解かれない暗号を求めて

宮城県仙台第三高等学校　普通科

要旨
私達の班では、数学を我々の身の回りのことに応用しようと考え、現在どのような暗号が使われているかを調べた。そこで、RSA 暗号という方式が現在世界で最も多く使われているということを知った。ただ、現在量子コンピュータの開発が進み、現在の暗号も容易に解かれてしまうということを知り、別な方法はないかと考え、調査を進めていくうちにまだ普及こそしていないもの、高いセキュリティを誇る楕円曲線暗号という方式があることを知り、実際に実験を行ったり、調査を進めたりして、この暗号を普及することができるか探究を行った。

1　はじめに
楕円曲線暗号の仕組みについての調査や Google Colaboratory を用いて実際の楕円曲線暗号での情報の送受信、暗号化の仕組みについての調査を行い、普及していくために何が必要なのかを調べた。

2　考察
まず、私達は楕円曲線暗号とはどんなものであるかについて、インターネットや本を用いて調査した。ただ、そこで調べることができた情報だけでは限界があったため、修学旅行の際に立命館大学の高田秀志教授と野島良教授を訪ね、楕円曲線暗号を用いた量子コンピュータの現状や情報の送受信の仕組みについて伺った。

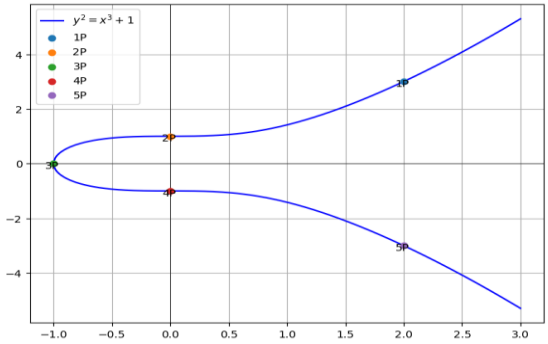
①量子コンピュータの現状について
まず量子コンピュータについてだが、現在普及しているコンピュータとの大きな違いは、同時に計算処理ができることにある。そのため、今のコンピュータで多くの時間を要する計算も、量子コンピュータならかなり早い時間で処理することができる。ただ課題は多く、処理の際に用いる量子ビットは現在の情報ビットに比べて不安定なためにエラーが多発してしまうことや、計算処理のみに特化したコンピュータであるため他の処理への応用がきかないことから開発を出資する企業が少ないこと、情報を送受信するのに非常に多くの費用を要することが挙げられる。
野島教授によると、現在世界中で量子コンピュータの開発が進められているが、実用化に向けた課題が多く、完成して実際に利用されるようになるのはまだまだ先になるだろうとのことだった。

②楕円曲線暗号の送受信の仕組み
楕円曲線暗号では、公開鍵暗号方式が使われている。公開鍵暗号方式とは、公開鍵と秘密鍵という2つの暗号方式を利用し、
1,受信者が秘密鍵から公開鍵を作成し送信者に渡す
2,送信者がその公開鍵を使い通信内容を暗号化する
3,暗号化された文書を受信者が受け取る
4,受信者が秘密鍵を用いて復号する
という手順で送受信が行われている。
そして、この方式の公開鍵・秘密鍵の部分に楕円曲線を用いたのが楕円曲線暗号である。次に楕円曲線暗号の仕組みについて説明する。この暗号では、楕円曲線における離散対数問題を活用している。離散対数問題には楕円曲線上のものの他にも整数上でのものなど様々な種類があり、どの種類にも共通して言えることは、ある計算の結果からその答えを逆算することが難しいということである。具体的に説明すると、楕円曲線上での加算を考えたときにある点 G が与えられた状態で n 回加算した点 nG を求めるのは簡単であるが、ある点(x,y)から点 G を求めるのは難しいというのがこの離散対数問題である。整数における離散対数問題を用いる

RSA 暗号に比べ、この楕円曲線暗号は少ないデータ量で同等のセキュリティを保つことができるため、新たな暗号方式として期待されている。

③実験内容

次に私達は google colaboratory を用いて実際に楕円曲線暗号のコードを出力してみてこの暗号が本当に十分なセキュリティを誇るのか検証した。



これが実際に出力した結果である。今回は一般的に使われている$y^2=x^3+1$という楕円曲線を用いて5G の値まで求めることができた。実際に作成してみて、十分な機材が揃わず5G の値までしか求めることができなかったが、この楕円曲線の式を変えるだけでも全く異なる暗号となるため、十分なセキュリティを持つことがわかった。

また、実際に情報の送受信も検証した。

公開鍵暗号方式を用いたプログラムを出力して検証した。

1、送信側が秘密鍵と公開鍵を作成する

2、実際に情報の送受信ができることを確認できた。

④まとめ

この探究を通して現在の情報セキュリティについて知り、情報化が進む現代のセキュリティ面についてはかなり多くの工夫がなされていることを知った。また、セキュリティだけでなく量子コンピュータなどの高性能なコンピュータの開発が進み、新たな暗号方式の発明が求められていることを知った。技術が急速に成長しているこの現代において、絶対に破られない暗号はもしかしたら存在しないのかもしれない。ただそれを発明しようとする志がそれを追求し続ける姿勢こそが、情報社会の安全性を支える技術革新を生む原動力であるといえるだろう。

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

abstract

This study explores what cryptography is the best in the future. RSA cryptography is used around the world such as bank security, and websites. However, it is not enough to protect completely. so, we found the new cryptography. It is elliptic curve cryptography. It can be more safe than RSA cryptography with using less byte. It is not known by many people. So, we want to spread it and protect our personal information.