Exercises: Enigma

1. The German Navy Enigma was exactly the same as the army's machine except they had three extra rotors. How many ways are there to pick 3 rotors from a choice of 8?

$$8 \times 7 \times 6 = 336$$

2. In 1942 the German U-Boats added a fourth rotor to the machine, which was not a choice and was not interchangable with the other navy rotors. How many ciphers did the U-Boat Enigma Machine have?

$$\frac{336 \times 26! \times 26^4}{2^{10}10!6!} \approx 2.3 \times 10^{22}$$

3. Here is a complete table of the ciphers performed by each rotor, reflector, and variants.

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
Rotor V	V	Z	B	R	G	I	T	Y	U	P	S	D	N	H	L	X	A	W	M	J	Q	O	F	E	C	K
Navy Rotor VI	J	P	G	V	O	U	M	F	Y	Q	B	E	N	H	Z	R	D	K	A	S	X	L	I	C	T	W
Navy Rotor VII	N	Z	J	H	G	R	C	X	M	Y	S	W	B	O	U	F	A	I	V	L	P	E	K	Q	D	T
Navy Rotor VIII	F	K	Q	H	T	L	X	O	C	B	J	S	P	D	Z	R	A	M	E	W	N	I	U	Y	G	V
U-Boat Beta rotor	L	E	Y	J	V	C	N	I	X	W	P	B	Q	M	D	R	T	A	K	Z	G	F	U	H	O	S
U-Boat Gamma rotor	F	S	O	K	A	N	U	E	R	H	M	B	T	I	Y	C	W	L	Q	P	Z	X	V	G	J	D
reflector B	Y	R	U	H	Q	S	L	D	P	X	N	G	O	K	M	I	E	B	F	Z	C	W	V	J	A	T
reflector C	F	V	P	J	I	A	O	Y	E	D	R	Z	X	W	G	C	T	K	U	Q	S	B	N	M	H	L

These ciphers are when the ring setting is A, and when the rotor is also at position A.

Kickover points for rotors I-V these are at position R, F, W, K, and A, respectively. For rotors VI-VII these are at A and at N.

(a) We are given the following Enigma settings:

Rotors: III, II, I (placed in the machine from left to right);
Ring Setting: AAA; Rotor Position: AAA; Reflector B;
Plugboard:
(AU)(BE)(CJ)(DO)(FT)(GP)(HZ)(IW)(KN)(LS)(M)(Q)(R)(V)(X)(Y).

What does an input of G become?

$G \mapsto P \mapsto H \mapsto U \mapsto K \mapsto N \mapsto N \mapsto T \mapsto L \mapsto S$