科学リテラシー

第13回
公開鍵暗号

久保田 匠

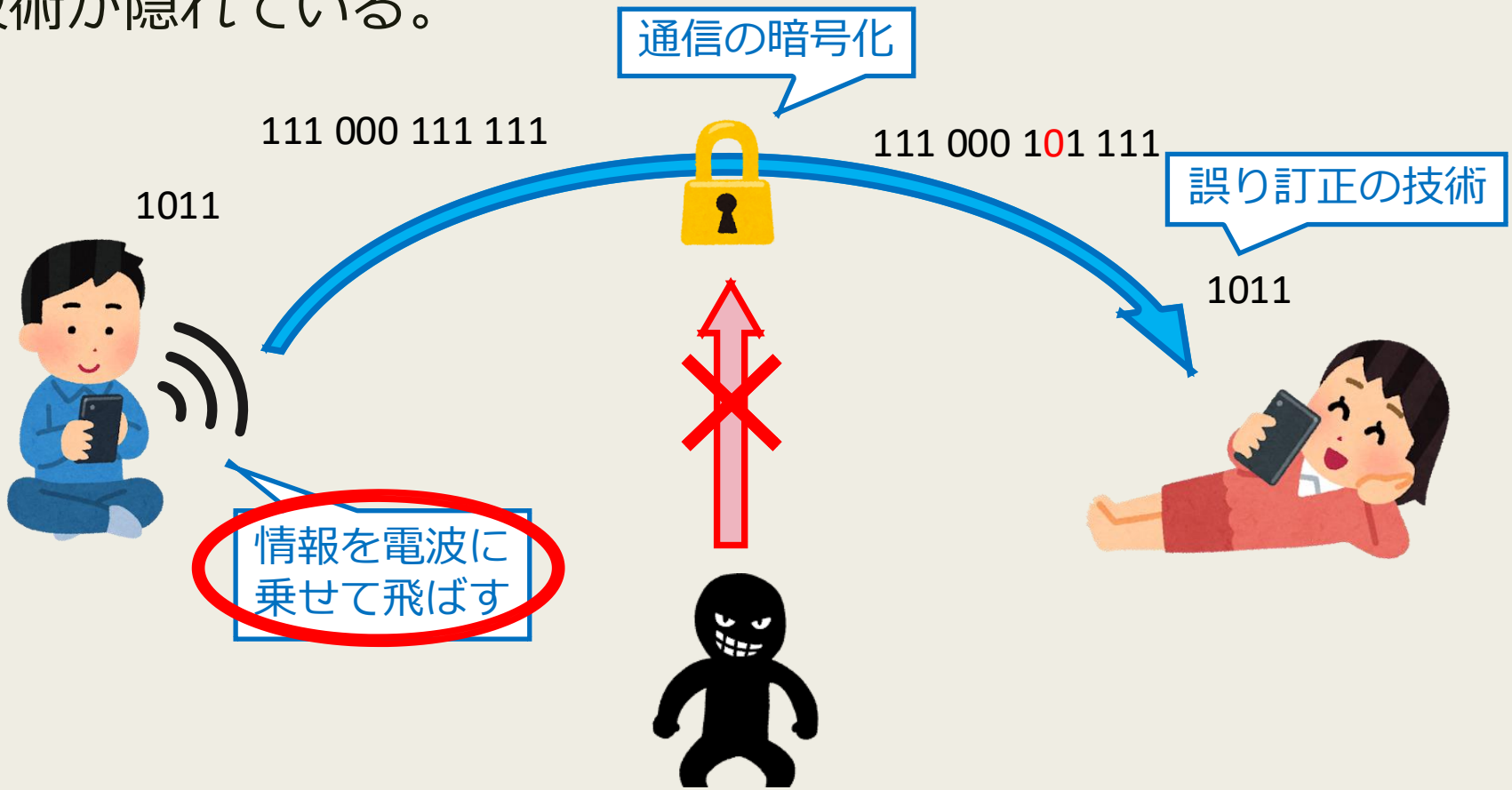
授業資料

- 今日の授業スライドはいつもの授業ホームページにアップロードされているので、適宜参照しながら授業を聞こう。

	内容	演習問題	補足事項
第1回	集合と論理	集合 全称命題と存在命題	
第2回	集合演算	集合演算	
第3回	べき集合と直積集合	包除原理 直積集合とべき集合	
第4回	二項関係	二項関係	
第5回	商集合	商集合	
第6回	1次合同方程式 (解がひとつに決まる)	1次合同方程式(1)	計算のコツ
第7回	1次合同方程式 (解なし or 解がひとつに決まらない)	1次合同方程式(2)	
第8回	連立合同方程式	連立合同方程式	
第9回	2次合同方程式 (法が素数で解をもつ)	2次合同方程式(1) 2次合同方程式(2)	
第10回	2次合同方程式 (法が合成数で解をもつ)	2次合同方程式(3) 2次合同方程式(4)	
第11回	平方剰余の相互法則	ルジャンドル記号 平方剰余の相互法則	
第12回	(オンデマンド)		レポート課題
第13回	2次合同方程式 (解を持たないことを示す)	2次合同方程式(5)	レポート提出日
第14回	公開鍵暗号	べき乗の剰余	スライド
		RSA暗号（送信者）	

情報通信にまつわる色々な科学

- 「スマートフォンを使って友達にメッセージを送る」という何気ない行為をひとつとっても、その背後には様々な学問的技術が隠れている。



- この授業のテーマは**暗号**だが、せっかくの機会なので「情報を電波に乗せる」ということについても考えてみよう。

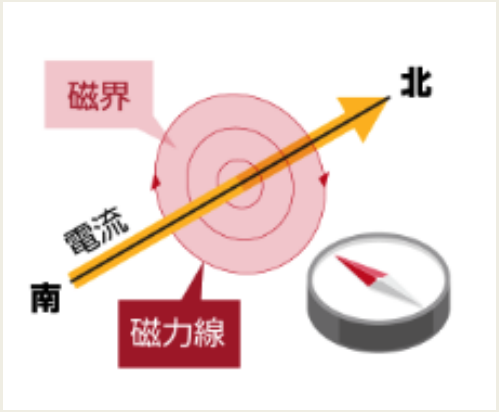
情報を電波に乗せるとは？

- 情報機器は、あなたが送ろうとしている**メッセージを「0」と「1」の列に変換**し、その列を **電波に乗せて** 世界中に飛ばしている。
- まずは、文字情報を「0」と「1」の列に変換してみよう。
- ここでは簡単のため、ひらがな五十音の変換を考える。
- ①各ひらがなに数値を対応させる。
  - 「あ」→ 0　「い」→ 1　「う」→ 2　…　「ん」→ 45
- ②数値を 6桁の2進数表記に変更
  - 0 → 000000, 1 → 000001, 2 → 000010, …, 45 → 101101
- 例：「やきにく」という文字列を変換する場合
  - やきにく → 36 6 11 7 → 100100 000110 001011 000111
- このような「0」と「1」からなる列を**電波**に乗せて飛ばすのだが、そもそも電波とは何だろうか？それを説明するにはいくつかの準備が必要である。

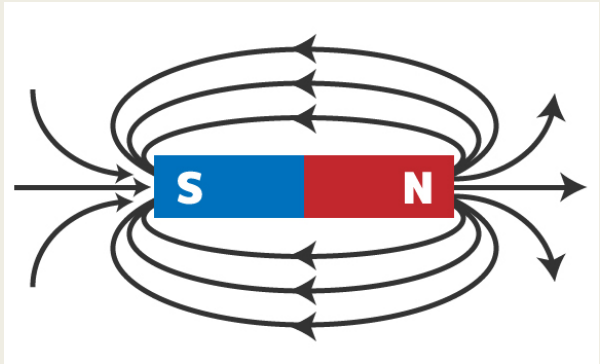
理科の復習その①（磁界）

- 電線に電流を流すと方位磁針の向きが変わる。
- これは、電線のまわりの空間の様子が変わっていることを意味する。
- 電線の周囲に生じたこの空間を 磁界 という。
- 磁界は、電線のまわりに円状に広がる。
- もちろん、磁石を近づけても周囲に磁界が生じる。

そこに磁石があるかのように振る舞う



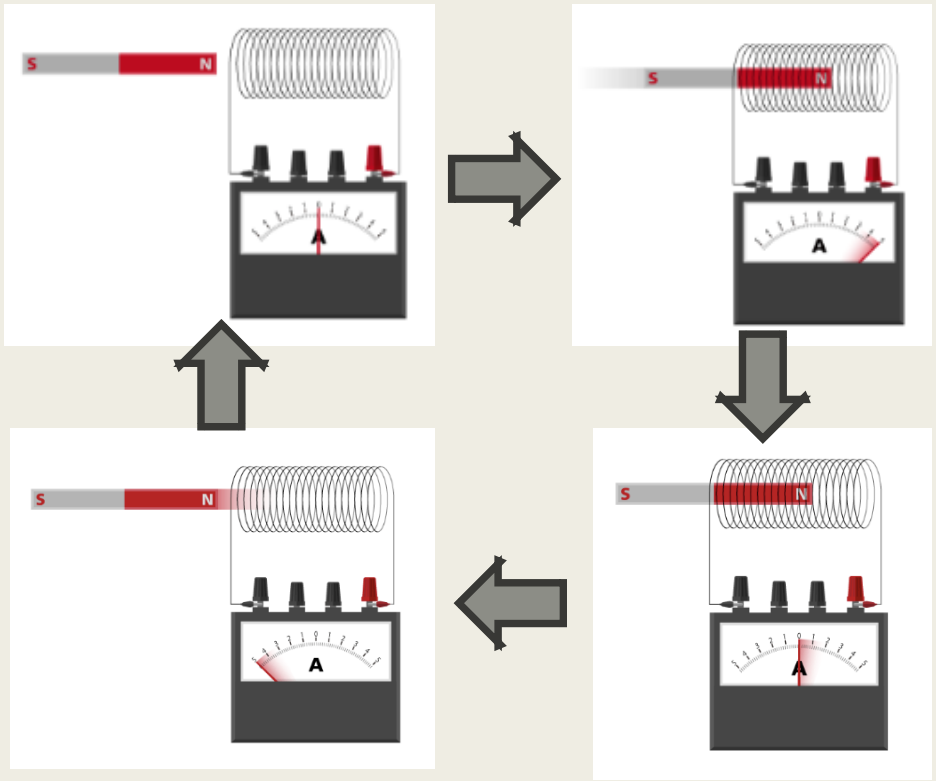
https://www.jrc.co.jp/casestudy/column/14



https://tohokuseigyo.net/

理科の復習その②（電磁誘導）

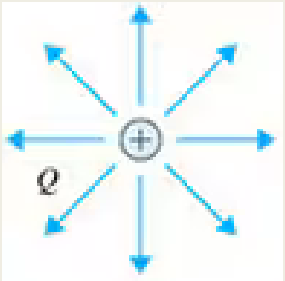
- コイルに電流計をつなぐ。
- 棒磁石をコイルの中に入れると、電流計の針が一瞬プラス側に振れ、すぐゼロに戻る。
- 次に、棒磁石を引き抜くと、電流計の針は一瞬マイナス側に振れ、すぐゼロに戻る。
- このように、磁石をコイルの中で素早く動かし続けると、電流は連続して流れ続ける。
- 次以降のスライドで、この現象（電磁誘導）をもう少し詳しく見てみよう。

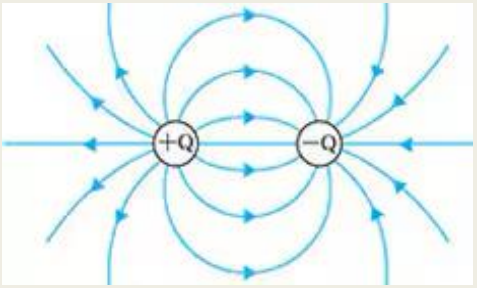


https://www.jrc.co.jp/casestudy/column/14

電界

- 子どもの頃、下敷きで髪の毛をこすると髪の毛が逆立つ現象を体験したことがあると思う。
- 下敷きと髪の毛がこすれ合うことで、両者に電荷の偏りが生じる。
- その結果、下敷きのまわりの空間には、髪の毛や下敷きに電気のはたらきが及ぶようになる。
- このような、電気のはたらきが及ぶ空間を電界という。
- 電界は電荷があることで生じる。
- 「電流が流れる」とは「電荷が動いている」ことである。

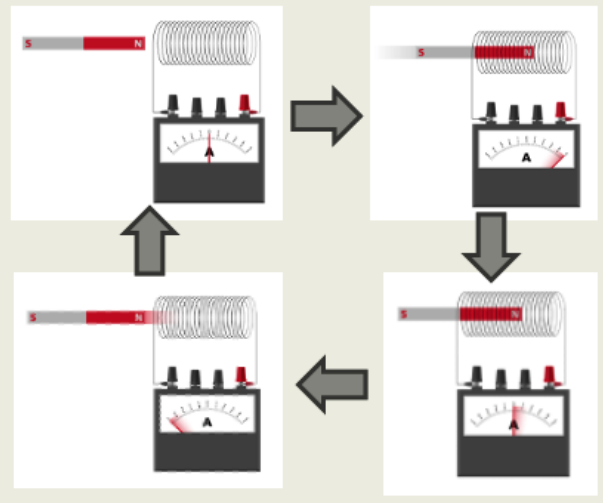




https://www.keyence.co.jp/ss/products/static/static-electricity/electrification/electric-field.jsp

電磁誘導と電界

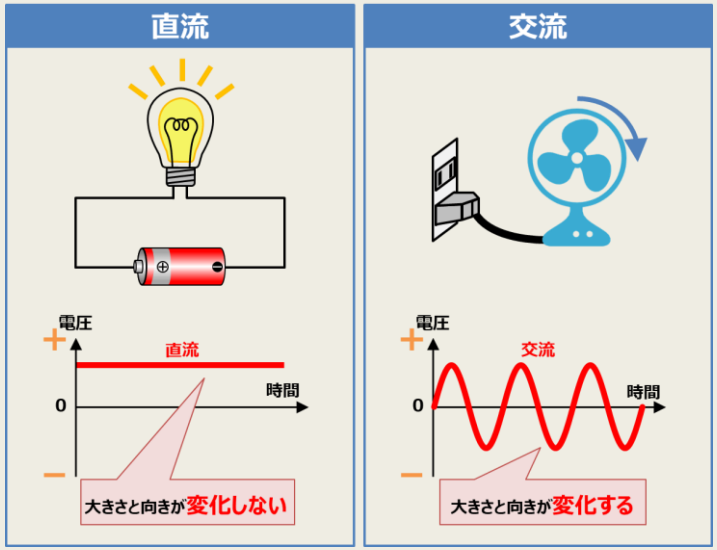
- 改めて電磁誘導について考えてみよう。
- 「コイルの中で棒磁石を動かすと電流が流れる」という現象は、正確には次のメカニズムで起きている。
  - ① コイルの中で棒磁石を動かす（＝磁界を変化させる）。
  - ② 磁界の変化によって周囲に電界が生じる。
  - ③ その電界によってコイル内の電荷が動く。
  - ④ 結果として電流が流れる。
- 本質は「磁界の変化→電界の発生」である。
- 詳細は割愛するが、実は「電界の変化→磁界の発生」も正しい。



https://www.jrc.co.jp/casestudy/column/14

直流電流と交流電流

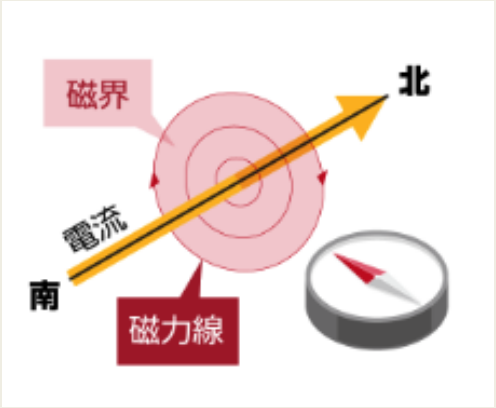
- 電気の流れ方には 直流 と 交流 の2種類がある。
- 直流電流とは、電圧と電流の向きや大きさが時間とともに変化しない電気の流れ方。
  - 乾電池が代表的な例。
- 交流電流とは、電圧と電流の向きや大きさが時間とともに周期的に変化する電気の流れ方。
  - 家庭用のコンセントが代表的な例。



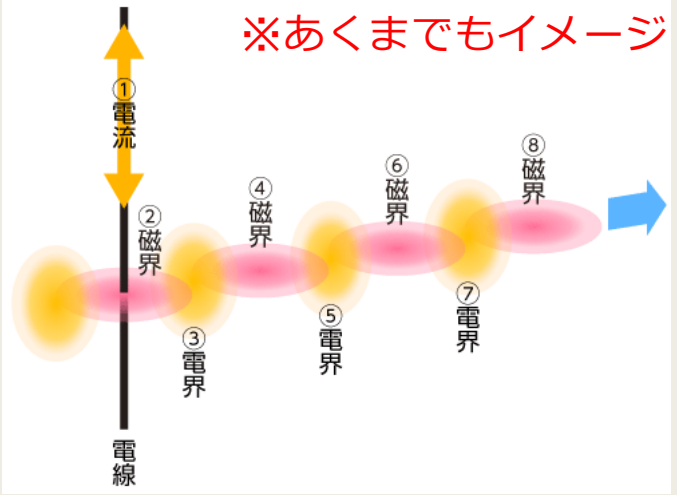
https://detail-infomation.com/ac-dc-difference/

電波（電磁波）の正体

- 以上の準備で電波の仕組みを説明することができる。
  - ① 電線に（交流の）電流を流す。
  - ② 電線のまわりに磁界が生まれる。
  - ③ 磁界の発生によって電界が生まれる。
  - ④ 電界の発生によって磁界が生まれる。
  - ⋮
- このように、「電界」と「磁界」は互いに影響しあい、遠くに波のように伝わっていく。
- この波を 電磁波 という。
- 電波 は電磁波の一部（周波数が 300Hz ～ 3 兆Hz である電磁波）を指す。
  - 周波数とは、1秒間に繰り返される波の数のこと。



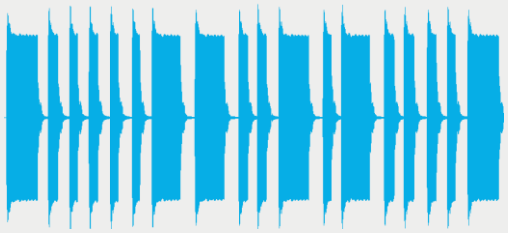
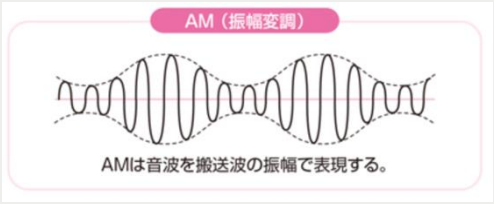
https://www.jrc.co.jp/casestudy/column/14



https://www.jrc.co.jp/casestudy/column/15

情報を電波に乗せる

- 電線に交流電流を流せば電波を飛ばせる。
- したがって、電線に流す電流の流し方をコントロールすれば、電波に「0」と「1」の情報を乗せることができ、遠く離れた相手に情報を瞬時に伝えることができる。
- 電波に情報を乗せる方法はたくさんあるが、ここでは簡単な例をいくつか紹介。

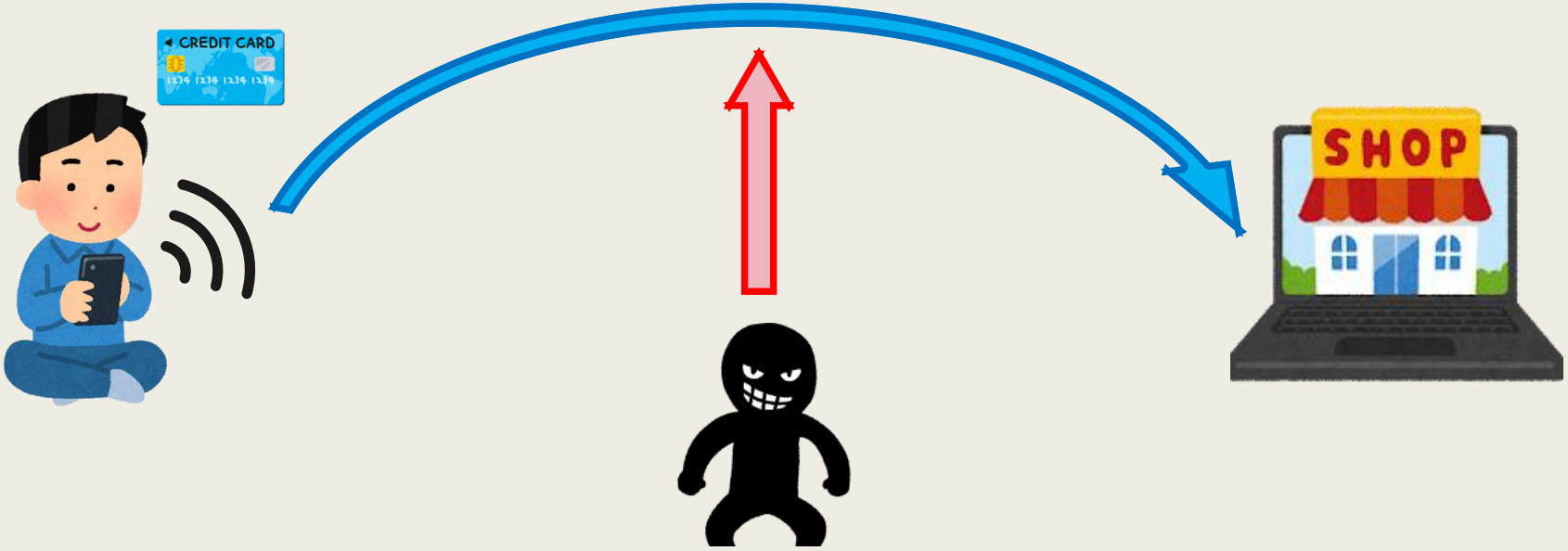
	モールス信号	**AM**	**FM**
情報の乗せ方	同じ形の波を 短時間／長時間 発生させる	波の大きさを 変える	周波数を 変える
波の形			

https://audiostock.jp/audio/61416

https://mainichigahakken.net/life/article/post-727.php

暗号

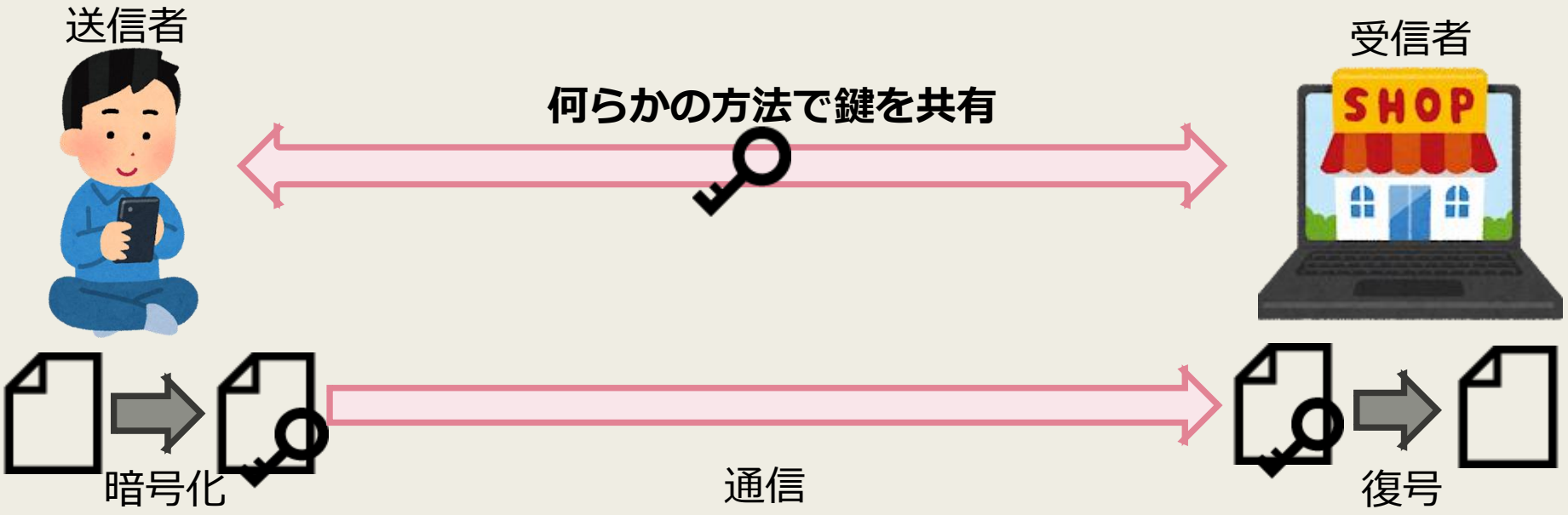
- インターネットでお買い物をするとき、クレジットカード番号を含む重要な情報を通信でやりとりする必要がある。



- クレジットカードの情報が第三者に盗まれると非常に困るので、通信内容を暗号化して送受信しなければならない。
- 世の中には様々な暗号方式が存在するが、それらを大きく分けると 共通鍵暗号方式 と 公開鍵暗号方式 の2種類に分類できる。

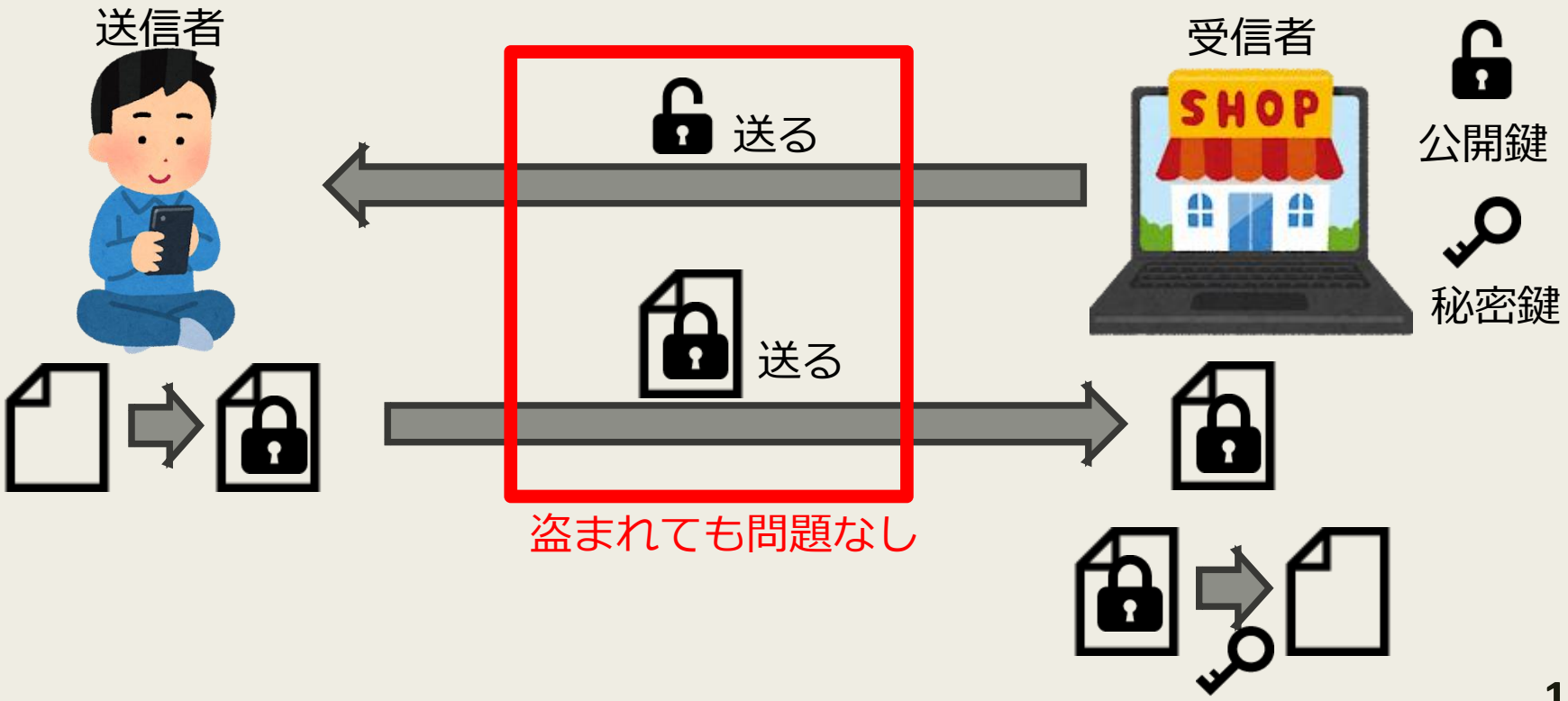
共通鍵暗号方式

- 暗号化と復号に同じ鍵を使う暗号方式を 共通鍵暗号方式 という。
- 送信者と受信者は同じ 共通鍵 を使い暗号化と復号を行う。
- 暗号化と復号の処理が速いという利点をもつ一方で、「共通鍵を受信者とどのようにして安全に共有するか？」という問題がある。
  - 通信によって鍵を共有しようとすると、その通信自体が盗聴される可能性がある。
  - 鍵を直接手渡しするなど、物理的に接触する方法は、安全ではあるが手間がかかる。



公開鍵暗号方式

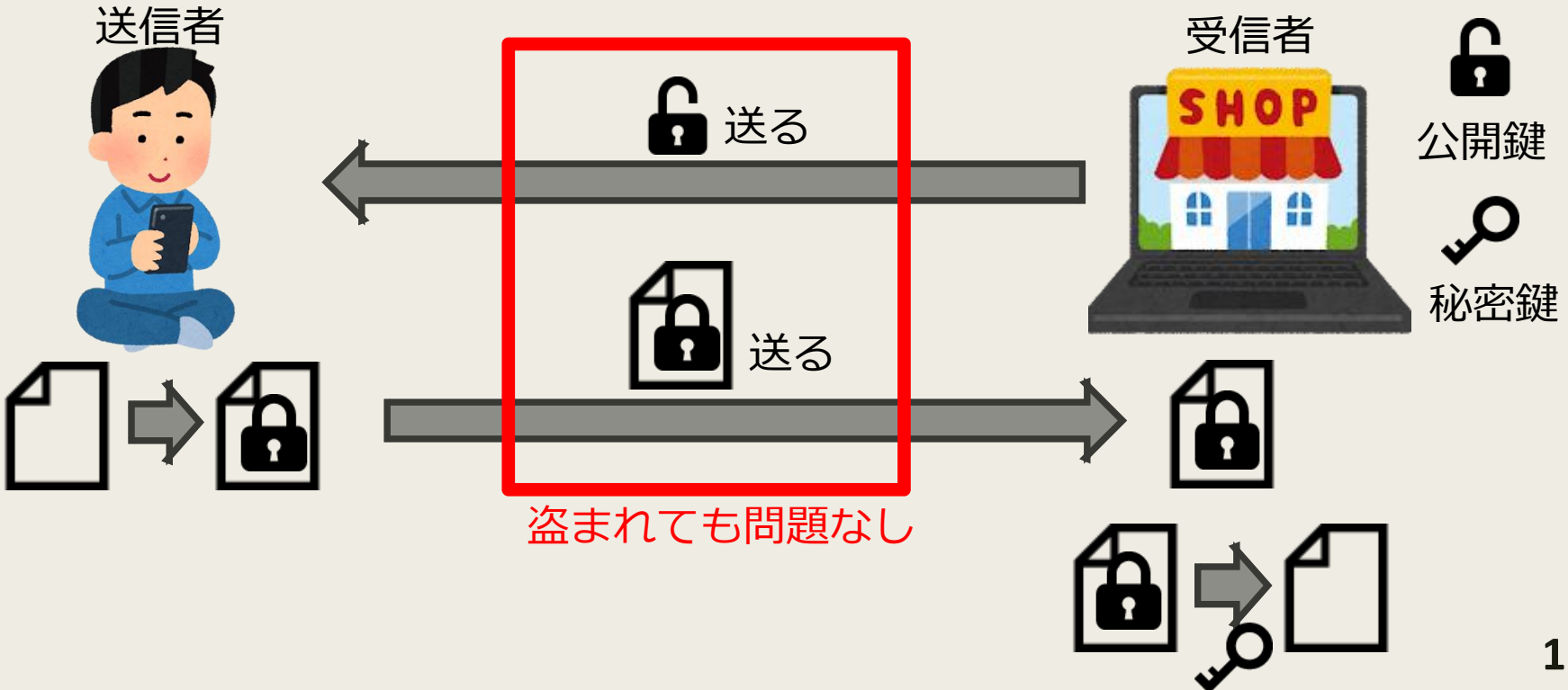
- 公開鍵暗号方式では、役割の違うふたつの鍵を使う。
  - 暗号化に使う鍵を 公開鍵 という。
  - 復号に使う鍵を 秘密鍵 という。
- 最初に情報の送信者が、受信者の公開鍵（「錠」と考えるとよい）を受け取り、それを使って暗号化した文章を送る。



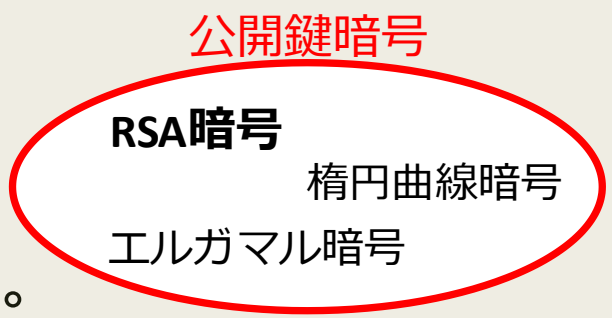
公開鍵暗号方式（詳細）

受信者が公開鍵をあらかじめ公開しておき、送信者がそれを取得することもある

1. 受信者は自身の公開鍵と秘密鍵を作る。
2. 受信者は公開鍵を送信者に送る。
3. 送信者は、受け取った公開鍵を使って送信情報を暗号化。
4. 送信者は暗号文を受信者に送る。
5. 受信者は、自身の秘密鍵を使って復号。送信情報を得る。



RSA暗号の概要



- RSA暗号は最も有名な公開鍵暗号。
  - 1977年に発表（発表前は機密扱い）。
  - RSA は発明者の Rivest-Shamir-Adelman にちなむ。
- RSA暗号では、ふたつの大きな素数 p, q を使って公開鍵と秘密鍵を作る。
  - 秘密鍵は、大きな素数 *p, q* と、ある自然数 *d*
  - 公開鍵は、積 *pq* と、ある自然数 *e*
- 素数の積 pq が公開鍵として使われるため、pq が盗まれる可能性はあるが、積 pq からもとの素数 p, q を復元することは容易ではない。
  - 5149551 を素因数分解してみよ。
- 実際には、p, q は300桁以上の素数が使われており、コンピュータを駆使しても pq から p, q を求めるのは1万年以上かかるため、公開鍵から秘密鍵を復元することは事実上不可能。

RSA暗号の詳細

1. 受信者は自身の公開鍵と秘密鍵を作る。
   - 素数 ***p***, ***q*** を用意し、 ***n*** = *pq* とする。
   - 自然数 ***e*** を *(p-1)(q-1)* と互いに素な数とする。
   - 自然数 ***d*** を $ed \equiv 1 \pmod{(p-1)(q-1)}$ を満たすようにとる。
2. 受信者は公開鍵（**n** と **e**）を送信者に送る。
3. 送信者は、受け取った公開鍵を使って送信情報（平文）を暗号化。
   - 送信情報を自然数 *x* とする（ただし $x < n$）。
   - x^e を計算し、 x^e を *n* で割った余りを *y* とする。

     つまり、$y \equiv x^e \pmod{n}$ である。
4. 送信者は暗号文 y を受信者に送る。
5. 受信者は、自身の秘密鍵を使って復号。送信情報を得る。
   - y^d を計算し、y^d を *n* でわった余りを求める。これが平文 *x* となる。

ここだけ数学的に非自明

y^d を n でわった余りが平文

定理 13.1

先の設定のもとで $y^d \equiv x \pmod n$ である。

1. 受信者は自身の公開鍵と秘密鍵を作る。
   - 素数 p, q を用意し、$n = pq$ とする。
   - 自然数 e を $(p-1)(q-1)$ と互いに素な数とする。
   - 自然数 d を $ed \equiv 1 \pmod{(p-1)(q-1)}$ を満たすようにとる。
2. 受信者は公開鍵（n と e）を送信者に送る。
3. 送信者は、受け取った公開鍵を使って送信情報（平文）を暗号化。
   - 送信情報を自然数 x とする（ただし $x < n$）。
   - x^e を計算し、x^e を n で割った余りを y とする。
     つまり、$y \equiv x^e \pmod n$ である。
4. 送信者は暗号文 y を受信者に送る。
5. 受信者は、自身の秘密鍵を使って復号。送信情報を得る。
   - y^d を計算し、y^d を n でわった余りを求める。これが平文 x となる。

証明.

$y^d \equiv (x^e)^d = x^{ed} \pmod{pq}$ なので、$x^{ed} \equiv x \pmod{pq}$ を示せばよい。

まず、$x^{ed} \equiv x \pmod p$ を示す。

d は $ed \equiv 1 \pmod{(p-1)(q-1)}$ を満たす自然数だったので、ある自然数 k が存在して $ed - 1 = k(p-1)(q-1)$ と書ける。

フェルマーの小定理（定理7.3）より $x^{p-1} \equiv 1 \pmod p$

$$x^{ed} = x \cdot x^{ed-1} = x \cdot x^{k(p-1)(q-1)} = x \cdot (x^{(p-1)})^{k(q-1)} \equiv x \cdot 1^{k(q-1)} = x \pmod p$$

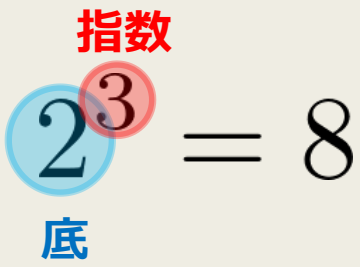
である。同様に、$x^{ed} \equiv x \pmod q$ である。

よって、$x^{ed} - x$ は pの倍数かつqの倍数なので pq の倍数である。

以上より、$x^{ed} \equiv x \pmod{pq}$ である。 ■

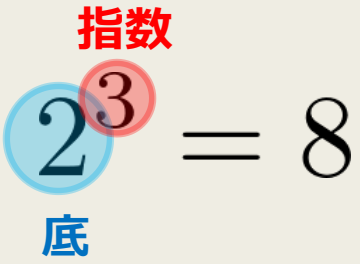
べき乗の剰余

- 以上でRSA暗号の解説は終わり。
- RSA暗号の演習問題は、手計算で済むような小さい素数 p, q に対して、「受信者側」「送信者側」「盗聴者側」になって実際に暗号化や復号をやってもらう（次回の内容）。
- その際、x^e を n で割った余りや、y^d を n で割った余りを計算してもらうことになる。
- ここの計算は多少のコツがいるので、べき乗の剰余の計算問題をやっておこう。



1. 受信者は自身の公開鍵と秘密鍵を作る。
   - 素数 *p, q* を用意し、*n = pq* とする。
   - 自然数 *e* を *(p-1)(q-1)* と互いに素な数とする。
   - 自然数 *d* を $ed \equiv 1 \pmod{(p-1)(q-1)}$ を満たすようにとる。
2. 受信者は公開鍵（n と e）を送信者に送る。
3. 送信者は、受け取った公開鍵を使って送信情報（平文）を暗号化。
   - 送信情報を自然数 *x* とする（ただし $x < n$）。
   - x^e を計算し、x^e を *n* で割った余りを *y* とする。
     つまり、$y \equiv x^e \pmod{n}$ である。
4. 送信者は暗号文 y を受信者に送る。
5. 受信者は、自身の秘密鍵を使って復号。送信情報を得る。
   - y^d を計算し、y^d を *n* でわった余りを求める。これが平文 *x* となる。

[例題]べき乗の剰余



例題

(1) $31^3 \equiv ??$ (mod 33)
(2) $25^5 \equiv ??$ (mod 35)
(3) $21^5 \equiv ??$ (mod 39)

■ 計算の基本的な方針は「要所要所で底の数を小さく」。

(1) mod 33 で $31^3 \equiv (-2)^3 = -8 \equiv 25$ である。

(2) mod 35 で

$$\begin{aligned} 25^5 &\equiv (-10)^5 \\ &= 100 \cdot 100 \cdot (-10) \\ &\equiv (-5) \cdot (-5) \cdot (-10) \\ &= -250 \equiv -5 \equiv 30 \end{aligned}$$

(3) mod 39 で

$$\begin{aligned} 21^5 &\equiv (-18)^5 \\ &= 324 \cdot 324 \cdot (-18) \\ &\equiv 12 \cdot 12 \cdot (-18) \\ &= 144 \cdot (-18) \\ &\equiv 27 \cdot (-18) = -486 \equiv 21 \end{aligned}$$

演習

- 授業ホームページの演習問題「べき乗の剰余」に取り組もう。
- ひと通り終わった人は、次回分の「RSA暗号（送信者）」「RSA暗号（受信者）」「RSA暗号（盗聴者）」に取り組もう。
- 次回、改めてRSA暗号の復習を行った後に演習問題の解説。

参考文献・参考サイト

[1] 日本無線株式会社
https://www.jrc.co.jp

[2] 株式会社東北制御
https://tohokuseigyo.net

[3] 株式会社キーエンス「静電気対策のノウハウを学ぶサイト」
https://www.keyence.co.jp/ss/products/static/static-electricity

[4] Electrical Information
https://detail-infomation.com

[5] 毎日が発見ネット
https://mainichigahakken.net/life/article/post-727.php