解かれない暗号を求めて

宮城県仙台第三高等学校 37－1班

1．背景と目的

初めに、私たちは「解かれない暗号」を求めるべく、RSA暗号について研究をしていた。しかし、今日では量子コンピュータの開発が進んでおり、その性能の高さ故、RSA暗号が容易に解かれてしまう問題が発生していることを知った。そこで私たちが目をつけたのが、今、暗号界で注目されている「楕円曲線暗号」である。この「楕円曲線暗号」を深く調べ、有効に利用することができれば、私たちが求める「解かれない暗号」ができるのではないかと考えた。

2．楕円曲線暗号について

①楕円曲線暗号とは

楕円曲線 と呼ばれる曲線で、
それに基づいた暗号のことを楕円曲線暗号と呼ぶ。
この暗号のセキュリティは「 **離散対数問題** （ECDSA）」の困難さに基づいている。

②楕円曲線暗号はなぜ強固な暗号なのか

楕円曲線暗号の強みとして、少ないデータ量であっても計算が膨大になるということが上げられる。　RSA暗号で2048bitを使って得られる安全性が、楕円曲線暗号では224bit程度で実現できるように、他の暗号と比べても少ないデータ量で強固な暗号を作ることができる。
楕円曲線暗号をこれほどまでに強固にする要因は、上記にもあるように離散対数問題の解決の困難さである。
（離散対数問題については右で詳しく説明）

4 実験方法

①Google Colaboratory　上でプログラミングを組み、楕円曲線暗号を実際に使用した

②$y^2=x^3+1$の楕円曲線で、初期値を (2,3)と定めて5Pの値まで求めた

1P: (2, 3)
2P: (0.0, 1.0)
3P: (-1.0, 0.0)
4P: (0.0, -1.0)
5P: (2.0, -3.0)

3－1 離散対数問題について

まず初めに、離散対数問題はモジュラ演算(mod)を使用して考える。
ある原始根rと素数pを用いて

$$r \bmod p \equiv n \cdots ①$$

を考える。

原始根とは、3以上の素数p
と 1以上p−1以下の整数r が
「r、r^2、r^3…r^{p-2}のいずれもがpで割って余り1でない」という性質を満たすとき、
rをmod p の原始根と呼ぶ。

Ex.)素数13の時を考えると、原始根は
2,6,7,11である。

また、①において、nは重複しない
（同じ値が出てこない）ため、
r、r^2、r^3…r^{p-2}と一対一の関係に
なる。そして、出てくるnの値には規則性
がないため、予測が困難である。

今、rとpがわかっている状態でnを求めるのは容易（ただ一つづつ計算すれば良い）である（11 mod 13 のような感じ）が、pとnがわかっている状態で、rを求めるのは難しい。（r mod 13≡3のような感じ）これを離散対数問題という。

3-2 楕円曲線上での離散対数問題について

加算について

楕円曲線上での加算については定義されており、２点A,Bについて、AとBを通る直線を引き、残りの交点をx軸を対称とした点をA+Bとする。

このとき、$y^2=x^3+ax+b \bmod p$の軸の部分は、mod pの部分の影響大きい

楕円曲線暗号では、nを秘密鍵、nGの値(x,y)を公開鍵とした暗号になっている
3-1で述べたものと同じように、nが与えられた状態でGを求めるのはコンピュータでも容易であるが、(x,y)からnを求めるのは困難である

実際の暗号では、
nをとてつもなく大きい数
を用いて作られるため、
解読がとても困難！

まとめ・結論

今後の展望

楕円曲線暗号や離散対数問題について調べ、それらがどのように関係し合っているかを知ることができた。また、楕円曲線暗号を実際にコンピューター上で使用することができた。これからは今まで調べてきたことを用いて、私達が実生活で用いることができるような暗号の作成をしたり、セキュリティについての関心を高めていきたい。

参考文献

1）CentOS8 構築・運用・管理 パーフェクトガイド/15-A 楕円曲線暗号
https://sbcr-dl-and-idea.s3.ap-northeast-1.amazonaws.com/2021-07-13-02567-CentOS8%E6%A7%8B%E7%AF%89%E3%83%BB%E9%81%8B%E7%94%A8%E3%83%BB%E7%AE%A1%E7%90%86%E3%83%91%E3%83%BC%E3%83%95%E3%82%A7%E3%82%AF%E3%83%88%E3%82%AC%E3%82%A4%E3%83%89/15-A%E6%A5%95%E5%86%86%E6%9B%B2%E7%B7%9A%E6%9A%97%E5%8F%B7.pdf

2）【保存版】ECDSAを理解するために！（離散対数問題／楕円曲線上の離散対数問題）https://note.com/standenglish/n/nf68d7bf8e5e2