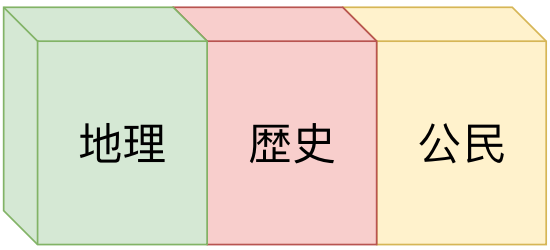

図 3　独立型教科の例

2.2 積み上げ型教科

積み上げ型教科では数学や英語が該当する．積み上げ型教科では図 4 のように学習した内容を次の学習の基礎知識として用いるため，順番に学習していくことになる．

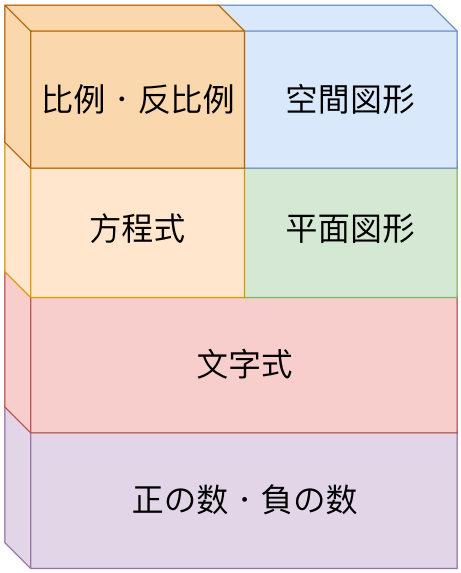

図 4　積み上げ型教科の例

3 暗号について

暗号とは通信を行う際，第三者にその内容を知られないようにするための手段である．元の文に一定の規則を用いて特定の変形を加えることを暗号化，暗号化する前の元の文を平文，暗号から平文に戻すことを復合化 (復号) と呼ぶ．暗号化する手段が暗号アルゴリズムであり，また暗号化や復号化に使うデータを鍵と呼ぶ．暗号は特性によって古典暗号と現代暗号に分かれる．アルゴリズムがわかれば解読が容易になる暗号を古典暗号，アルゴリズムは公開するが鍵を非公開にすれば安全な暗号を現代暗号という．

3.1 共通鍵暗号

暗号化と復号に同じ鍵を用いる暗号の方式である．通信相手に鍵を送り，その鍵を用いて情報を暗号化する．暗号化された情報が送られてきたら，同じ鍵を使って復号する．

図 5　共通鍵暗号通信の流れ

共通鍵暗号通信では暗号化と同じ鍵を使っているため，鍵を送る際に第三者に傍受される危険がある．また同じ鍵を複数のユーザーで使用すると，他のユーザーが復号する危険性があるため，ユーザーごとに鍵を生成する必要がある．

3.1.1 換字式暗号の仕組みと例

平文の文字を他の記号や文字に置き換えて暗号文を作る古典暗号の方式である．換字式暗号の代表としてシーザー暗号がある．シーザー暗号は鍵である決められた文字数分のアルファベットをずらして暗号化を行う．図 6 は鍵が 1 であるときの例である．

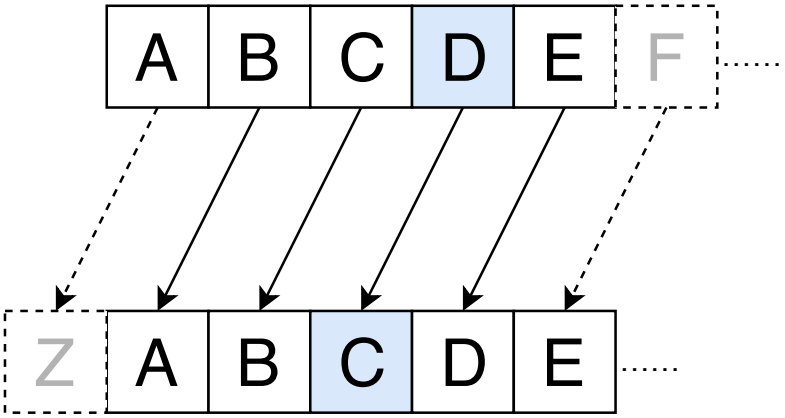

図 6　シーザー暗号の例

3.1.2 転置式暗号の仕組みと例

平文の位置を並び替えて暗号文を作る古典暗号の方式である．転置式暗号の代表としてスキュタレー暗号がある．スキュタレー暗号はスキュタレーと呼ばれるシリンダーに細長い紙を巻きつけ，平文を横書きに書く．紙をスキュタレーから外すと順番が入れ替わった暗号ができる．暗号の受け取る側は同じ半径のスキュタレーを用意し，紙を巻きつけることで復号することができる．この場合，鍵は同じ直径であることである．

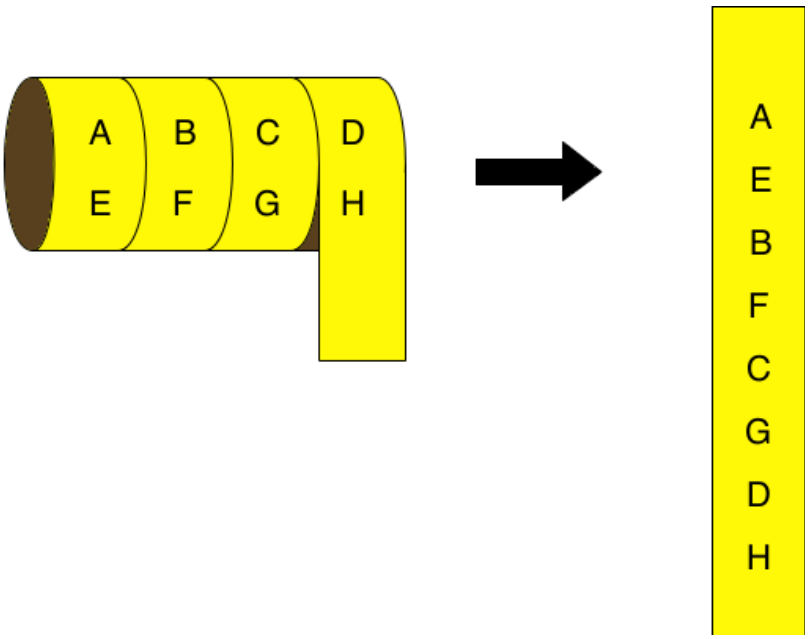

図 7　スキュタレー暗号の例

3.2 公開鍵暗号

暗号化と復号に別の手順を用いる暗号方式である．ユーザは秘密鍵から公開鍵を生成する．通信相手に送る鍵を公開鍵と呼び，自分の手元に保管しておく鍵を秘密鍵と呼ぶ．公開鍵を通信相手に送り，通信相手は公開鍵を使って情報を暗号化する．ユーザは受け取った暗号化

された情報を秘密鍵を用いて復号する．

公開鍵暗号では「閉じることはできても開けることができないこと」を安全の根拠としており，一方向関数である素因数分解や楕円曲線が使われる．

図 8　公開鍵暗号通信の流れ

公開鍵暗号は共通鍵暗号とは違い各ユーザーごとに鍵を生成する必要がない．また鍵の受け渡しの際に傍受される可能性がある共通鍵暗号通信とは違い，公開鍵では復号することができない．そのため共通鍵暗号通信よりも安全性が高い．しかし復号に複雑な計算を用いるため負荷が大きくなるため通信に時間がかかるという欠点もある．

公開鍵暗号の代表的な方式である RSA 暗号など電子署名の役割を持つ暗号方式もある．RSA 暗号など公開鍵と秘密鍵が同じ構造をしている暗号では，どちらの鍵を使っても暗号化することができる．そのため秘密鍵で暗号化し，公開鍵で復号することによって. 送信者が本人である根拠とする．

図 9　公開鍵暗号における電子署名の流れ

3.2.1 RSA 暗号の仕組みと例

RSA 暗号は桁数の多い素数の掛け算をするのは簡単だが，その合成数の素因数分解をするのは困難であることを安全性の根拠とした公開鍵暗号の一つである．

3.3 SSL 暗号化通信の仕組み

共通鍵暗号方式は公開鍵暗号方式よりも負荷が小さいが，鍵の受け渡し時に傍受される危険性があった．そこで鍵の受け渡し時に公開鍵暗号方式を用いることで安全性を確保したものが SSL 暗号化通信である．

SSL 暗号化通信ではまずユーザが通信相手に接続要求をする．通信相手から送られてきた公開鍵を使って共通鍵を暗号化し，通信相手に送付する．通信相手は暗号化された共通鍵を秘密鍵を使って復号する．これで共通鍵が安全に通信相手に渡ったので，共通鍵暗号通信で情報を送ることができる．

図 10　SSL 暗号化通信の流れ

3.4 暗号の歴史

4 ハッシュについて

5 ブロックチェーンについて

6 実験

本章では，提案した仮説が正しいことを証明するために実験を行う．以下で実験方法の解説を行う.

6.1 実験目的

本研究で提案した「学習する単元を前提知識とする単元の概要をあらかじめ説明することで, 内容の理解を促進することができる」という仮説が正しいことを証明することを目的と

する．

6.2 実験方法

6.2.1 実験対象

千葉工業大学 情報科学部 情報ネットワーク学科の学生のうち
2018 年後期に開講された情報数学応用の受講者
1 限 76 名，2 限 76 名，計 152 名
ただし複数回の講義を用いての実験であるため，比較や分析に使用するデータは小テスト受験者のみである．

6.2.2 実験期間

情報数学応用の講義にて 3 週かけて行う．
1 週目：平成 30 年 11 月 16 日
2 週目：平成 30 年 11 月 30 日
3 週目：平成 30 年 12 月 7 日

6.2.3 実験方法

1 限では仮説を用いた講義を行い，2 限では仮説を用いない講義を行う．最後に両クラスで同一の小テストを行い，点数の比較と分析を行う．また小テストと同じ用紙にてアンケートを行う．
(1) 講義スケジュール
実験を行う講義は図 11 のように行う．仮説を用いた 1 限の講義では最初に暗号とハッシュを前提知識とするブロックチェーンの概要について学習した後に，暗号とは負について学習する．仮説を用いない 2 限の講義では最初に暗号とハッシュについて学習した後に，ブロックチェーンについて学習し始める．

	1限	2限
1週目	ブロックチェーンとは	暗号の仕組み
	暗号の仕組み	ハッシュの仕組み
2週目	ハッシュの仕組み	ブロックチェーンとは
	ブロックチェーンのアルゴリズム	ブロックチェーンのアルゴリズム
3週目	小テスト	小テスト

図 11　講義スケジュール

(2) 小テスト内容

小テストでは以下の内容を問う.

① RSA 暗号の特徴

②ハッシュと暗号の違い

③ブロックチェーンの仕組み

点数配分は①と②で 5 点，③で 5 点の合計 10 点とする.

(3) アンケート内容

7 実験結果

8 考察

9 結言

10 参考文献

11 謝辞

12 付録