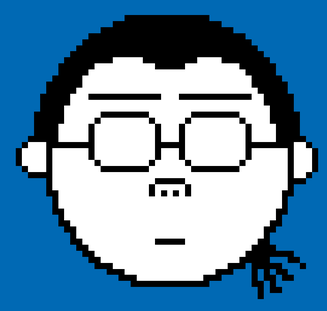
RSA暗号の教材は作ったものの...

中西渉 watayan@meigaku.ac.jp
名古屋高等学校



勤務校について

創立1887年
名古屋市内の私立男子校
中学6クラス，高校12クラス（1学年あたり）
「情報の科学」を高2で実施

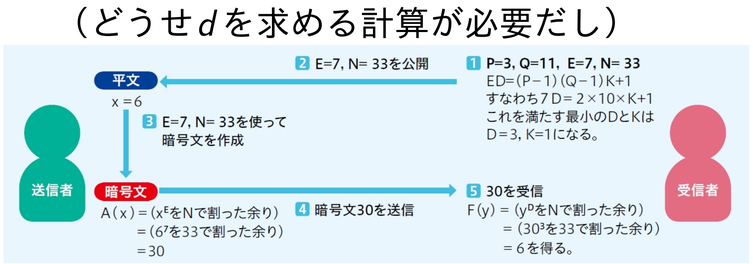
RSA暗号の概略

1. 2つの大きい素数p，qをとり，$n = pq$とする
2. $(p-1)(q-1)$と互いに素なeをとる
3. $de \equiv 1 \pmod{(p-1)(q-1)}$となる$d$をとる
4. nとeを公開鍵，dを秘密鍵とする
5. 送信者は平文Mを，受信者の公開鍵eで暗号化する
   $M^e \equiv C \pmod{n}$となるCが暗号文
6. 受信者は暗号文Cを，自分の秘密鍵dで復号する
   $C^d \equiv M \pmod{n}$

実習を考えるにあたって

教科書では...

- MとCはただの数
  →暗号っぽくない
  →文字列にしよう（27進法で整数↔文字列）
- 表計算で処理できる程度の数
  →小さすぎてつまらん
  →そのためのプログラムを作ろう
  （どうせdを求める計算が必要だし）



（日本文教出版「新・情報の科学」77ページ図版）

実習用画面

計算するプログラムを作って，ブラウザで実習

1. p，qは決める
2. eも決める
3. 「鍵生成」でnとdを計算
4. p，q，dは隠す
5. 平文（単語）→27進法で数値化(M)→ 暗号化(C)→文字列化→暗号文
6. 暗号文→数値化(C)→復号(M)→文字列化→元の単語

授業の流れ

1. 自分で鍵を作って暗号化→復号
2. 2人ペアで送信と受信（あとで入れ替わる）
   鍵や文字列はプリントに記入して伝える
3. p，qとeがわかればdが生成できることを確認
4. こちらが示したnについてp，qの値を問う
   →無理に決まってるやん... でもコンピュータなら？
   →素因数分解のプログラムをライブコーディング
   「でもな，これが何百桁だったら...」

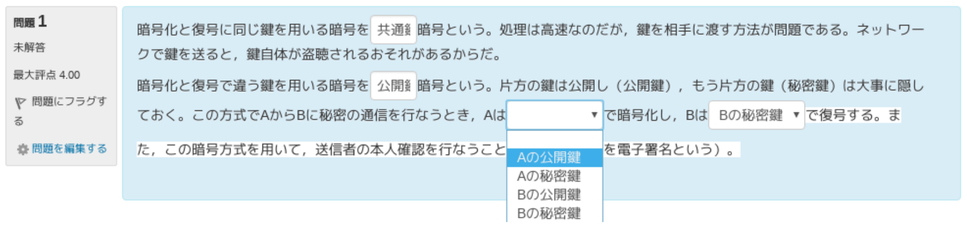
生徒の反応

- ちゃんとした単語にならない！
- あ，eとdが逆だった...
- 秘密鍵どうやって相手に教えるの？

正確に入力してね
画面に書いてあるやん

ちょっと待て

- テストの出来が...

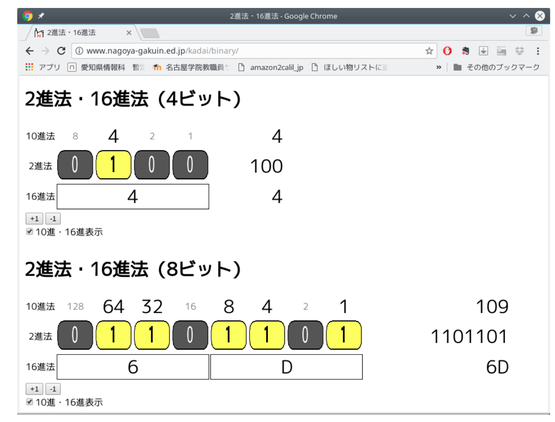


何が足りない？

時間？
数学的な説明？
UIのわかりやすさ？
手作業の部分？

余談：他にもいろいろ作ってます

- 2進法・16進法・10進法
- 2進法時計
- 2進法の補数
- 文字コード16進表示
- 色の加法混色
- 画像圧縮の比較
- RSA暗号
- WaPEN



http://www.nagoya-gakuin.ed.jp
自作教材が職場サーバに置けなきゃレンタルサーバでもいいよね？