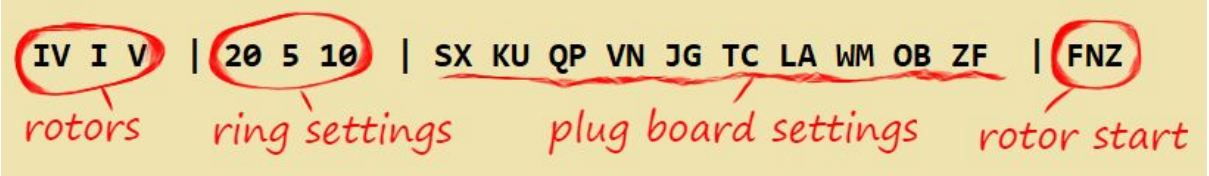
Enigma Messages

Consulting your Enigma settings sheet, you find out that the settings for today are as follows:



Decrypt a message

1. Open Python 3, then open the file called `decrypt.py`
2. Type in the chosen rotors between the green quote marks ‘ ‘ next to `chosen_rotors`
3. Now type in the letters for the rotor start position between the green quote marks ‘ ‘ next to `rotor_start`

```
Here is the secret message: GON XXLXYFQNZIK
```

4. Type in the message key **GON** between the green quote marks ‘ ‘ next to `message_key`
5. Type in the plaintext which is the secret message `XXLXYFQNZIK`
6. Run the program by pressing the F5 key (say yes to saving)

- What is the decrypted message?
- Can you decrypt this message? Use the same Enigma settings but don’t forget to change the message key
  `LJE OIVGWVHOVHKAU`

Encrypt a message

1. Open Python 3, then open the file called `encrypt.py`
2. Type in the chosen rotors and the rotor start position again from the settings sheet
3. Type in the message key **BFR** between the green quote marks ‘ ‘ next to `message_key`
4. Run the program and check it works - the resulting cipher text should be “XXLXYFQNZIK” for the plain text “RASPBERRYPI”.

Now it’s time to encrypt your own message!

- Choose a different three letter `message_key` and type it in
- Choose a different `plaintext` message and type it in. Make sure there are no spaces!
- Run the program, then write down the encrypted key and the cipher text and give it to someone else to decrypt

Challenge

Decrypt this message:

```
GED HYZFQOOVVBBKBWPDZLSL
```

Brute force attack

You need to know the Enigma settings to be able to decrypt the message! Here are today's settings. Unfortunately someone has spilt some ink on the rotor settings :(

Crib text is where you know both the plain text and the cipher text.

Crib text: WEATHER
Cipher text: VZTLMPU

Can you decrypt this message using a brute force attack if you know the crib text and part of the settings?

```
VZTLMPUSLKTEXYWZWKXDOTT
```

Brute force attack

1. Open Python 3, then open the file called `bruteforce.py`
2. Type in the crib text and the corresponding cipher text
3. Run the brute force attack to find the rotors and the message key

Decrypt the message

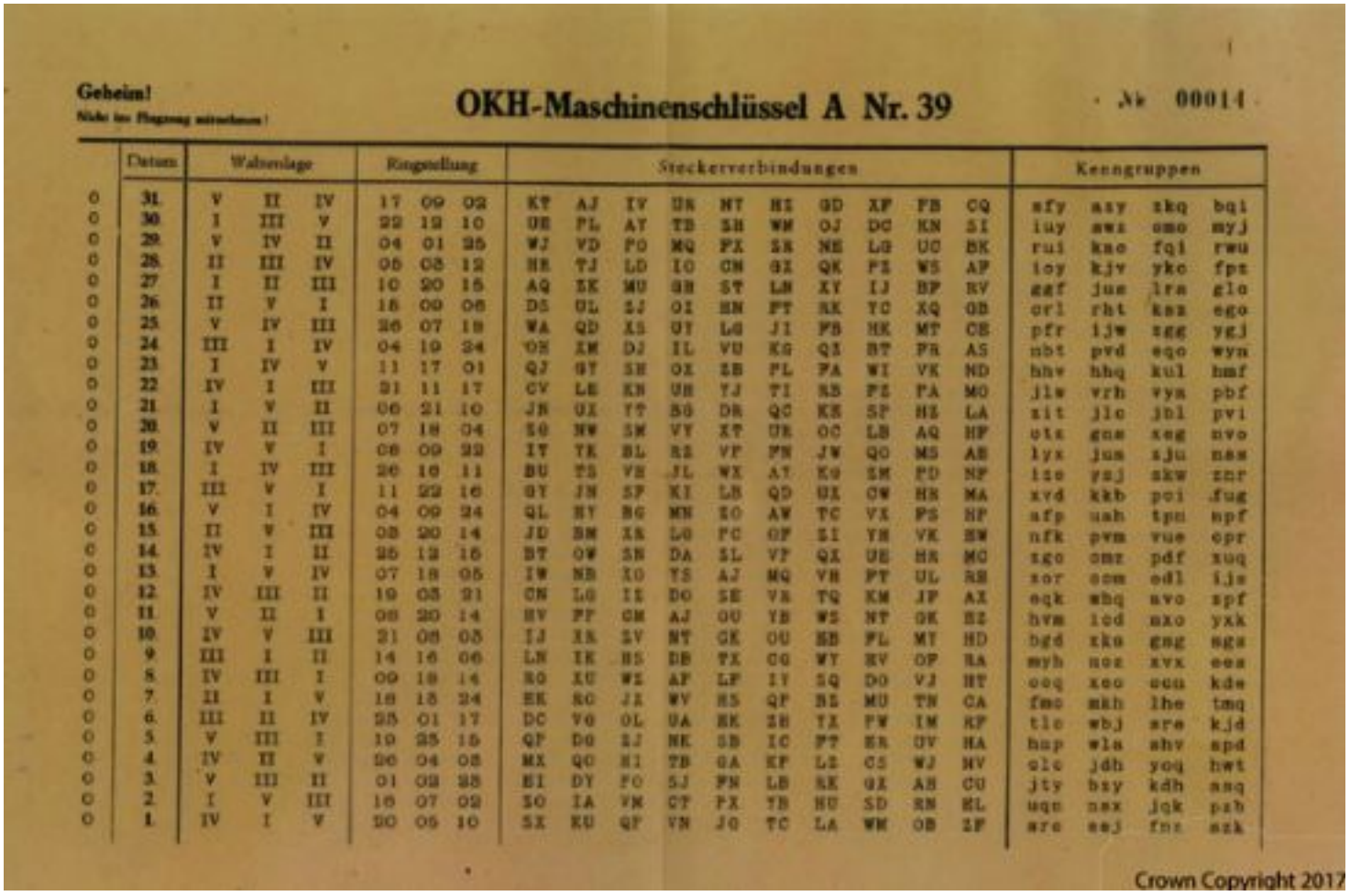
4. Now open the `decrypt.py` program you used before
5. Type in the **rotor start** setting, and this time you will need to type in the **ring** and **plug board** settings from the settings sheet as well
6. Type in the **chosen rotors** you found via the brute force attack
7. This time we already know the decrypted message key. Find this line of code:

```
decrypted_message_key = machine.process_text(message_key)
```

Change it to say `decrypted_message_key = '???'` where ??? is the three letter key you found in the brute force attack.

- What is the secret message?

Final challenge



Geheim!

OKH-Maschinenschlüssel A Nr. 39 · Nr 00014 ·

	Datum	Walzenlage			Ringstellung			Steckerverbindungen										Kenngruppen			
0	31.	V	II	IV	17	09	02	KT	AJ	IV	UN	MT	HI	GD	XF	FB	CQ	sfy	asy	zkq	bqi
0	30.	I	III	V	22	13	10	UE	PL	AT	TB	SH	WM	OJ	DC	KN	SI	iuy	awz	omo	myj
0	29.	V	IV	II	04	01	25	WJ	VD	FO	MQ	PX	SR	NE	LG	UC	BK	rui	kno	fqi	rwu
0	28.	II	III	IV	05	08	12	HE	TJ	LD	IO	CN	GI	QK	PS	WS	AP	ioy	kjv	yko	fpt
0	27.	I	II	III	10	20	15	AQ	ZK	MU	GH	ST	LN	XY	IJ	BP	RV	ggf	jus	lra	glo
0	26.	II	V	I	15	09	06	DS	UL	SJ	OI	HN	FT	RK	TC	XQ	GB	orl	rht	kas	ego
0	25.	V	IV	III	26	07	19	WA	QD	XS	GT	LG	JI	FB	HK	MT	CE	pfr	ijw	zgg	ygj
0	24.	III	I	IV	04	19	24	OE	XM	DJ	IL	VU	KG	QI	BT	PR	AS	nbt	pvd	eqo	wyn
0	23.	I	IV	V	11	17	01	QJ	GT	SH	OI	ZB	PL	PA	WI	VK	ND	hhv	hhq	kul	hmf
0	22.	IV	I	III	21	11	17	CV	LE	KN	UH	YJ	TI	RB	PZ	PA	MO	jlw	vrh	vyn	pbf
0	21.	I	V	II	06	21	10	JR	UI	TT	BG	DR	QC	KS	SP	HZ	LA	xit	jlc	jbl	pvi
0	20.	V	II	III	07	18	04	SO	MW	SM	VY	XT	UR	OC	LB	AQ	HP	uts	gns	xsg	nvo
0	19.	IV	V	I	08	09	22	IT	TK	BL	RZ	VF	PN	JW	QO	MS	AB	lyx	jun	xju	nsx
0	18.	I	IV	III	26	16	11	BU	TS	VE	JL	WX	AY	KG	SM	FD	NP	ise	ysj	skw	zmr
0	17.	III	V	I	11	22	16	GY	JN	SP	KI	LB	QD	UI	OW	HX	MA	xvd	kkb	poi	fug
0	16.	V	I	IV	04	09	24	QL	EY	BG	MN	IO	AW	TC	VX	PS	HP	afp	uah	tpn	npf
0	15.	II	V	III	03	20	14	JD	BM	XR	LG	FC	OP	SI	YE	VK	EW	nfk	pvm	vue	opr
0	14.	IV	I	II	25	13	15	BT	OW	SN	DA	SL	VP	QX	UE	HR	MC	xgo	omr	pdf	xuq
0	13.	I	V	IV	07	18	05	IW	NB	IO	YS	AJ	MQ	YH	PT	UL	RS	xor	ocm	odl	ijs
0	12.	IV	III	II	19	03	21	CN	LG	IZ	DO	SE	VR	TQ	KM	JP	AX	eqk	wbq	nvo	spf
0	11.	V	II	I	08	20	14	HV	PF	GM	AJ	OU	YB	WS	NT	GK	SZ	hvm	lcd	nxo	yxk
0	10.	IV	V	III	21	08	03	IJ	XR	LV	NT	GK	OU	EB	FL	MT	HD	bgd	zko	gng	sgs
0	9.	III	I	II	14	16	06	LN	IK	BS	DE	TX	CG	WT	EV	OP	RA	myh	noz	xvx	eos
0	8.	IV	III	I	09	18	14	SO	XU	WZ	AF	LP	IY	SQ	DO	VJ	HT	ooq	xeo	ocu	kde
0	7.	II	I	V	18	15	24	EK	SC	JZ	WV	RS	QP	BZ	MU	TN	CA	fmc	mkh	lhe	tmq
0	6.	III	II	IV	25	01	17	DC	VO	OL	UA	EK	ZH	TZ	FW	IM	KP	tlc	wbj	sre	kjd
0	5.	V	III	I	19	25	15	QP	DG	ZJ	NK	SB	IC	PT	ER	UV	HA	hup	wla	shv	spd
0	4.	IV	II	V	20	04	08	MX	QC	RI	TB	GA	KP	LZ	CS	WJ	NV	olc	jdh	yoq	hwt
0	3.	V	III	II	01	03	25	EI	DY	FO	SJ	PN	LB	EK	GZ	AH	CU	jty	bzy	kdh	asq
0	2.	I	V	III	16	07	02	IO	IA	VM	QT	PX	TB	HU	SD	RN	EL	uqn	nsx	jqk	pzb
0	1.	IV	I	V	20	05	10	SZ	KU	QP	VN	JG	TC	LA	WM	OB	ZF	sre	sej	fnr	szk

RASPBERRY JAM Cotswold

DHPCMHCQ PXE

18/05/18

ZOC EJDTLFHR BT UKW.