暗号研究

研究者：小野、勝野

１　はじめに

課題研究の選択時に暗号研究というものがあり、情報セキュリティに興味があった。そのため、暗号化技術を元に暗号機の製作をすることにした。

２　研究内容

歴史的に有名な暗号を調べ理解し、C 言語でプログラムして暗号化、復号化の様子を再現する。この暗号技術を元にハードウェア版とソフトウェア版とを二人で分担しオリジナル暗号機の製作をした。

３　研究過程

４月　　：歴史的な暗号の調査
５月～　６月：調査した歴史的な暗号を
　　C 言語で再現
７月～　８月：＜ハードウェア版＞
　　VHDL の演習
　　＜ソフトウェア版＞
　　C#の学習
９月～１０月：＜ハードウェア版＞
　　暗号機の制作
　　＜ソフトウェア版＞
　　歴史的な暗号を C#で再現
１１月　　：＜ハードウェア版＞
　　FPGA 基板のカバーを
　　加工
　　＜ソフトウェア版＞
　　オリジナル暗号の作成
１２月　　：レポートの作成
１月　　：レジュメ、プレゼンの作成

４　使用したソフト

・BCPad

＜ハードウェア版＞

・Xilinx　ISE 9.1i
・Adept

＜ソフトウェア版＞

・Microsoft Visual Studio

５　研究の成果

＜ハードウェア版＞

キーボードから平文を入力し、FPGA で処理し、PC を介さずにディスプレイに暗号を出力させることを目標に製作した。

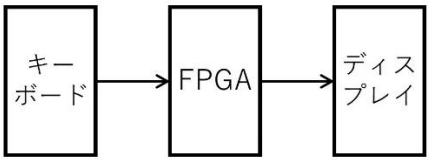

図１　暗号機の構成

FPGA 基板のスライドスイッチから鍵となるデータを入力し、それを用いて暗号化する。また、スライドスイッチの余ったところで暗号化の方法を変換する仕組みを VHDL でプログラムし、切り替えができるようにした。

図２　完成形

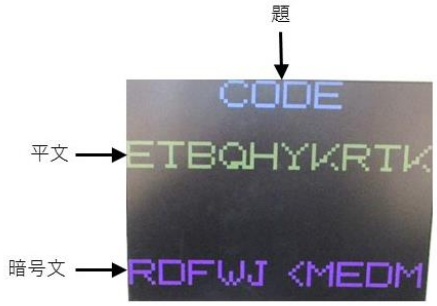

図３　暗号機の画面

上段に文字を入力すると、下段に暗号化された文字が表示されていく。文字数の制限は１０文字で空白も一文字として数えられる。

＜ソフトウェア版＞

オリジナル暗号を作成し、C#で暗号化ができるようにすることを目標に制作した。

```
char x;
int k;
char[] hai = textBox1.Text.ToCharArray();
k = int.Parse(textBox3.Text);
textBox2.Text = "";
for (int i = 0; i < hai.Length; i++)
{
    x = hai[i];
    x = (char)(x - 'A');
    x = (char)(25-x);
    x = (char)(x + k);
    x = (char)(x % 26 + 'A');
    textBox2.Text = textBox2.Text + x;
```

図４　プログラム画面

このプログラムでは平文を２５から引くことでアルファベットの逆から暗号化することができる。(例：ABC→ZYX)

逆にした平文に鍵の値を足すことで他の文字へシフトさせることができる。このオリジナル暗号はシーザー暗号と似ているが、アルファベットを逆にする処理をしているためシーザー暗号よりも強固な暗号といえる。

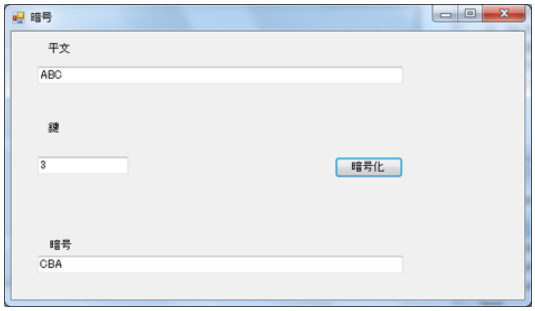

図５　実行結果

平文の枠に文字を入力し、鍵を指定して暗号化ボタンをクリックすると暗号化され、暗号の枠に表示される。

７　まとめ

オリジナル暗号を作成することで暗号化技術をより深く考えることができた。暗号化は情報セキュリティにとって必要不可欠な要素なので今後も勉強していきたい。

８　感想

【　小野　】

はじめは全く VHDL の知識がなくプログラムできるか不安だったが、演習を通し理解した。理解してからもつまずくことはあったが、最終的には自分が目標としていた暗号機を製作することができた。

【　勝野　】

オリジナル暗号が本当に作れるか不安で当初は C#の理解に苦しんだ。プログラミングに慣れてからはスムーズに制作を進めることができた。オリジナルの難しい暗号を考案したが復号の処理に苦労した。なんとか作品にまとめることができた。難しい課題だったが、自分の思うようにできたのでよかった。