ECSE 323 — Group 47 Lab 5 Enigma Machine

Jun Young Shin id. 260499663
Timothee Flichy id. 260557686

April 15, 2016

1 Introduction

The enigma machine is a cipher machine which encrypts a string of words or numbers so that a non partisan will not be able to understand the message. This system was extensively used during the world war 1 and 2 by Germany to plan strategic assault to enemy territory. to encrypt the message, the machine used a set of mechanical rotors and electrical circuit. The each rotor can be set by rotating the rotor and ring, and by changing the encryption type. In total, there is 3 independent rotors. In the electrical circuit, there is a circuit called a reflect and stecker which creates another level of encryption by generation a secondary pattern. This complex encryption system is able to create over 158 million million million combinations with 10 pairs of 26 letters. This makes it almost impossible for a human to decrypt the code. To make it even harder and increase the odd, the combination was changed every 24 hours during world war 2. In the course of Digital System Design, we used VHDL to write electronic version of this mechanical system. This report will explain the procedure of creating this device using the Altera board.

2 Designing of the Enigma machine

Before jumping into the VHDL, we first must understand how to implement the mechanical machine to a hardware. In our case the Altera's Cyclone II FPGA model EP2C20F484C7. In figure 1 we can see how the hardware will work.

So here is how the enigma machine will work on the FPGA. The user inputs a letter to be encrypted. When the

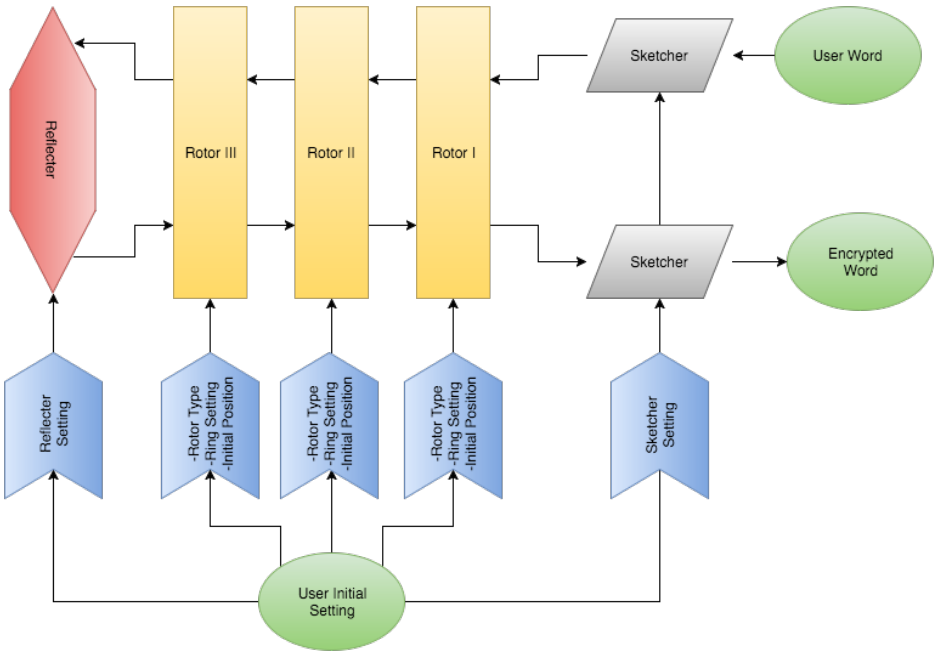

Figure 1: Block diagram of the enigma machine.

user click a button called a key_press, the program receives the letter and sends it to the stecker. Stecker meaning

plugboard in German, is a simple version of a fixed rotor. It then passes through the first rotor to get the first encryption. The encryption pattern in shown in figure 2. The encrypted letter will then pass to the second rotor and to the third rotor.

It will then pass to the reflector which does another encryption. The reflector will encrypt the letter to its mirrored.

INPUT	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Rotor I	E	K	M	F	L	G	D	Q	V	Z	N	T	O	W	Y	H	X	U	S	P	A	I	B	R	C	J
Rotor II	A	J	D	K	S	I	R	U	X	B	L	H	W	T	M	C	Q	G	Z	N	P	Y	F	V	O	E
Rotor III	B	D	F	H	J	L	C	P	R	T	X	V	Z	N	Y	E	I	W	G	A	K	M	U	S	Q	O
Rotor IV	E	S	O	V	P	Z	J	A	Y	Q	U	I	R	H	X	L	N	F	T	G	K	D	C	M	W	B

Figure 2: Encryption pattern for the rotor.

Meaning, if $'A'$ is mirrored with $'Y'$, if any of the letter is passed to the reflector, the mirrored letter will to output it. The encryption of the reflector can be seen in figure 3.

The reflected letter will then pass back to the third rotor, to the second rotor, and to the first rotor. It finally

reflector B	(AY) (BR) (CU) (DH) (EQ) (FS) (GL) (IP) (JX) (KN) (MO) (TZ) (VW)
reflector C	(AF) (BV) (CP) (DJ) (EI) (GO) (HY) (KR) (LZ) (MX) (NW) (TQ) (SU)

Figure 3: Encryption pattern for the reflector.

come back to the stecker which output the encrypted letter.

The user will initialize the enigma machine. There are multiple setting that can be configured.

3 User Interface