RSA暗号を用いた暗号化

東京都立南多摩中等教育学校 5 年 天野 匠

序論：RSA暗号の特徴と教育上の課題

RSA暗号とは

桁数が大きい合成数の素因数分解が困難であるという性質とフェルマーの小定理を利用した暗号である。

RSA暗号の利点

桁数の大きい秘密鍵を使用して、素因数分解によって暗号を復号することを困難にすることで、安全性を高められる。

RSA暗号の欠点

暗号化したデータ量に比例して復号にかかる時間が増加するため、大量のデータの暗号化には向かない。

教育上の課題

フェルマーの小定理を知らない場合や計算が不得意な場合には、暗号化や復号の過程を理解しにくい。そのため、暗号化の方法を説明するだけでは理解するためには不十分である。

▶実際に暗号化を体験させることで、興味や理解度の増加を補助できると考えた。

解決策：プログラムの作成

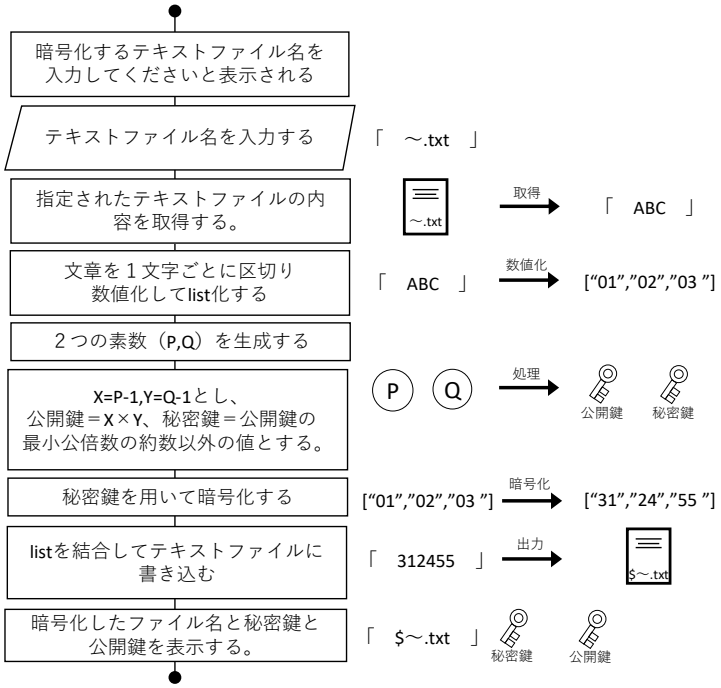
本研究ではRSA暗号を用いた暗号化を体験できるプログラムを作成した。プログラムはPythonで記述した。

プログラムのコンセプト

・自分で作成した文章を暗号化し、秘密鍵を用いて暗号化された文章を復号できる。
・公開鍵の桁数の増加と暗号化する文字数の増加に伴って復号にかかる時間が増加することを実感できる。

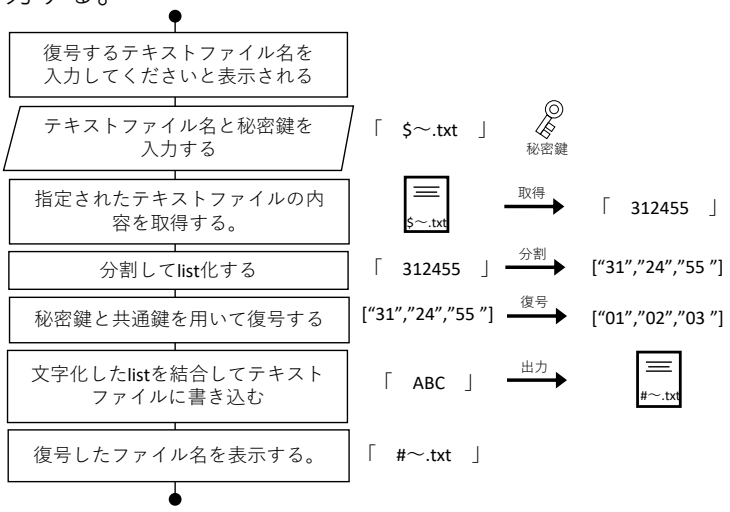
暗号化の過程

1. テキストファイルから暗号化する文章を取得し、Unicodeのコードポイントによって1文字ごとに数値化する。
2. 秘密鍵を生成して 1 の数値を暗号化する。
3. 暗号化した数値をつなぎ合わせてテキストファイルに出力する。



復号の過程

1. 暗号化されたテキストファイルを分割してlist化する。
2. 公開鍵と秘密鍵を用いて 1 を復号する。
3. 1 をUnicodeのコードポイントによって文字化して、listをつなぎ合わせてテキストファイルに出力する。



評価：フィードバックと改善

RSA暗号に詳しくないクラスメイトにプログラムを使用してもらい、RSA暗号の特性を理解する際に役立つのかという観点で評価してもらった。

フィードバック

・実際に暗号化のプログラムを体験したほうがRSA暗号について理解できた。
・公開鍵の桁数によって復号するのにかかる時間の変化するということが直感的にわからない。
・CUIだけでなくGUIがあるとわかりやすい。

改善

・Pythonの外部ライブラリのtqdmを利用して復号するときにプログレスバーを表示する。

```
復号中:  38%|          | 66531/175098 [00:04<00:07, 14904.47文字/s]
```

・Microsoft Formsを利用してWindowsのアプリケーションをビルドする。（未実装）

結論

成果

・RSA暗号を用いて文章の暗号化と復号をできるプログラムを作成し、フィードバックをもとに改善した。
・RSA暗号の仕組みを理解するためにプログラムを利用して暗号化を体験することは効果的であることが分かった。

今後の課題

本研究ではコンソールアプリケーションを作成したが、この表現方法のみで改善していくことには限界がある。よって、GUIアプリケーションを作成することでより直感的に操作できるようにすることが今後の課題である。