自主課題研究

工学部　情報システム工学科　3年　059　山田奈槻　0708060442

☆テーマ
暗号作りとその解読

☆概要
文献「数学で犯罪を解決する」よりテーマを選び、研究した。
自分の選んだテーマは「暗号作りとその解読」だったので、インターネット通信における暗号作りとその解読について、を取り上げ調査及び研究をした。

調査した主な内容は、今現在インターネット通信で使われている暗号化方法の種類とその内容、そしてその解読方法などについて。
調査には上記の文献「数学で犯罪を解決する」や「暗号技術大全」など他数冊とインターネットを使用した。

調査の結果、暗号化には主に共通鍵暗号（代表的なもの：DES）・公開鍵暗号（代表的なもの：RSA）などの方法が使われており、同時にその解読も進んでいるが、今のところ安全性が保たれていることもわかった。

また、パスワードを安全に保つためオンライン認証などで使われている“ハッシュ”についても調査した。
これはパスワードをハッシュ関数に従い別の文字列に変換し、ログインなどにはそのハッシュ版を使う、というもの。
このハッシュについては、自分でも簡単なハッシュ関数をC言語を用いて作り、暗号化を行ってみた。だが、実際に使われているハッシュ関数と比べて、自作プログラムの完成度は圧倒的に低かった。

更に、暗号化技術に対する解読についても調査した。
解読方法としては、主に総当り攻撃、単語を使った予測攻撃、確率論による予測攻撃、以前に解読したパスワードのデータを使った予測攻撃など、様々なものがある。
だが、それに対抗する策もあり、暗号化技術には取り込まれている。

以上のように、このテーマは完全にいたちごっこ状態であることがわかった。
現在は暗号化する際の暗号鍵を長くすることにより安全性が保たれている。