暗号の歴史

情報システム工学科３年０５６　盛岡佑太

1.目的

私は暗号の攻撃方法に興味があり、最初はどのような暗号があるかを調べているとどの暗号にも攻撃方法が確立されているため暗号作成者と暗号解読者のどちらが優位に立っているかに興味をもち暗号の歴史を調べた。

2.調査内容

暗号とは第三者が通信文を見ても特別な知識「鍵」なしでは読めないようする変換方法である。方法として通信文を人目につかないような場所に記録するステガノグラフィと通信文をアルゴリズムにしたがって１ビットごとに置換や転置を行うサイファという方法がある。私はこのサイファと呼ばれる方法の暗号について調べた。

3.結論

今回の調査をふまえて暗号の歴史は暗号作成者と暗号解読者の戦いの歴史であり弱点を見つけるとそこを修正していくものであることがよくわかった。またほとんどの暗号が解読されていることがわかった。また現在の理論では量子暗号は解くことができないので暗号解読者のほうが有利である。

4.反省

本当はプログラムも作ってみたかったがプログラムの知識だけでなくサーバーの知識が必要なためうまくいかなかった。また機会があればサーバーの勉強をして簡単なＳＳｌを作ってみたい。