自主課題研究

―最短経路問題を用いた RSA 暗号―

情報システム工学科 3 年　名列番号 018：木下中世

1. 研究内容

　あるアルゴリズムに別のアルゴリズムを組み合わせることで、元のアルゴリズムの性能を向上させることを考える。今回は RSA 暗号アルゴリズムに最短経路問題を組み合わせることでセキュリティの向上を図った。

2. 研究方法

　実際に 2 つのアルゴリズムをどう組み合わせるか思考し、その短所を克服できる組み合わせ方をまた思考する。これを繰り返していった。

3. 研究結果・感想

　何度か思考を繰り返して最終的に、RSA 暗号の秘密鍵を最短経路問題を利用して隠す考えに行き着いた。RSA 暗号は素数同士の積の因数分解が困難であることを利用した暗号方式で、公開されている鍵（公開鍵）で平文を暗号化し、鍵を公開した人間に暗号文を送信する。鍵を公開した人間は公開した鍵以外にもう一つ鍵を持っており（秘密鍵）これを用いて暗号文を復号する。素因数分解の困難性が暗号の安全性と直結しているので、第三者が攻撃する方法は復号するための秘密鍵を盗聴することであると考えた。そのため秘密鍵を隠すという発想に至った。復号する人間は秘密鍵をそのまま手元に保管するのではなく、秘密鍵を別の形にして保管するのである。

　実際に考えた隠し方は、秘密鍵の数字と特定の最短経路問題の解の積 N を手元に置いておくことだ。その最短経路問題を解くアルゴリズムと、最短経路問題そのもの、N の三つを別々に格納し、秘密鍵が必要になったらこの三つを用いて復元することを考えた。

　この研究では既存のアルゴリズムを組み合わせて機能の向上、または新しいアルゴリズムの開発を目指したが、とても難しいことであることが判った。二つのアルゴリズムの性質をよく見極めて組み合わせなければいけず、研究の初期段階では長所をつぶしあって元より機能が劣ってしまう組み合わせもあった。そのアルゴリズムは何が問題でそれをどう改良するか、またその改良により他の影響はでてこないのか。新しいものを創り出すことの難しさを実感する研究であった。