暗号研究

研究者：天池　太治、岩田　陽介
河合　佑斗、渡邊　俊也

１　はじめに

「エニグマ」と呼ばれる第二次世界大戦で使用されたエニグマという暗号機のシミュレータをFPGA で制作しながら暗号変換の仕組みについて研究した。

２　研究過程

６月　：調べ学習及びテーマ決め
７月　：FPGA での演習
８月　：FPGA での応用演習
９月　：エニグマ製作
１０月　：システム作成
１１月　：システム作成
１２月　：エニグマ操作ボックス製作

３　FPGA とは

FPGA とは論理回路設計を誤ったとしても即座にその場で何度も書き換え修正が可能なプログラマブルロジックデバイスである。プログラムには VHDL と呼ばれるアメリカ国防総省が開発したハードウェア記述言語を使用している。

VHDL（画像表示部分）

４　研究内容

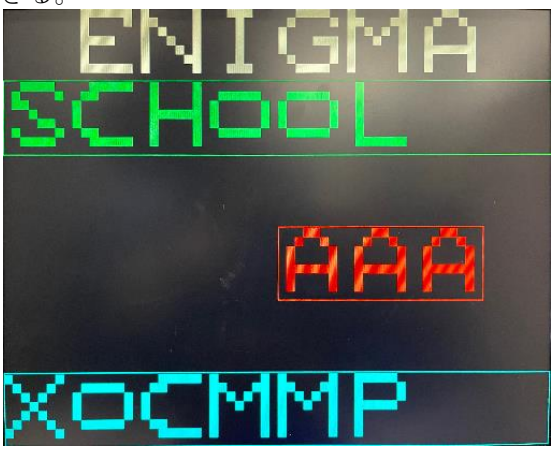
本研究では、エニグマを製作するための作業分担として、まず FPGA を用いた画像表示を岩田が、エニグマの操作ボックス製作を天池、暗号表変換処理を河合が、暗号復合化ソフト作成を渡邊が担当し、FPGA ボードの使い方や Java プログラミングの方法を学習しながら製作を進めた。

```
process(CLK25)
begin
if CLK25'event and CLK25='1' then
if(h_counter<799) then
h_counter<=h_counter+1;
else
h_counter<="0000000000";
if(v_counter<520) then
v_counter<=v_counter+1;
else
v_counter<="0000000000";
end if;
end if;
end if;
end process;
HS<='0' when h_counter>=640+16 and
        h_counter<640+16+96 else'1';
VS<='0' when v_counter>=480+10 and
        v_counter<480+10+2 else'1';
blank<='0' when h_counter>=640 or
        v_counter>=480 else '1';
```

５　研究成果

（１）FPGA での画像表示

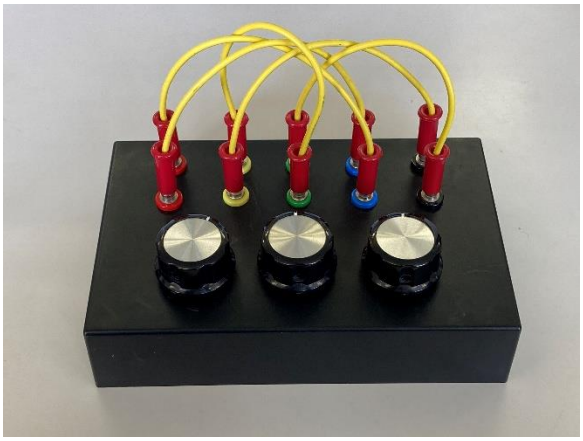
FPGA の VGA インタフェースを利用して A～Z までの文字を画面に表示できるようになった。起動時のタイトル表示や平文のキーボードから入力された文字がエニグマシミュレータで暗号化されていく様子をディスプレイに表示することができる。



エニグマの文字入力画面

（２）操作ボックス製作

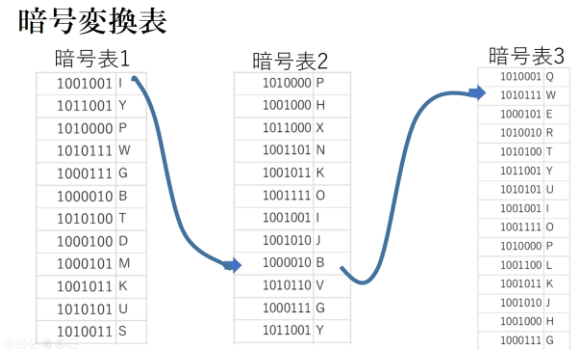
暗号の KEY に相当するエニグマのローター（歯車）の代わりにロータリーエンコーダを３個取り付けた。回しやすいように大きめのダイヤルのつまみも取り付けた。また、入力した単語の文字コード文字コードを５ビットの間で入れ替えるためのプラグ端子を取り付けた。



製作した操作ボックス

（３）エニグマの暗号変換

ランダムに換字処理を行うための「暗号変換表」の作成と FPGA によるプログラミングを行った。これのおかげでエニグマ自体での暗号化がやっと可能になる。また、キーボードと FPGA を接続して、キーボードからシリアルで送られてくるスキャンコードを文字コードに変換してモニター上で文字を表示させることができるようにした。



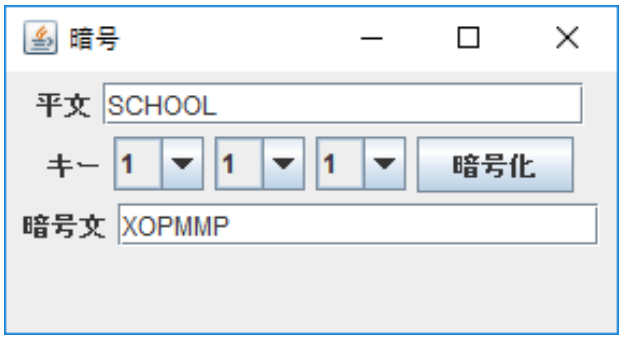
作成した暗号変換表

（5）ソフトウェア版エニグマの作成

使用したプログラム言語は Java である。実際に暗号化を行う場所であるウィンドウの作成には、使用言語の Java にあらかじめ入っている「Swing」を使用してプログラム作成を行った。

```
import javax.swing.JFrame;↓
import javax.swing.JTextField;↓
import javax.swing.JLabel;↓
```

```
flow = new FlowLayout();↓
text = new JTextField(20);↓
text1 = new JTextField(20);↓
String[] combodata = {"1","2","3","4","5","6","
combo1 = new JComboBox(combodata);↓
String[] combodata2 = {"1","2","3","4","5","6",
combo2 = new JComboBox(combodata2);↓
String[] combodata3 = {"1","2","3","4","5","6",
combo3 = new JComboBox(combodata3); ↓
```



実際に暗号化を行うウィンドウの図

ハードウェア版と同様に平文を入力するとキーの値に合わせて暗号文が出力される。

6　まとめ

（1）　成果

今回の研究を通して、FPGA ボードや VHDL でのプログラミングや動作実験を通して班員全員が知識を深めることができた。知識が乏しい状態での暗号研究のスタートであったが、試行錯誤や成功・失敗を繰り返して製作に取り組んだおかげで今回の目標であった「エニグマシミュレータの製作」という目標を無事に達成できた。暗号研究のおかげで個人個人がいろいろな面において成長できたと感じた。

（2）課題

製作したシミュレータはエニグマ本来の仕組みをまだ完全に再現できていない。エニグマのスクランブラーの部分で平文をキーボードで打つごとに英字が記された歯車が連動して動き、暗号化がさらに複雑なものになっている。また、入力の文字を消して誤再入力できるようにしたい。

7　チームの感想

【　岩田　陽介　】

はじめは無知の状態だったので戸惑うことを多々あったが、分からないことは先生に聞きそれ以外は自力で考え、より良いものを作ろうと放課後や家で試行錯誤することができた。自分の力量を深く知ることができたのでよかった。

【　天池　太治　】

今回の暗号研究では、途中でプログラムや加工作業でのミスが多発することがよくあって何度も心が折れそうになった場面があったが、周りのメンバーの支えのおかげでエニグマを完成させることができて嬉しさと感謝で一杯である。

【　河合　佑斗　】

暗号を製作するということは初めての行いだったので変換の仕組みやプログラミングなど大変であったが、放課後の時間などを用いてエラーの修正を行い合作のプログラムを完成させることができ達成感であふれている。

【　渡辺　俊也　】

今回の課題研究では自分の作業はほかの 3 人と違い、自分だけ Java を使い作業をしていたので個人製作のように一人で作業することになっていたのでとてもきつかったのでプログラムは完成までとても苦労した。