暗号技術と電子署名

東京都立戸山高等学校　SS情報　2年　徳田瑞生

研究動機
電子署名などに使われている公開鍵暗号方式では「RSA暗号」と「ECC暗号」が主流である。しかし量子技術の発展によって、どちらの暗号技術も安全性が危ぶまれつつある。そこで既存の暗号技術を比較することにした。

研究目的
時と場合に応じた電子署名のシステムを実装する。

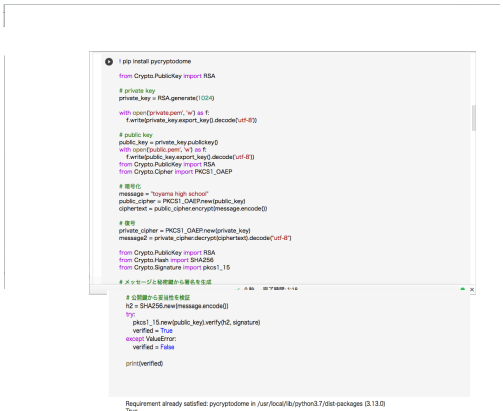
RSA暗号とは
桁数が大きい合成数（＝素数でない数）の素因数分解がコンピュータの演算能力でも困難であることを根拠にした暗号技術

ECC暗号とは
楕円曲線暗号と呼ばれており、楕円曲線上の離散対数問題が解読困難であることを根拠にした暗号技術

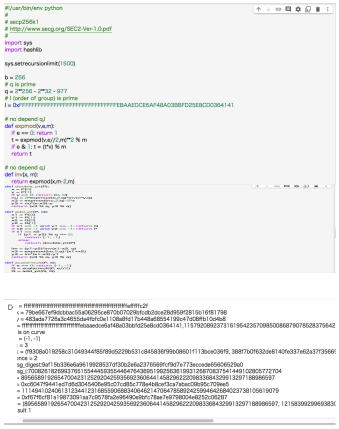
研究方法
Pythonを用いてRSA暗号による電子署名とECC暗号による電子署名を実装する。

※RSA暗号ではpythonのライブラリであるpycryptodomeを用いて電子署名を作成し、妥当性を判断した。
※ECC暗号では外部ライブラリを用いずに既存のアルゴリズムを参考にして電子署名を作成し、妥当性を判断した。

電子署名（RSA暗号）



電子署名（ECC暗号）



結果
どちらも署名の作成に時間がかかる。
RSA暗号は署名の妥当性を判断する速度が速い。
ECC暗号では署名の作成と妥当性の判断の時間にそこまで差が見られなかった。

考察
今回はライブラリを使って実装したものとライブラリを使わないで実装したもので比較を行ってしまったので、正確な比較になっていないのではないか。
ECC暗号も作成に時間がかかるが、妥当性を判断する時間と大差なかったので、何処かのタイミングでRSA暗号より電子署名の作成と判断が速くなるのではないかと考えられる。

今後の展望
RSA暗号版とECC暗号版の速度が逆転するのは、暗号鍵の長さであると仮定して、研究を進める。

参考文献
ECDSAでの署名と検証をpythonで行う　1/24
https://pebble8888.hatenablog.com/entry/2018/04/21/210617
Google colab　1/15
https://colab.research.google.com/drive/1HtIvwE7hOFLG9vqMCar2UTKvK0xCQXXH#scrollTo=I71tmSqLenD0
RSA暗号と電子署名　10/24
https://www.python.ambitious-engineer.com/archives/2042#i-3