RSA 暗号の実習にて

名古屋高等学校　中西渉

自己紹介

- 名古屋高等学校　中西渉（わたやん）
- 1989 年　大学卒業→現勤務校に奉職（数学）
- 2000 年　現職教員研修で情報科免許取得
- 2004 年～情報で教壇に
- プログラミング大好き
- https://watayan.net

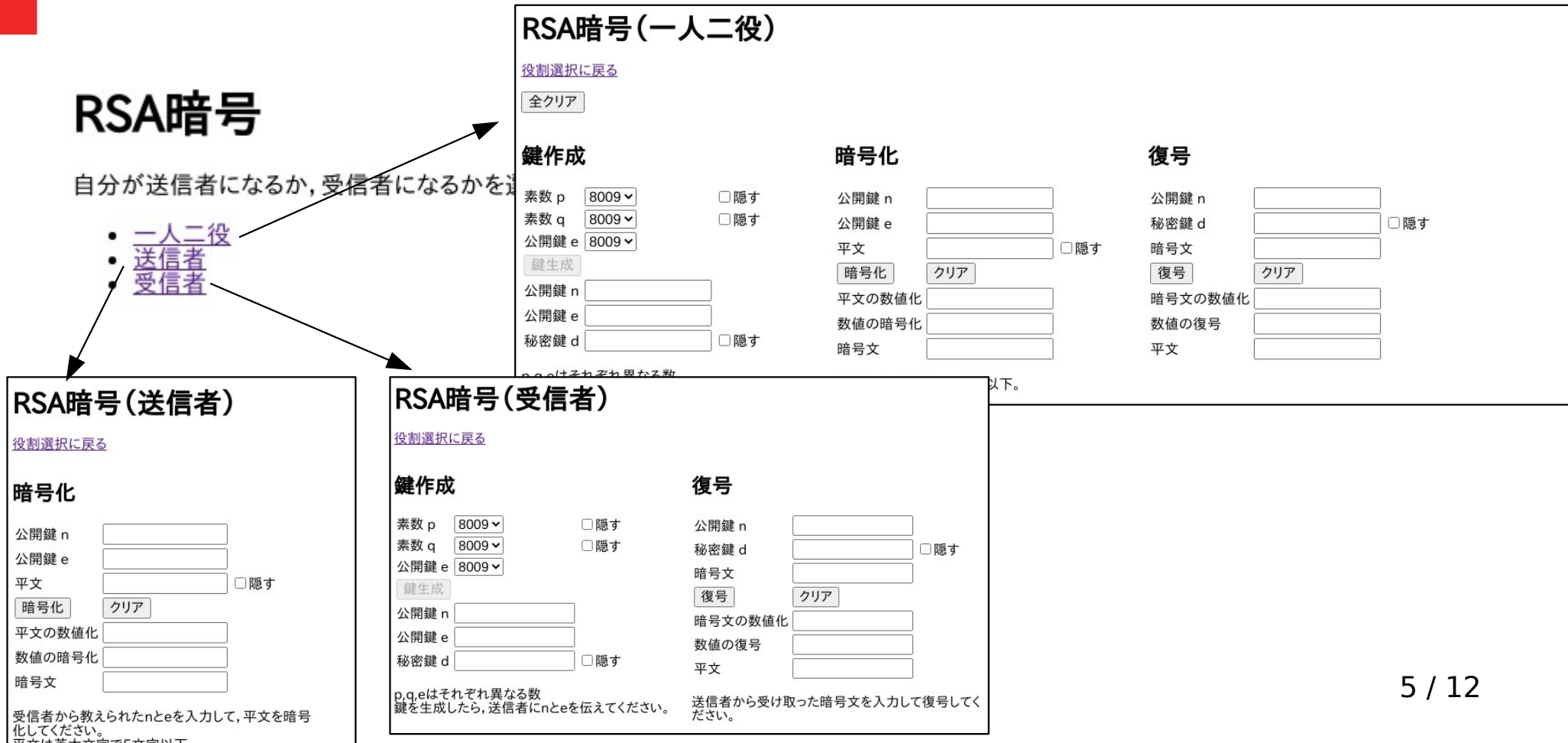
勤務校紹介

- 1887 年創立
- キリスト教
- 併設型中高一貫校
- 男子校

RSA 暗号の実習

- https://www.nagoya-gakuin.ed.jp/rsa/
- 実習の流れ
  - 受信者が鍵作成→送信者に公開鍵を教える
  - 送信者が公開鍵で平文を暗号化→受信者に暗号を教える
  - 受信者が秘密鍵で復号

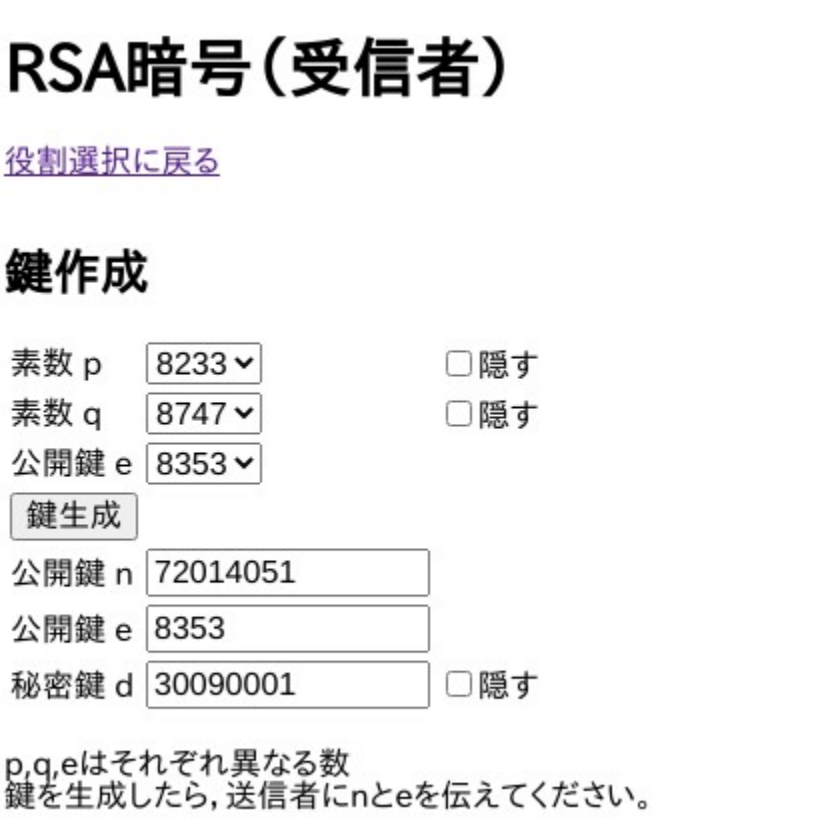
過去の反省を踏まえて


RSA暗号
自分が送信者になるか，受信者になるかを
一人二役
送信者
受信者
RSA暗号（一人二役）
役割選択に戻る
全クリア
鍵作成
素数 p 8009 隠す
素数 q 8009 隠す
公開鍵 e 8009
鍵生成
公開鍵 n
公開鍵 e
秘密鍵 d 隠す
暗号化
公開鍵 n
公開鍵 e
平文 隠す
暗号化 クリア
平文の数値化
数値の暗号化
暗号文
復号
公開鍵 n
秘密鍵 d 隠す
暗号文
復号 クリア
暗号文の数値化
数値の復号
平文
以下。
RSA暗号（送信者）
役割選択に戻る
暗号化
公開鍵 n
公開鍵 e
平文 隠す
暗号化 クリア
平文の数値化
数値の暗号化
暗号文
受信者から教えられたnとeを入力して，平文を暗号化してください。
RSA暗号（受信者）
役割選択に戻る
鍵作成
素数 p 8009 隠す
素数 q 8009 隠す
公開鍵 e 8009
鍵生成
公開鍵 n
公開鍵 e
秘密鍵 d 隠す
p,q,eはそれぞれ異なる数
鍵を生成したら，送信者にnとeを伝えてください。
復号
公開鍵 n
秘密鍵 d 隠す
暗号文
復号 クリア
暗号文の数値化
数値の復号
平文
送信者から受け取った暗号文を入力して復号してください。

受信者

- p,q,e を決める
- 「鍵生成」
- 公開鍵 n,e を送信者に教える

n は 72014051
e は 8353



送信者

- 教えられた n,e を入力
- 平文の単語を入力
- 「暗号化」
- 暗号文を受信者に教える

D=TV=M

RSA暗号（送信者）

役割選択に戻る

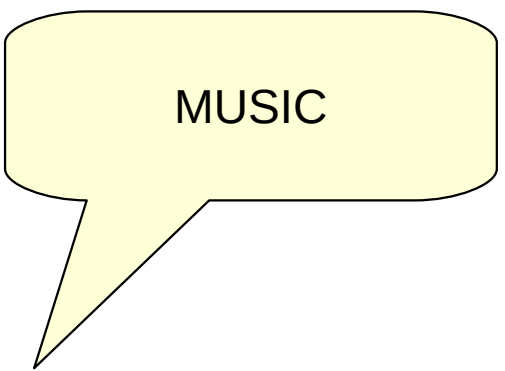
暗号化

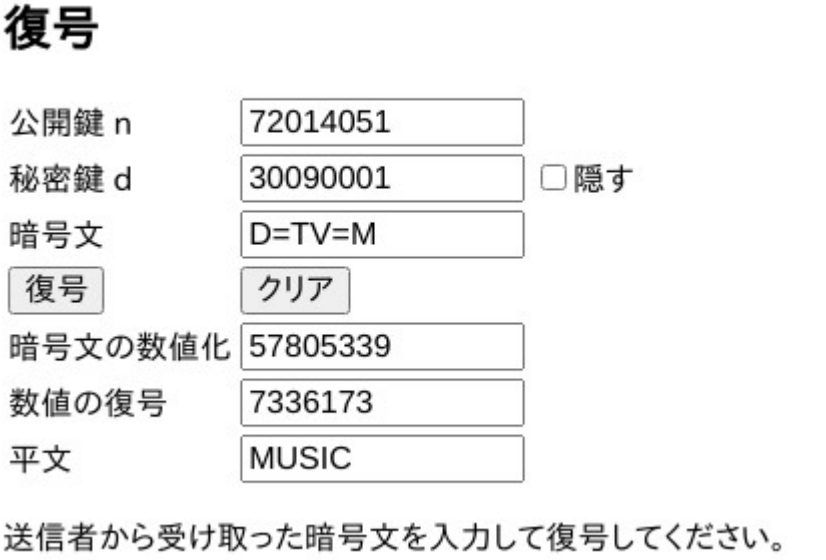
公開鍵 n	72014051	
公開鍵 e	8353	
平文	MUSIC	☐隠す
暗号化	クリア	
平文の数値化	7336173	
数値の暗号化	57805339	
暗号文	D=TV=M	

受信者から教えられたnとeを入力して，平文を暗号化してください。
平文は英大文字で5文字以下。

受信者

- 教えられた暗号文を入力
- n,d を入力
- 「復号」





これをやってる隙に…

RSA暗号（一人二役）

役割選択に戻る

全クリア

鍵作成

素数 p 8237 ☐隠す
素数 q 8543 ☐隠す
公開鍵 e 8389
鍵生成
公開鍵 n 70368691
公開鍵 e 8389
秘密鍵 d 46140925 ☐隠す

p,q,eはそれぞれ異なる数

暗号化

公開鍵 n 70368691
公開鍵 e 8389
平文 AICHI ☐隠す
暗号化 クリア
平文の数値化 711000
数値の暗号化 11312724
暗号文 UGTCU

平文は英大文字で5文字以下。

君たちは盗聴者だ！

d が知りたい？

n=pq だから
p と q がわかれば
自分で d が
作れるよね

70368691 を
素因数分解
するだけだよ

ちょっと
無理

8237 と
8543 ！

RSA暗号（一人二役）

役割選択に戻る

全クリア

鍵作成

素数 p ☑隠す
素数 q ☑隠す
公開鍵 e 8389
鍵生成
公開鍵 n 70368691
公開鍵 e 8389
秘密鍵 d ☑隠す

p,q,eはそれぞれ異なる数

暗号化

公開鍵 n 70368691
公開鍵 e 8389
平文 ☑隠す
暗号化 クリア
平文の数値化
数値の暗号化 11312724
暗号文 UGTCU

平文は英大文字で5文字以下。

復号

公開鍵 n 70368691
秘密鍵 d ☐隠す
暗号文 UGTCU
復号 クリア
暗号文の数値化
数値の復号
平文

どうやった？

- 「素因数分解」でググりました

https://keisan.casio.jp/exec/system/1161228771

正しいコンピュータの使い方

- 「ググる」ばかりでは困るが
  - それさえしないのはいかがなものか
  - 目の前にある箱は何ができるの？
- 「使わない自分」＜「使う自分」
- 「１人１台」で期待したいのは，こんな「当たり前」