Project: Enigma Machine and Turing-Welchman Bombe

Maria Camila REMOLINA GUTIÉRREZ maria.remolina_gutierrez@telecom-sudparis.eu

Advisor: Prof. Eric RENAULT

June 19, 2019

Abstract

This is the work proposal to follow in the course Project as part of the master M1 in Computer Science and Communication Networks at Télécom SudParis. The goal is to implement the Enigma machine used in World War II, followed by the Bombe machine that breaks the cipher, created by Alan Turing and Gordon Welchman at Bletchley Park.

1 Introduction

The enigma machine is a cipher machine used by the Nazi Germany during World War II in order to send secret coded messages. It was initially a commercial machine bought by banks are businesses. But then the military took it and added an extra security layer called plugboard. It was innovative at the time because it was not a substitution cipher, i.e. the same letter can get different results after encryption.

The machine works by a combination of moving rotors and inside wiring as seen in Fig. 1. The way to use it is that when the sender types a message, a bulb lights up indicating the correspondent coded letter. Then, in order to decode, the receiver types the coded message he received and the initial message lights up on the board. In war times the coded messages were transmitted over morse code.

In the military version of the Enigma Machine there were 5 possible rotors to pick from, each with 26 possible positions, then there were 10 possible switching in the plugboard that could choose a pair from the available 26 letters. That accounts for 15896255217826360000 different combinations for the setting of the army Enigma Machine [2]. The initial setting for each day was given to the bases in a sheet of paper that



Figure 1: Enigma Machine - Military Edition

had the monthly configurations of the machine. So they changed the setting everyday.

So in order to decipher the code, you needed either to have the code sheet or to break the message. This latter was what the scientists at Bletchley Park did; and what I will try to recreate in this project.

2 General Goal

To understand the code breaking process behind the enigma cipher.

3 Specific Goals

- To implement the Enigma machine with software
- To implement the Bombe machine that breaks the Enigma cipher
- To understand the mathematical and probabilistic techniques used to break a cipher with limited time and computational resources.

• To understand the weaknesses exploited that allowed to break the Enigma cipher

4 Implementation

I implemented a project in the Python programming language that replicates both the Enigma Machine and the Bombe Machine. I explain in the following subsections the details of each of them.

4.1 Enigma Machine

There are different models of the Enigma machine that were developed through time. In this project I chose one of the latest, i.e. with more complicated settings. This is the model M3 & M4 Naval (from Frebuary 1942) that has 8 possible rotors [8, 9].

4.1.1 Enigma's algorithm

The enigma machine consists on a set of physical connections that allow electrical signals to travel through inner cross wirings that move place every time a key is pressed. In the most simple form we could express that any typed key in the keyboard is transformed to another letter that lights up in the bulbs panel. So we could say:

$$SIGNAL_{OUT} = P(S(P(SIGNAL_{IN})))$$

$$S(SIGNAL) = R_1(R_2(R_3(F(R_3(R_2(R_1(SIGNAL)))))))$$

Where P represents the Plugboard; S represents the Set of rotors an reflectors; R_i represents the i-th rotor (in this case there are 3 but there could be more); and F represents the reflector. All of this process can be graphically understood with the image below (Fig. 2):

The machine has a symmetric property so in order to decipher the message one has to put the same rotor settings as when the person typing the message started. So this leads us to the configuration of the machine, i.e. the input.

4.1.2 Input

The machine has different settings that changed each day and that were communicated via code sheets like the one in Fig. 3.

I handle this as a configuration text file in my implementation. I will describe the components as follows:

• Rotor selection and order: Depending on the machine there are up to 8 different rotors (I-VIII) from which to choose 3 or 4. So an input is which of them and in which permutation from left to right. Example - V IV I.

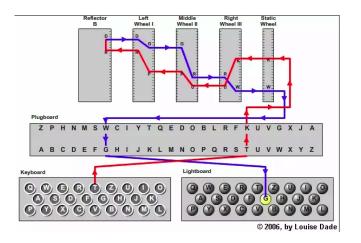


Figure 2: Enigma Machine Wiring

31.	QK PC VY GA SO EM may vts gvt csx FK AR WH SO NJ DG aky vdv oyo tzt HV UU GK FW PZ XC nfh vco tur wnb WQ TY HE JU XN KD bec jmv vtp xdb MG TY HE JU XN KD bec jmv vtp xdb MG TY HE JU XN KD bec jmv vtp xdb MG TY HE JU XN KD bec jmv vtp xdb MG TY HE BD YW wtw yem vtp ydg vsm MG TY CG RW LT LT ded vdg vsm mt lt lt		4		ı	rupper	Kenng	l l			n	unge	bind	rver	tocke	Sı			ıng	ngstellu	Rin	ige	alzenla	M.	atum
V V I O4 25 O1 DI ZL RX UH QK PC VY GA SO EM mqy vts gvt csx	FK AR WH SO NJ DG Aky vdv oyo tzt HV IU GK FW PZ XC nfh vco tur wnb WQ TY HE JU XN KD bec jmv vtp xdb HI BO JP UZ FT RN WF LJ OT EN BD YW ktv muq cqm cpm QS OV ZA GW CH XF EB YN CO IK WE GZ NU MD SA ZK QR LT HD RG KM BL NS JW EX WR BJ DK FU LA JP YU EF TB ZL XQ AJ UO CN BV TM KI PK JX RS GF IA QH GF BH TK QE AR OP NX PR WL GA BU SF JA VD OI HK NX ZS WM TR XU FO ZB ED TW GV FB ZL EQ OX SU DK IT FY BL AZ EG PC VD KI XH WZ JS CX PT YB ZG MU DS HR CV XE QV NT WW LW MW DX NG CY UE MhW DX NG CY UE mhw lwb mdm ybe myb mdm Myb m		, 1		gví	xxo	vuc	yqv	ZK	XP	RL	WI	QC	OU	HG	AY	SD	BF	02	14	10	v	II	I	31.
28. I III II 09 16 12 NE MT RL OY HV IU GK FW PZ XC nfh vee tur wnb 27. III II 1 06 03 15 BF GR SZ OM WQ TY HE JU XN KD bec jmv vtp xdb 28. I III V 19 26 08 GS VD CQ LE HI BO JV UX KD bec jmv vtp xdb 29. III I IV 05 01 16 KA ZH QP GR MF LJ OT EN BD YW ktv muq cqm cpm 24. III II IV 22 02 02 06 PI KM JB YU QS OV ZA GW CH XF Zcd iwo urp glg 23. IV III I 08 11 07 SX TD QP HU FB YN CO IK WE GZ 25. I V II 13 02 26 GP XH IW BO NU MD SA ZK QR LT aam mvy jqq wqm 21. IV I V 17 24 03 XC AQ OT UZ HD RG KM BL NS JW 1tl blu frk xrh 19. V I III 13 24 21 PO TV QC ZS EX WR BJ DK FU LA 19. V I III 13 24 21 HA GM DI VK JP YU EF TB ZL XQ ecd ciq uvr ppt 18. IV V I 28 09 90 XF FZ SQ GR AJ UO CN BV TM KI 11. II V V 17 24 05 XF XF SQ GR AJ UO CN BV TM KI 11. II V V 17 24 15 UT ZC YN BE PK JX RS GF, IA QH 18. IV III V 07 01 13 IN YJ SD UV GF BH TK QE AR OP 15. IV III V 07 01 13 IN YJ SD UV GF BH TK QE AR OP 16. IV III V 10 23 21 WT RE PC FY JA VD OH HK NX ZS 12. IV RS 11 IV V 13 15 11 NX EC RV GP SU DK IF FY BL AZ 11. IV V 13 15 11 NX EC RV GP SU DK IF FY BL AZ 29 in qub cob vef plu cm 1di ods 12. II V II 10 25 VK DW LH RF JS CX PT YB ZG MU nyh fbd ohs Jrp 8. IV V I 12 20 416 PV XS ZU EQ BW CH XF EQ VNT UWW Valle mww val	HV IU GK FW FZ XC WQ TY HE JU XN KD HI BO JP UZ FT RN MF LJ OT EN BD YW QS OV ZA GW CH XF FS YN CO IK WE GZ RU MD SA ZK QR LT HD RG KM BL NS JW TX WR BJ DK FU LA DY YU EF TB ZL XQ AJ UO CN BV-TM KI PK JX RS GF IA QH OUB GF BH TK QE AR OP NX PR WL GA BU SF JA VD OI HK NX ZS WM TR XU FO ZB ED TW GY FS ZL EQ OX SU DK IT FY BL AZ EG PC VD KI XH WZ DS HR CV XE QV NT DW HAD NG W ND DS HR CV XE QV NT UWW WARK IT mgd				csx	gvt	vts	mqy			GA	VY	PC	QK	UH	RX	ZL	DI	01	25	04	I			
27. III II I	WQ TY HE JU XN KD HI BO JP UZ FT RN WYU yem buz rjk MY LJ OT EN BD YW Ktv muq cqm cpm QS OV ZA GW CH XF FB YN CO IK WE GZ FB YN CO IK WE GZ FB YN CO IK WE GZ HD RG KM BL NS JW HT LA HO CN BV TM KI FJ 2ts uqu cft QC ciq uvr ppt AJ UO CN BV TM KI FJ 2ts uqu cft QC ecd ciq uvr ppt KI FJ 2ts uqu cft QC PW YN MY RS GF, IA QH CF BH TK QE AR OP Kex paw flw onw NX PR WL GA BU SF JA VD OI HK NX ZS WM TR XU FO ZB ED TW GV FB ZL EQ OX ASY XZB uvc fmr SU DK IT FY BL AZ BC PY YB ZG MU NT BY TW BW CH AO RL JN TD HW FM DX NG CY UE NTW WL WAL TH mgd				tzt	оуо	vdv	aky	ĎG	NJ	SO	WH	AR	FK	YX	TP	BQ	ZM	06	11	13	II	V	III	29.
26. I III V 19 26 08 GS VD CQ LE HI BO JP UZ FT RN	HI BO JP UZ FT RN MF LJ OT EN BD YW QS OV ZA GW CH XF EB YN CO IK WE GZ NU MD SA ZK QR LT HD RG KM BL NS JW EX WR BJ DK FU LA JP YU EF TB ZL XQ AJ UO CN BV- TM KI PK JX RS GF IA QH OF BH TK QE AR OP NX PR WL GA BU SF JA VD OI HK NX ZS WM TR XU FO ZB ED TW GV BF ZL EQ OX SU DK IT FY BL AZ GG PC VD KI XH WZ JS CX PT YB ZG MU DS HR OX NG CY UE WW CH AO RL JN TD HW FM DX NG CY UE DS HR CV XE QV NT WWW WRW LCD TR WWW MR DX NG CY UE MW UWW WORK LTH mgd				wnb	tur	vco	nfh	XC		FW	GK	IU	HV	OY	RL	MT	NE	12	16	09	II	III	I	28.
25. II I I IV 05 01 16 KA ZH QP GR MF LJ OT EN BD YW	MF LJ OT EN BD YW QS OV ZA GW CH XF FB YN CO IK WE GZ NU MD SA ZK QR LT HD RG KM BL NS JW TX WR BJ DK FU LA JP YU EF TB ZL XQ AJ UO CN BV TM KI AJ UO CN BV TM AJ UN CN BV TM AJ UO CN BV AJ UO CN BV TM AJ UO CN BV TM AJ UO CN BV AJ UO CN BV AJ UO CN				xdb	vtp	jmv	bec			JU	HE	TY	WQ	OM	SZ	GR	BF	15	03	06	I	II	III	27.
24. III II IV	QS				rjk	·buz	yem	wvu										GS	08	26	19	V	III	I	26.
23. IV III II 08 11 07 SX TD QP HU FB YN CO IK WE GZ ePm mgz vqg vsm 22. I V II 13 02 26 GP XH IW BO NU MD SA ZK QR LT aam myy jqq wqm 21. IV I V 17 24 03 XC AQ OT UZ HD RG KM BL NS JW 1tl blu frk xrh 20. IV I III 15 22 12 PO TV QC ZS EX WR BJ DK FU LA non lic oxr usr 19. V I III 13 24 21 HA GM DI VK JP YU EF TB ZL XQ ecd ciq uvr ppt 18. IV V I 23 09 20 XF PZ SQ GR AJ UO GN BV TM KI 17. III IV 21 24 15 UT ZC YN BE FF JX RS GF IA QH oub eci pyf rqi 16. IV III V 07 01 13 IN YJ SD UV GF BH TK QE AR OP 15. I IV II 15 04 25 TM IJ VK OY NX PR WL GA BU SF 18. V II 15 04 25 TM IJ VK OY NX PR WL GA BU SF 18. V II 16 04 25 TM IJ VK OY NX PR WL GA BU SF 18. V II 17 14 04 12 AN IV LH YP WM TR XU FO ZB ED 18. V II 19 07 19 02 HR NC IU DM TW GV FB ZL EQ OX asy xza uvc fmr 11. I V IV 13 15 11 NX EG RV GP SU DK IF FY BL AZ gyd iuq ocb vef 10. V II I 09 20 19 FN TA YJ SO EG PC VD KI XH WZ PYZ AGE PTU Uyc 19. IV V 14 10 25 VK DW LH RF JS CX PT YB ZG MU 19. fbd ohs Jrp 8. IV V I 22 04 16 PV XS ZU EQ BW CH AO RL JN TD tck rts nro mkl 7. V I IV 18 11 25 TS IK AV QP HW FM DX NG CY UE mhw lab mdm ybe 6. IV I II V 26 09 14 VW LT PB FO ZK GS RI QJ HW XE SU BY LTH mgd 5. I V IV 26 09 14 VW LT PB FO ZK GS RI QJ HW XE SUW by 10. IN WD 11. I WW WALL IN MPD 15. I V II V 26 09 14 VW LT PB FO ZK GS RI QJ HW XE SUW by 10. IN WD 11. II WW WALL IN MPD 15. I V IV 26 09 14 VW LT PB FO ZK GS RI QJ HW XE SUW by 10. IN MPD 15. I V III V 26 09 14 VW LT PB FO ZK GS RI QJ HW XE SUW by 10. IN MPD 15. I V III V 26 09 14 VW LT PB FO ZK GS RI QJ HW XE SUW by 10. IN MPD 15. I V III V 26 09 14 VW LT PB FO ZK GS RI QJ HW XE SUW by 10. IN MPD 15. I V III V 26 09 14 VW LT PB FO ZK GS RI QJ HW XE SUW by 10. IN MPD 15. II W VI V 26 09 14 VW LT PB FO ZK GS RI QJ HW XE SUW by 10. IN MPD 15. III NW 15. III NW 15. III NW III WW LT WW LT PB FO ZK GS RI QJ HW XE SUW by 10. IN MPD 15. IN MPD 15. II W VI V 26 09 14 VW LT PB FO ZK GS RI QJ HW XE SUW by 10. IN MPD 15. IN MPD 15. III NW VI V 26 09 14 WW LT PB FO ZK GS RI QJ HW XE SUW by 10. IN MPD 15. III NW VI V 26 09 14 VW	FB YN CO IK WE GZ NU MD SA ZK QR LT HD RG KM BL NS JW EX WR BJ DK FU LA JP YU EF TB ZL XQ AJ UO CN BV- TM KI FJ 2ts uqu cft OTH BH TK QE AR OP NX PR WL GA BU SF JA VD OI HK NX ZS WM TR XU FO ZB ED TW GV BF ZL EQ OX SU DK IT FY BL AZ EG PC VD KI XH WZ JS CX PT YB ZG MU DX NR CH AO RL JN TD HW FM DX NG CY UE BW MM TR XU RO CO CO CO CO SU DK IT FY BL AZ BG PC VD KI XH WZ JS CX PT YB ZG MU DX HT FM DX NG CY UE DX HT MM				cpm	cqm	muq	ktv							GR	QP	ZH	KA	16	01	05	IV	I	II	25.
22. I V II 13 02 26 GP XH IW BO NU MD SA ZK QR LT aam mvy jqq wqm 21. IV I V 17 24 03 XC AQ OT UZ HD RG KM BL NS JW 22. IV I V 17 24 03 XC AQ OT UZ HD RG KM BL NS JW 23. IV I III 15 22 12 PO TV QC ZS %X WR BJ DK FU LA non lic oxr usr 19. V I III 13 24 21 HA GM DI VK JP YU EF TB ZL XQ ecd ciq uvr ppt 18. IV V I 28 09 80 XF PZ SQ GR AJ UO CN BV TM KI fjh zts uqu cft 19. III II V 21 24 15 UT ZC YN BE PK JX RS GF IA QH OU eci pyf rqi 16. IV III V 07 01 13 IN YJ SD UV GF BH TK QE AR OP kex paw flw onw 15. I IV III V 10 23 21 WT RB PC FY JA VD OI HK NX ZS mbz lff lnq giy 18. V F II 14 04 12 AN IV LH YP WM TR XU FO ZB ED rqh ucm ldi ods 12. II Y I 07 19 02 HR NC IU DM TW GV FB ZL EQ OX asy xza uvc fmr 18. I V II 15 55 11 NX BO RV GP SU DK IT FY BL AZ gyd iuq ocb vef 19. I IV V 14 10 25 VK DW LH RF JS CX PT YB ZG MU 19. I IV V 14 10 25 VK DW LH RF JS CX PT YB ZG MU 19. I IV V 14 10 25 VK DW LH RF JS CX PT YB ZG MU 19. I IV V 14 10 25 VK DW LH RF JS CX PT YB ZG MU 19. I IV V 14 10 25 VK DW LH RF JS CX PT YB ZG MU 19. I IV V 14 10 25 VK DW LH RF JS CX PT YB ZG MU 19. I IV V 14 10 25 VK DW LH RF JS CX PT YB ZG MU 19. I IV V 14 10 25 VK DW LH RF JS CX PT YB ZG MU 19. I IV V 14 10 25 VK DW LH RF JS CX PT YB ZG MU 19. I IV V 14 10 25 VK DW LH RF JS CX PT YB ZG MU 19. I IV V 18 11 25 TS IK AV QP HW FM DX NG CY UE mhw lwb mdm ybe 19. I V II V 26 09 14 VW LT PB FO ZK GS RI QJ HM XE sw tsy nfp yjc 19. I V III V 26 09 14 VW LT PB FO ZK GS RI QJ HM XE sw tsy nfp yjc 19. IV III V 26 09 14 VW LT PB FO ZK GS RI QJ HM XE sw tsy nfp yjc 19. IV III V 26 09 14 VW LT PB FO ZK GS RI QJ HM XE sw tsy nfp yjc 19. IV III V 26 09 14 VW LT PB FO ZK GS RI QJ HM XE sw tsy nfp yjc 19. IV III V 26 09 14 VW LT PB FO ZK GS RI QJ HM XE sw tsy nfp yjc 19. IV III V 26 09 14 VW LT PB FO ZK GS RI QJ HM XE sw tsy nfp yjc 19. IV III V 26 09 14 VW LT PB FO ZK GS RI QJ HM XE sw tsy nfp yjc	NU MD SA ZK QR LT				glg	urp	iwo	zcd						QS	YU	JB	KM	PI	06	02	22	IV	II	III	24.
21. IV I V 17 24 03 XC AQ OT UZ HD RG KM BL NS JW 1tl blu frk xrh non, lic oxr usr 19. V I III 15 22 12 PO TV QC ZS EX WR BJ DK FU LA non, lic oxr usr 19. V I III 13 24 21 HA GM DI VK JP YU EF TB ZL XQ ecd ciq uvr ppt 18. IV V I 23 09 80 XW PZ SQ GR AJ UO CN BV TM KI 6jh zts uqu cft 17. III II V 21 24 15 UT ZC YN BE PK JX RS GF IA QH OD OW 15. I IV III 15 04 25 TM IJ VK OY NX PR WL GA BU SF 8dr pbu byv khb 14. III II IV 10 25 21 WT RE PC FY JA VD OI HK NX ZS 8dr pbu byv khb 14. III II V 10 25 21 WT RE PC FY JA VD OI HK NX ZS 8dr pbu byv khb 18. III IV I 06 25 21 WT RE PC FY JA VD OI HK NX ZS 8dr pbu byv khb 19. III Y I 07 19 02 HR NC IU DM TW GV FB ZL EQ OX asy xza uvc fmr 11. I V IV 13 15 11 NX EO RV GP SU DK IT FY BL AZ gyd iuq ocb vef 19. III V 1 09 20 19 FN TA YJ SO EG PC VD KI XH WZ Pyz ace pru uyc 19. I IV V 14 10 25 VK DW LH RF JS CX PT YB ZG MU 19. IV P TO 05 05 07 07 09 02 07 07 09 XS ZU EQ BW CH AO RL JN TD tck rts nro mkl 17. V I IV 18 11 25 TS IK AV QP HW FM DX NG CY UE mhw lwb mdm ybe 15. I V VI 12 07 01 12 QS YA XW KR MP HT DU OV CL FZ uby usi min mwb	HD RG KM BL NS JW SX WR BJ DK FU LA JP YU EF TB ZL XQ ecd ciq uvr ppt AJ UO CN BV TM KI FJh zts uqu cft pK JX RS GF, IA QH GF BH TK QE AR OP NX PR WL GA BU SF JA VD OI HK NX ZS WM TR XU FO ZB ED TW GV FB ZL EQ OX SSU DK IT FY BL AZ EG PC VD KI XH WZ JS CX PT YB ZG MU DS HR CV XE QV NT WWW TR DX NG CY UE mhw Lyb mdm ybe bb HR CU XE QV NT www wydk lrh mgd	1.3			vsm	yqg	mgz	epm					YN		HU	QP	TD,	SX	07	11	08	ľI	III	IV	23.
20. IV I III	EX WR BJ DK FU LA JP YU EF TB ZL XQ AJ UO CN BV- TM KI PK JX RS GF IA QH OF BH TK QE AR OP NX PR WL GA BU SF JA VD OI HK NX ZS WM TR XU FO ZB ED TW GV BF ZL EQ OX SU DK IT FY BL AZ EG PC VD KI XH WZ JS CX PT YB ZG MU Nyh Fbd ohs JR PV WS BG WS BG WC H AO RL JN TD HW FM DX NG CY UE DS HR CU XE QV NT UNW WWL WAK LTH mgd				wqm	jqq										IW.	XH	GP	26	02	13	II	V	I	22.
19.	JP YU EF TB ZL XQ	11			xrh	frk		1tl										XC	03	24	17	V	I	IV	21.
18.	AJ UO CN BV TM KI PK JX RS GF, IA QH GF BH TK QE AR OP NX PR WL GA BU SF JA VD OI HK NX ZS WM TR XU FO ZB ED TW GV FB ZL EQ OX SU DK IT FY BL AZ EG PC VD KI XH WZ JS CX PT YB ZG MU BW CH AO RL JN TD HW FM DX NG CY UE DS HR CU XE QV NT WWW TR X DT OZ U TW GV FB ZL EQ OX ASY XZE UVC fmr SU DK IT FY BL AZ EG PC VD KI XH WZ TY BZ GW NYh fbd ohs Jrp tck rts nro mkl mhw Lwb mdm ybe DS HR CU XE QV NT UWW Wdk lrh mgd					oxr		non										PO	12	22	15	III	I	IV	20.
17.	PK JX RS GF IA QH GF BH TK QE AR OP NX PR WL GA BU SF Sdr pbu byv khb NX PR WL GA BU SF JA VD OI HK NX ZS WM TR XU FO ZB ED TW GV FB ZL EQ OX SU DK IT FY BL AZ EG PC VD KI XH WZ JS CX PT YB ZG MU Nyh fbd ohs Jrp BW CH AO RL JN TD HW FM DX NG CY UE DS HR CU XE QV NT Uwww ydkk lrh mgd					uvr	ciq											HA	21	24	13	III	I	V	19.
16. IV III V 07 01 13 IN YJ SD UV GF BH TK QE AR OP kex paw flw onw str plus byv khb that it is in the str plus byv khb that is in the str plus byv khb that it is in the str plus byv khb that it is in the str plus byv khb that it is in the str plus byv khb that it is in the str plus byv khb that it is in the str plus byv khb that it is in the str plus byv khb that it is in the str plus byv khb that it is in the str plus byv khb that it is in the str plus byv khb that it is in the str plus byv khb that it is in the str plus byv khb that it is in the str plus byv the str plu	GF BH TK QE AR OP NX PR WL GA BU SF Sdr pbu byv khb sdr pbu byv khb sdr pbu byv khb sdr pbu lev lev khb sdr pbu byv khb sdr pbu lev				oft-		zts	fjh											80	09	23	-I	¥	IV	18.
15.	NX				rqi		eci	.oub												24	21	V	II	III	17.
14. III II V 10 25 21 WT RE PC FY JA VD 01 HK NX ZS mhz lff lnq giy 13. V F II 14 04 12 AN IV LH YP WM TR XU FO ZB ED rqh ucm ldi ods 12. II Y I 07 19 02 HR NC IU DM TW GV FB ZL EQ 0X asy xza uve fmr 11. I V IV 15 15 11 NX EO RV GP SU DK IT FY BL AZ gyd iuq och vef 10. V II I 09 20 19 FN TA YJ SO EG PC VD KI KH WZ pyz ace pru uyc 9. I IV V 14 10 25 VK DW LH RF JS CX PT YE ZG MU nyh fbd ohs jrp 8. IV V I 22 04 16 PV XS ZU EQ BW CH AO RL JN TD tck rts nro mkl 7. V I IV 18 11 25 TS IK AV QP HW FM DX NG CY UE mhw lwb mdm ybe 15. IV IV 26 09 14 VW LT PB FO ZK GS RI QJ HM XE Suw tsy nfp yd 54 IV III V 07 01 12 QS YA XW KR MP HT DU 0V CL FZ uby usi min mwb	JA VD OI HK NX ZS mhz lff lnq gly WM TR XU FO ZB ED rqh ldi ods TW GV FB ZL EQ OX asy xza uve fmr SU DK IT FY BL AZ gyd iuq ocb vef EG PC VD KI MW Z Dyz ace pru uyc JS CX PT YB GG MU nyh fbd ohs jrp BW CH AO RR JN TD tck rfs nro mkl HW FM DX NG CY UE mhw lwb ndm ybe DS HR CU XE QV NT uww vdk lrh mg	1						kex											13	01	07	V	III	IV	16.
13.	WM TR XU FO ZE ED rqh ucm Idi ods TW GV FB ZL EQ OX asy xza uvc fmr SU DK IT FY BL AZ gyd iug oob vef BG PC VD KI XH WZ pyz ace pru uyc JS CX PT YB ZG MU nyh fbd ohs jrp BW CH AO RL JN TD tck rts nrq mkl HW FM DX NG CY UE mhw lwb ndm ybe DS HR CU XE QV NT uwu vdk lrh mg							sdr											25	04	.15	II	IA	I	15.
12. II Y I 07 19 02 HR NC IU DM TW GV FB ZL EQ OX asy xza uvc fmr 11. I Y IV 13 15 11 NX EC RV GP SU DK IT FY BL AZ gyd iug och vef 10. V II I 09 20 19 FN TA YJ SO EG PC VD KI XH WZ PYZ ace Pru uyc 9. I IV V 14 10 25 VK DW LH RF JS CX PT YB ZG MU nyh fbd ohs Jrp 8. IV V I 22 04 16 PV XS ZU EQ BW CH AO RL JN TD tck rts nro mkl 17. V I IV 18 11 25 TS IK AV QP HW FM DX NG CY UE mhw lwb mdm ybe 18. IV I II 02 17 20 KZ FI WY MP DS HR CU XE QV NT uw vdk lrh mgd 19. I V IV 26 09 14 VW LT PB PO ZK GS RI QJ HM XE suw tsv nfp yjc 19. I V III V 07 01 12 QS YA XW KR MP HT DU OV CL FZ uby usi mhh mwb	TW GV FB ZL EQ OX	1					lff													23	10	IV	II.	III	14.
11. I V IV 13 15 15 11 NX EC RV GP SU DK IT FY BL AZ gyd iuq och vef 10. V II I 09 20 19 FN TA YJ SO EG PC VD KI KH WZ pyz ace pru uyc 9. I IV V 14 10 25 VK DW LH RF JS CX PT YB ZG MU nyh fbd ohs jrp 8. IV V I 22 04 16 PV XS ZU EQ BW CH AO RL JN TD tck rts nro mkl 7. V I IV 18 11 25 TS IK AV QP HW FM DX NG CY UE mhw lwb mdm ybe 6. IV I III 02 17 20 KZ FI WY MP DS HR CU XE QV NT uwu vdk lrh md 5. I V IV 26 09 14 VW LT PB FO ZK GS RI QJ HM XE suw tsv nfp yjc 4. IV III V 07 01 12 QS YA XW KR MP HT DU OV CL FZ uby usi min mwb	SU DK IT FY BL AZ EG PC VD KI XH WZ DYZ ace pru uyc DYZ ace pru uyc DYZ ace pru wyc DYZ ace pr																				7			V	13.
10.	EG PC VD KI XH WZ Pyz ace pru uyc yc yc yc py by c ace pru uyc yc yc py fbd chs jrp by ch AO RL JN TD tck rts nro mkl hw FM DX NG CY UE mhw lwb mdm ybe DS HR CU XE QV NT uwu ydkk lrh mgd	-																					Y	II	12.
9. I IV V 14 10 25 VK DW LH RF JS CX PT YB ZG MU nyh fbd ohs Jrp 8. IV V I 22 04 16 PV XS ZU EQ BW CH AO RL JN TD tck rts nro mkl 7. V I IV 18 11 25 TS IK AV QP HW FM DX NG CY UE 6. IV I II 02 17 20 KZ FI WY MP DS HR CU XE QV NT uwu vdk lrh mgd 7. I V IV 26 09 14 VW LT PB FO ZK GS RI QJ HM XE suw tsv nfp yjc 8. IV III V 07 01 12 QS YA XW KR MP HT DU OV CL FZ uby usi mhh mwb	JS CX PT YB ZG MU nyh fbd ohs Jrp BW CH AO RL JN TD tck rfs nro mkl HW FM DX NG CY UE mhw lwb mdm ybe DS HR CU XE QV NT uwu ydkk lrh mgd				O cri	STATE OF THE PARTY OF	1000																		11.
8. IV V I 22 04 16 PV XS ZU EQ BW CH AO RL JN TD tck rts nro mkl 7. V I IV 18 11 25 TS IK AV QP HW FM DX NG CY UE mhw lwb mdm ybe 6. IV I III 02 17 20 KZ FI WY MP DS HR CU XE QV NT uwu vdk lrh mgd 5. I V IV 26 09 14 VW LT PB FO ZK GS RI QJ HM XE suw tsv nfp yjc 4. IV III V 07 01 12 QS YA XW KR MP HT DU 0V CL FZ uby us1 min mwb	BW CH AO RL JN TD tck rts nro mkl HW FM DX NG CY UE mhw lwb mdm ybe DS HR CU XE QV NT uwu ydk lrh mgd																								10.
7. V I IV 18 11 25 TS IK AV QP HW FM DX NG CY UE mhw lwb mdm ybe 6. IV I III 02 17 20 KZ FI WY MP DS HR CU XE QV NT uwu ydkk lrh m yde 5. I V IV 26 09 14 WW LT PB FO ZK GS RI QJ HM XE suw tsy hrh m yd 4. IV III V 07 01 12 QS YA XW KR MP HT DU 0V CL FZ uby usi min mwb	HW FM DX NG CY UE mhw lwb mdm ybe DS HR CU XE QV NT uwu ydk lrh mgd																								9.
6. IV I III 02 17 20 KZ FI WY MP DS HR CU XE QV NT uwu vdk lrh mgd 5. I V IV 26 09 14 VW LT PB 170 ZK GS RI QJ HM XE suw tsv nfp yjc 4. IV III V 07 01 12 QS YA XW KR MP HT DU 0V CL FZ uby usi min mwb	DS HR CU XE QV NT uwu vdk lrh mgd																						V		8.
5. I V IV 26 09 14 VW LT PB WO ZK GS RI QJ HM XE suw tsw nfp yjc 4. IV III V 07 01 12 QS YA XW KR MP HT DU OV CL FZ uby usi min mwb								1															I		7.
4. IV III V 07 01 12 QS YA XW KR MP HT DU OV CL FZ uby usi with mwb	ZK GS RI OJ PM XK I SUW tsw nth vici						100 100 100 100																_	IV	6.
TO THE TOTAL PROPERTY OF THE P				W. 1.																				I	5.
																					-	10000		IV	4.
3. I II V 05 16 03 FW DL NX BV KM RZ HY IQ EC JU the von grw axi 2. III I II 12 22 17 DW UO PY GR FS EQ KT CL AI ZB smz lbl bic sym	KM RZ HY IQ EC JU tns von grw axl					644	A OTT								BV	ИX	DL	FW	03	16	05	V	II	I	3.

Figure 3: Enigma Machine Wiring

- Rotor's ring settings (*Ringstellung*): Within each rotor there is an internal ring that maps position to a letter, but it can be switched so that the internal wiring mapping is offset. Example N D V.
- Rotor's initial positions (*Grundstellung*): Within the machine, when locating the rotors, they have to be in a particular initial position. This is achieved by inserting the rotor and turning it to the respective starting point. Example: D Y A.

- Plugboard pairs: This corresponds to the symmetric correspondence of letters in the other plugboard panel. They are typically 10 pairs.
- Reflector selection: As with the rotors, there are 4 different reflectors from which to choose, all with different cross-connections.

Apart from all of these values that changes from user to user, I also have an input configuration file that loads the historically accurate wiring of each reflector and rotor. For the rotors there is an additional parameter called the turnover point. The rotors work as a clock in the way they rotate. The right-most represent the second, the middle the minutes, and the left-most the hours. However they don't turn all in the same letter ('Z' as one would expect), they all each have their own turnover point that triggers its right partner rotation. Those turnovers are obtained from [6]. Finally the message to cipher is also input as a text file.

4.1.3 Processing

As for the processing of the plain text, here is a pseudo code with the simplified process:

for letter in text:

```
# advance rotors according to their own position,
# and turnover points
step_rotors()
\# enter plugboard switch, if no correspondance there
# is no connection, so letter doesn't change
plugboard_letter = plugboard.get(letter, letter)
\# enter rotors (inwards - right to left)
rotor_names_inverted = rotor_names[::-1]
pin_in = ALPHABET.index(plugboard_letter)
for rotor_name in rotor_names_inverted:
        rotor = rotors [rotor_name]
        pin_in = rotor.process_inwards(pin_in)
# enter reflector
pin_out = reflector.reflect(pin_in)
\# enter rotors (outwards - left to right)
for rotor_name in rotor_names:
```

```
rotor = rotors[rotor_name]
pin_out = rotor.process_outwards(pin_out)

# enter plugboard switch
rotor_letter = ALPHABET[pin_out]

# calculate ciphered letter
ciphered_letter = plugboard.get(rotor_letter, rotor_letter)
```

Somethings to be aware of in the processing are that the rotors step before ciphering, not after. Also, the turnover points need to be checked each time the rotors step, some of them even have 2 different turnovers.

4.1.4 Output

The output of the machine is straightforward, it correspond to the cipher letter of each key press after going through the transformations. And for a whole text is just the concatenation of those letters. If this output is to be typed again in the machine with the same initial configuration, the operator on the other side of the line will obtain the original plain message.

4.1.5 Challenges

The biggest challenge in implementing the Enigma machine is knowing exactly how it worked. Even thought there is a great amount of information online, the depth of it is not that significant. Most of the resources tend to shallowly explain the behavior but there are several subtleties and details that were hard to find. I put in the references the most trustworthy and complete information I found on the matter [3, 4, 5, 6, 7, 10].

Another challenge was the translation of this information, because the original machine settings are in German. This implies that there are multiple acceptable translations for several parts of the machine that might be opposite among different sources. A concrete example of this goes within the rotor, where there are 2 different settings called *Ringstellung* and *Grundstellung*. They refer to the ring setting within each the rotor and to the ground setting or offset of the rotor within the machine, respectively. However figuring out which one was which presented a problem because different sources referred to them by different names, sometimes even opposite. So I had to solve this by recurring to the German words.

Finally, I would like to refer as well to different simulators that are found on the internet in which I could get a phenomenological understanding of the machine. I was able to try out different configurations and learning its way to function. I also confirmed

my solution against these simulators in order to test my implementation. This was a positive match.

- Cryptii Simulator: https://cryptii.com/pipes/enigma-machine
- Louise Dade Simulator: http://enigma.louisedade.co.uk/enigma.html

4.2 Bombe Machine

4.2.1 Enigma Exploits

In order to break the enigma, mathematicians Alan Turing and Gordon Welchman, with the collaboration of the staff at Bletchley Park, design the Bombe Machine. It exploited the Enigma Machine's flaws to crack the Nazi's communications. However, the machine itself was not all, it exploited behavioral patterns in the communication as well. Here I list the main weaknesses that lead to deciphering the Enigma:

- The biggest flaw of the Enigma Machine is that because of the internal wiring and design, a letter can never be encrypted to itself. This opened the door to cryptoanalysts to locate possible message deciphers. [11]
- Another breakthrough was when they realized about specific patterns that would repeat themselves in a conversation. For example the daily weather forecast, the heil Hitler salute, or war jargon. These parts of the conversation tipically followed a standard format that allows to create "cribs", an intelligent guess of part of the code. [12]
- In addition to the previous facts, sometimes reckless operators forgot to change the daily settings, which lower the odds of combinations and gave more data to the analysts.

4.2.2 Bombe's algorithm

- with those typical messages we can scan the transmissions and locate where it is within the text (where no letter ciphers to itself)
- with all the possible positions we create a set of hypothesis called a menu, a diagram like fig x. from there, we need to fing a enigma configuration that corresponds to the menu. that was the role of the bombe https://www.youtube.com/watch?v=2dKG21u2aSo

- 4.2.3 Input
- 4.2.4 Processing
- **4.2.5** Output

4.2.6 Challenges

-getting info, very sensitive, most of it classified. Some of it released in 2010, less than 10 years ago -less than 200 bombes, as opposed to enigma machines that were even commercial

. . .

Finally, and as in the previous step, I got some insights from two Bombe simulators online. However as the is very complex, using them is not as straightforward and required a lot of learning. After all, each bomb had several operators. So I just had a glimpse on their configuration files, specially the menu input. Here are the references:

- Ekhall & Hallenberg Simulator: http://www.lysator.liu.se/~koma/turingbombe/[13]
- 101 Computing Simulator: https://www.101computing.net/turing-welchman-bombe/

4.3 Code

The code of both machines is available in the project attached to this report. The structure is as follows:

PICTURE OF CODE STRUCTURE

There is a program called example.py that shows how to use the programs and when executed, outputs the result of both enigma and bombe machines to their respective results files. It also outputs to console like this:

5 Discussion

- historic relevance - not only breaking it, it needed strategy, not letting them know they cracked the code - conclusions, goals achieved

5.1 Future Work

References

- [1] A. Hodges. Alan Turing: The Enigma. Princeton, N.J. Princeton University Press (2012).
- [2] Numberphile. 158,962,555,217,826,360,000 (Enigma Machine). YouTube (2013).

```
mcrg@thegirlwhocan:~/Documents/GitHub/enigma_bombe/enigma_bombe/src$
python example.py

ENIGMA

Clear text:
HIERICIAMMARIAANDTHISISMYPROJECTIPRESENTHERETHEENIGMAMACHINEUSEDINWOR
LDWARTWOASWELLASTHEBOMBEMACHINETHATBREAKSTHECIPHER

Ciphered Text:
SEZALVGDPKKDBSNUMMPQLOAIXTDLANSIXVMAJFAJCXFNKRZURAYCYGTUCNARZDXFLZJWQ
AREVTDJNXNQDXSOQSBUVXQJOPOHUGCMHELDFBSFDJFWTVRSXNJ

BOMBE

Bombe finished and it output the possible plugboards to the file: ..
/data/example_plugboards.txt
```

Figure 4: Example Code Standard Output

- [3] D. Rijmenants. Technical Details of the Enigma Machine. Obtained from: http://users.telenet.be/d.rijmenants/en/enigmatech.htm
- [4] T. Sale. *Military Use of the Enigma*. Obtained from: https://www.codesandciphers.org.uk/enigma/enigma3.htm
- [5] Cryptomuseum. Enigma Cipher Machines. Obtained from: https://www.cryptomuseum.com/crypto/enigma/index.htm
- [6] Wikipedia. Enigma Machine. Obtained from: https://en.wikipedia.org/wiki/ Enigma_machine
- [7] Wikipedia. Cryptanalysis of the Enigma. Obtained from: https://en.wikipedia.org/wiki/Cryptanalysis_of_the_Enigma
- [8] L. Dade. Enigma Machine: How It Works. Obtained from: http://enigma.louisedade.co.uk/howitworks.html
- [9] Wikipedia. Enigma Rotor Details. Obtained from: https://en.wikipedia.org/wiki/Enigma_rotor_details
- [10] G. Ellsbury. The Enigma and The Bombe. Obtained from: http://www.ellsbury.com/enigmabombe.htm
- [11] Numberphile. Flaw in the Enigma Code. YouTube (2013).
- [12] Computerphile. Tackling Enigma (Turing's Enigma Problem). YouTube (2013).
- [13] M. Ekhall, F. Hallenberg. US Navy Cryptanalytic Bombe A Theory of Operation and Computer Simulation. Proceedings of the 1st Conference on Historical Cryptology, pages 103-108, Uppsala, Sweden, 18-20 June, 2018.