研究テーマ：RSA 暗号と素数の不思議

名列番号　０６２　　宮本　一成

１．まえがき

RSA 暗号は、現在最も使われている公開鍵暗号方式である。ここでは、公開鍵暗号方式ができるまでの歴史、公開鍵暗号方式の社会的利用を主に研究した。

２．研究課題

暗号の歴史について調べる。
RSA の社会的利用について調べる。
暗号の実装としてアルベド語翻訳プログラムを作る。

３．研究方法

図書館の文献を調べ、さらにインターネットで最新の情報を得た。同じ暗号方式についても時代によって評価が異なっていたので、なるべく新しい情報を用いるようにした。

４．実験と考察

暗号の歴史を調べて、現在用いられているまでの暗号の変遷の様子がわかった。
現在では秘密鍵暗号方式では DES が、公開鍵暗号方式では RSA が主要である。今後は、RSA 方式に代わって楕円暗号方式が注目されている。楕円暗号方式は、RSA 方式よりも少ない時間で暗号でき、かつ安全性が RSA よりも高いからだ。
他には、**量子暗号方式**が注目されている。これは、盗聴された時に、**盗聴されたことが分かる**という、画期的な暗号方式である。
しかし、これらの暗号方式も、コンピュータの進化とともに破られてしまうかも知れない。今後の暗号技術に注目したい。
RSA 暗号方式に用いられるビットは、データ通信で用いる場合、**５６ビット**の暗号鍵が用いられている。
サーバの公開鍵は、非常に重要な鍵となるため、**１２８ビット**の暗号鍵が用いられていた。しかし、コンピュータの進化とともに、上記のビット数では安全と言えなくなってきたため現在では、**５１２ビット**の暗号鍵が用いられている。しかし、本当に安全と言いきるためには、**１０２４ビット**が推奨されている。
　アルベド語翻訳プログラムを実装したところ、hello が lammu となり、ちゃんとアルベド語に翻訳された。

５．まとめと今後の課題

今回の研究によって、暗号は、多くの科学者と長い年月によって現在に至るということがよく分かった。
ケース・バイ・ケースによって暗号方式を使い分けることが重要だ。
この自主課題研究を通して、暗号がいかにこのネットワーク社会において重要か、ということがよく分かった。

参考文献

辻井重男(1996)　講談社
暗号　ポストモダンの情報セキュリティ