
ENIGMA

But first: Cryptography

Imagine there is a war, and a battle is going on.

Sending a message

The army needs to send a message to another part of the army across a long distance .

FRIENDSHIP ARMY A ⟶ FRIENDSHIP ARMY B

Message Intercepted

On the way, the enemy is able to intercept the message.

Plaintext Message

If the message is written as it is, then the enemy can just read it and understand what it is saying. Then use the information to defeat the army.

Encrypted Message

But if the message is encrypted, then the enemy cannot easily read it.

For example: WE NEED REINFORCEMENT is encrypted into KLRSRNFADCBMKCGATDOZU

All together

Message on its way

Message Intercepted

Unencrypted message (plaintext)

Can be read and understood

Encrypted message

No idea what the message means

Examples of Encryption

- 400-487 BC: Scytale

  Allegedly used by the Spartans

- 50-60 BC: Caesar shift

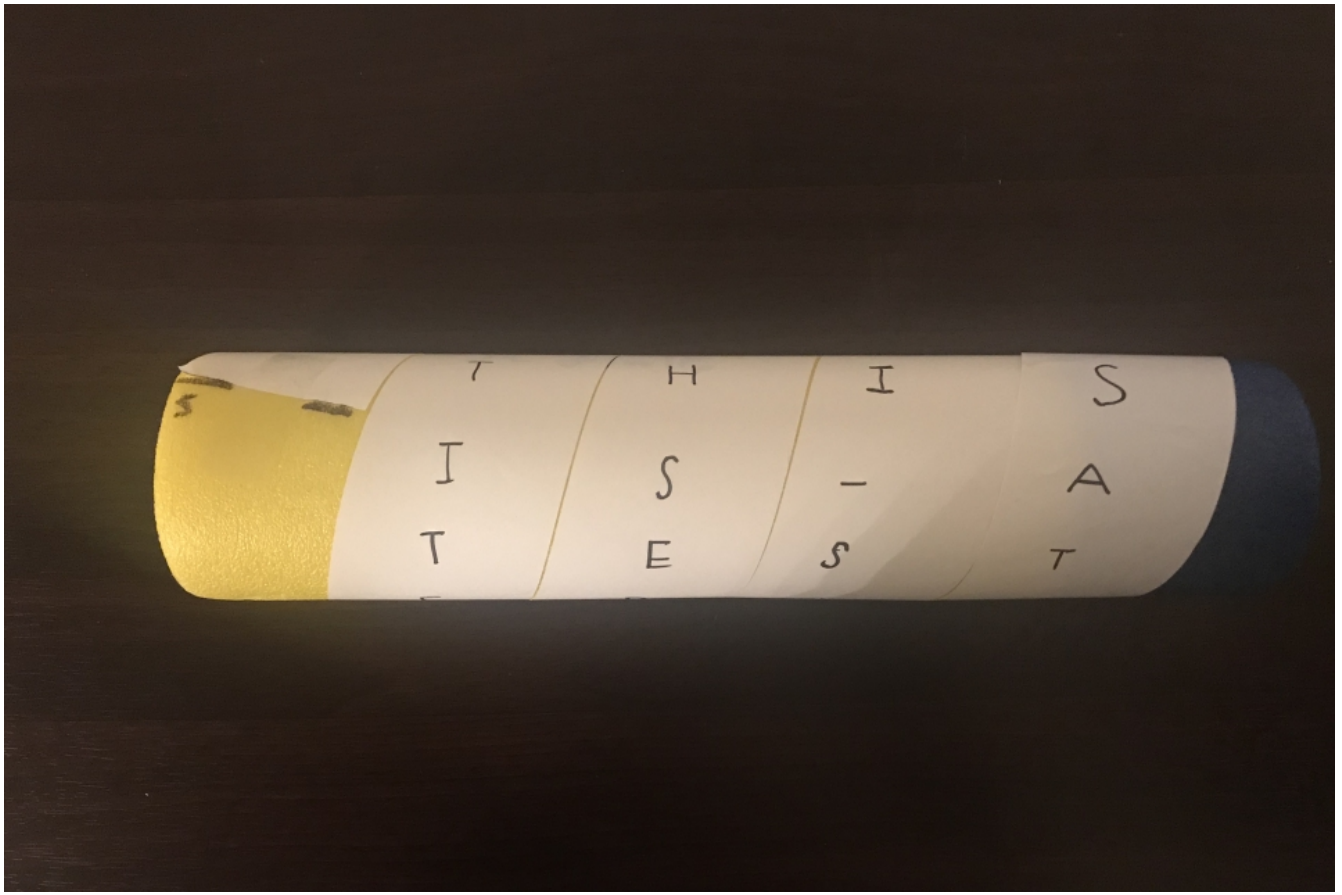
  AKA: Caesar cipher, Caesar's cipher, the shift cipher, Caesar's code

- Simple substitution cipher

  500-600 BC: Atbash, reverse alphabet substitution

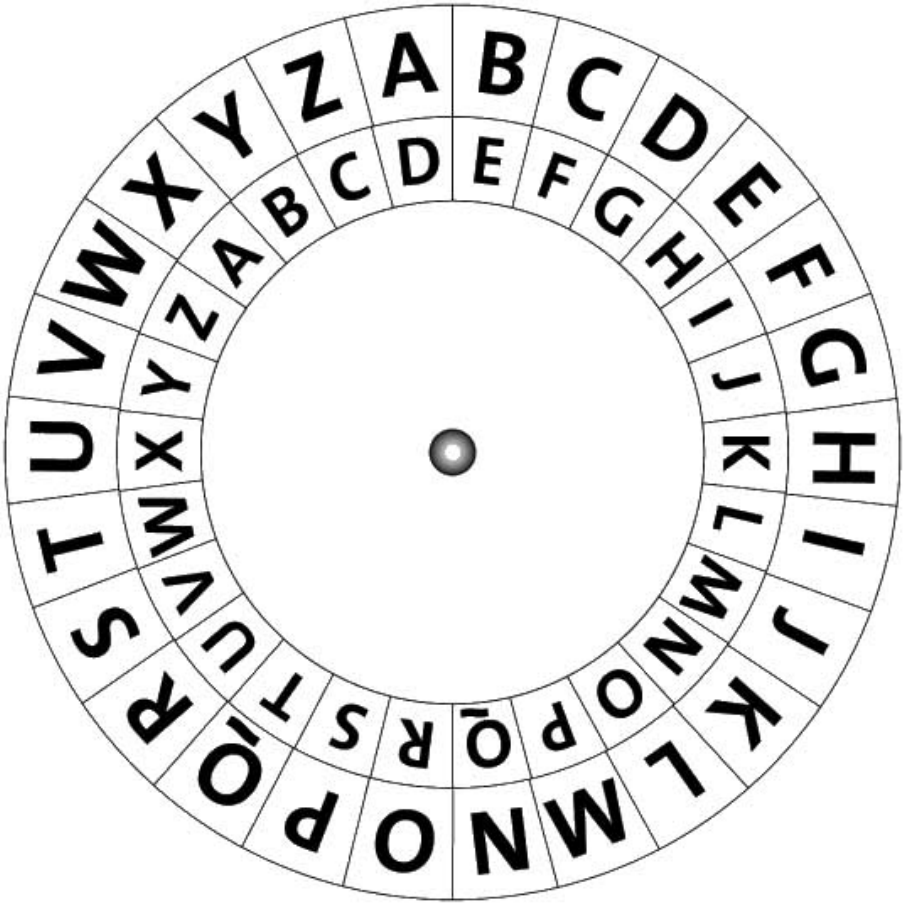
Scytale

- Get a stick or some kind of cylinder
- Wrap a long strip of blank paper or fabric around it.
- Write message across
- Unwrap



Caesar Shift

- A Caesar Shift of 3 makes A become D, so that the alphabet becomes like this:



Simple Substitution Cipher

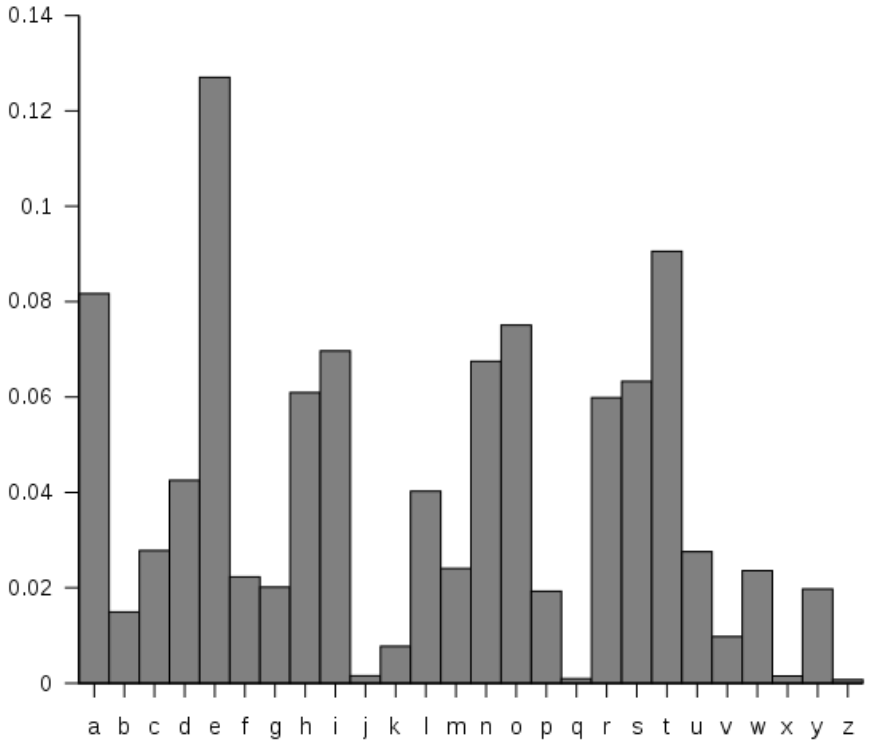
- Caesar Shift is a type of substitution cipher, but ciphertext is ordered from A to Z.
- But a simple substitution cipher can make one letter of alphabet into another different alphabet of your choice (or numbers or symbols).
- Example of a Simple Substitution Cipher:

  plain alphabet : abcdefghijklmnopqrstuvwxyz

  cipher alphabet: phqgiumeaylnofdxjkrcvstzwb

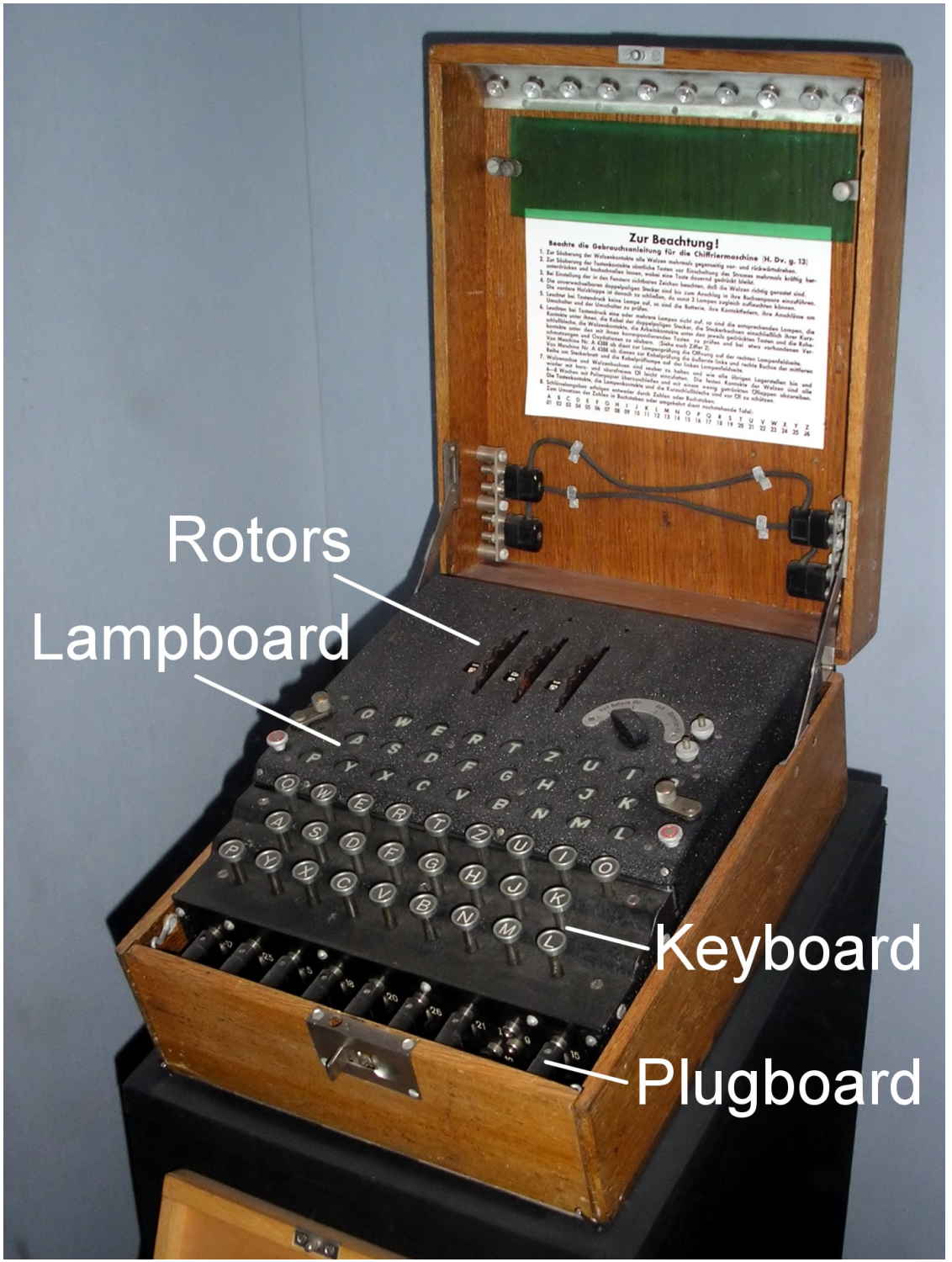
Cracking substitution cipher

- AD 800: Frequency Analysis
- This way of cracking substitution cipher (remap letters) is surprisingly ancient.
- What you do is for each letter, count how many there are. Then can slowly decipher the scrambled text.
- For English should be similar to this: (can also find a graph for punctuations too)



Enigma

- The concept of rotor encryption started from around 1915.
- Enigma was invented in 1918, right at end of WW1.
- Improvements were made.
- The modified version for German military use is ready in 1932.


Rotors
Lampboard
Keyboard
Plugboard

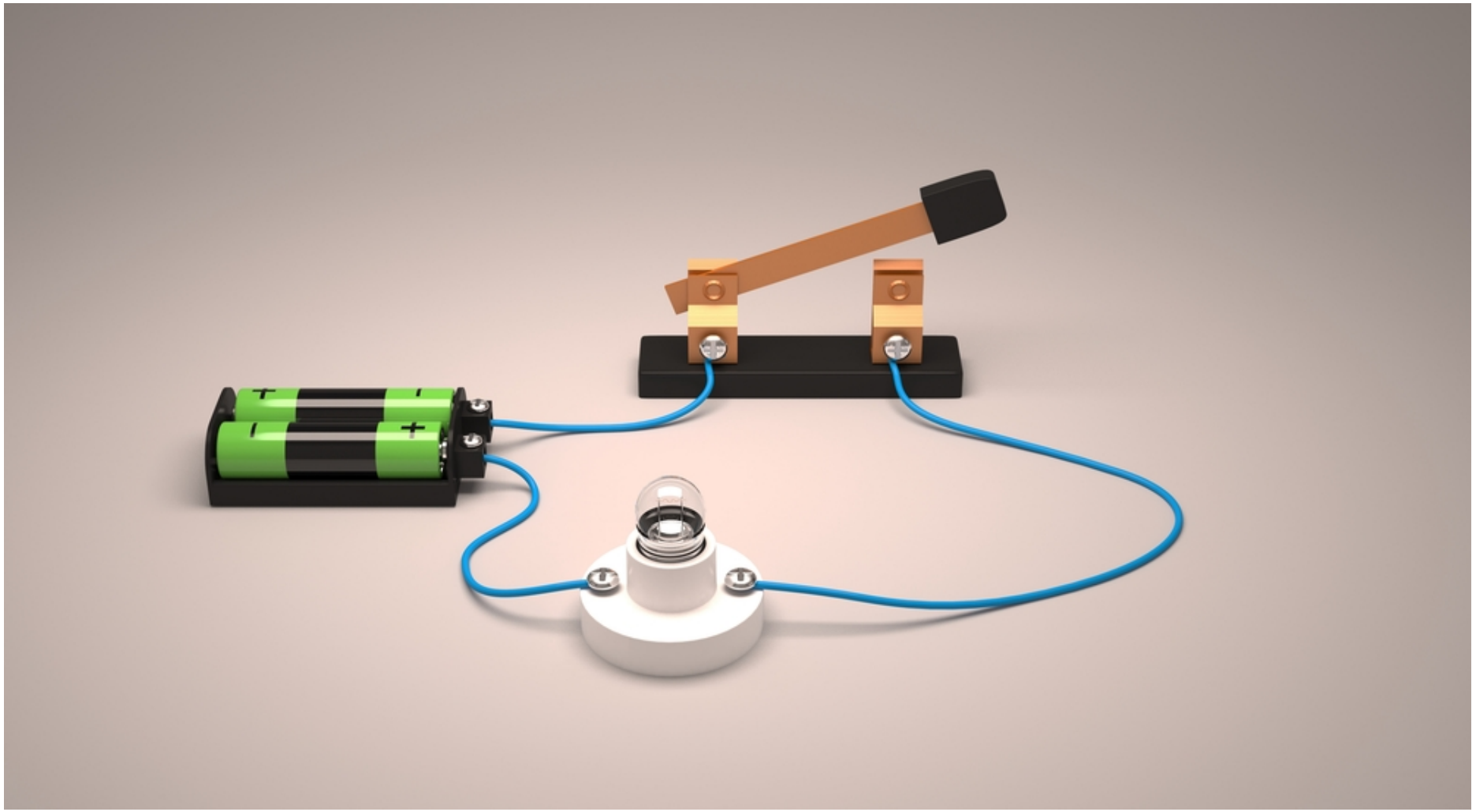
Spot The Difference

Commercial Enigma

Military Enigma

How Does Enigma Work?

- At the very basic level, it is just this:

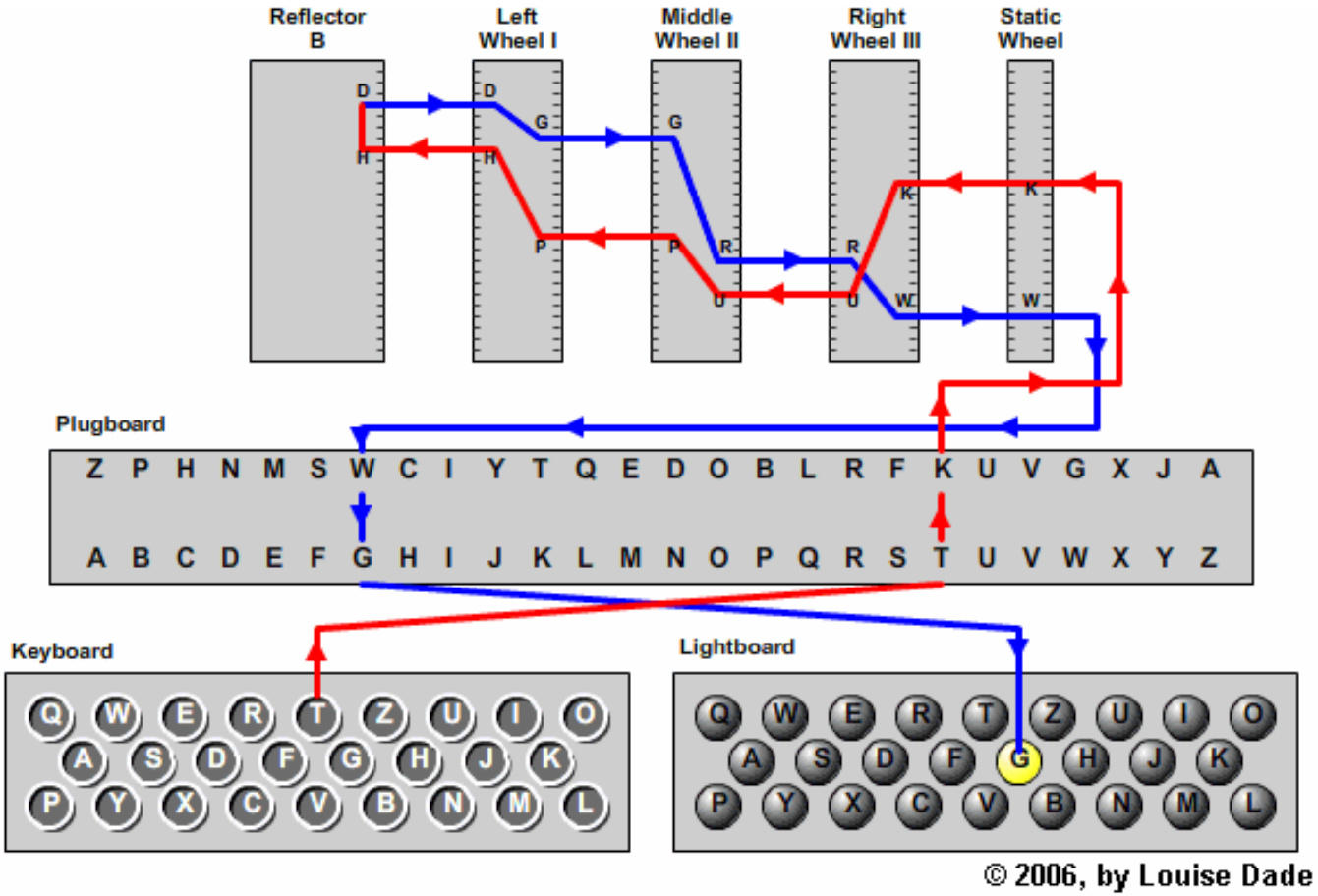


But wait, there's more

- There are 26 keys from A to Z.
- There are 26 light bulbs from A to Z.
- So there are 26 wires, sort of.
- Each key is a switch. When pressed, a key will complete the circuit and turn on a light bulb.
- But also, when a key is pressed, the rotor drum will be rotated. So it is both electrical and mechanical machine.

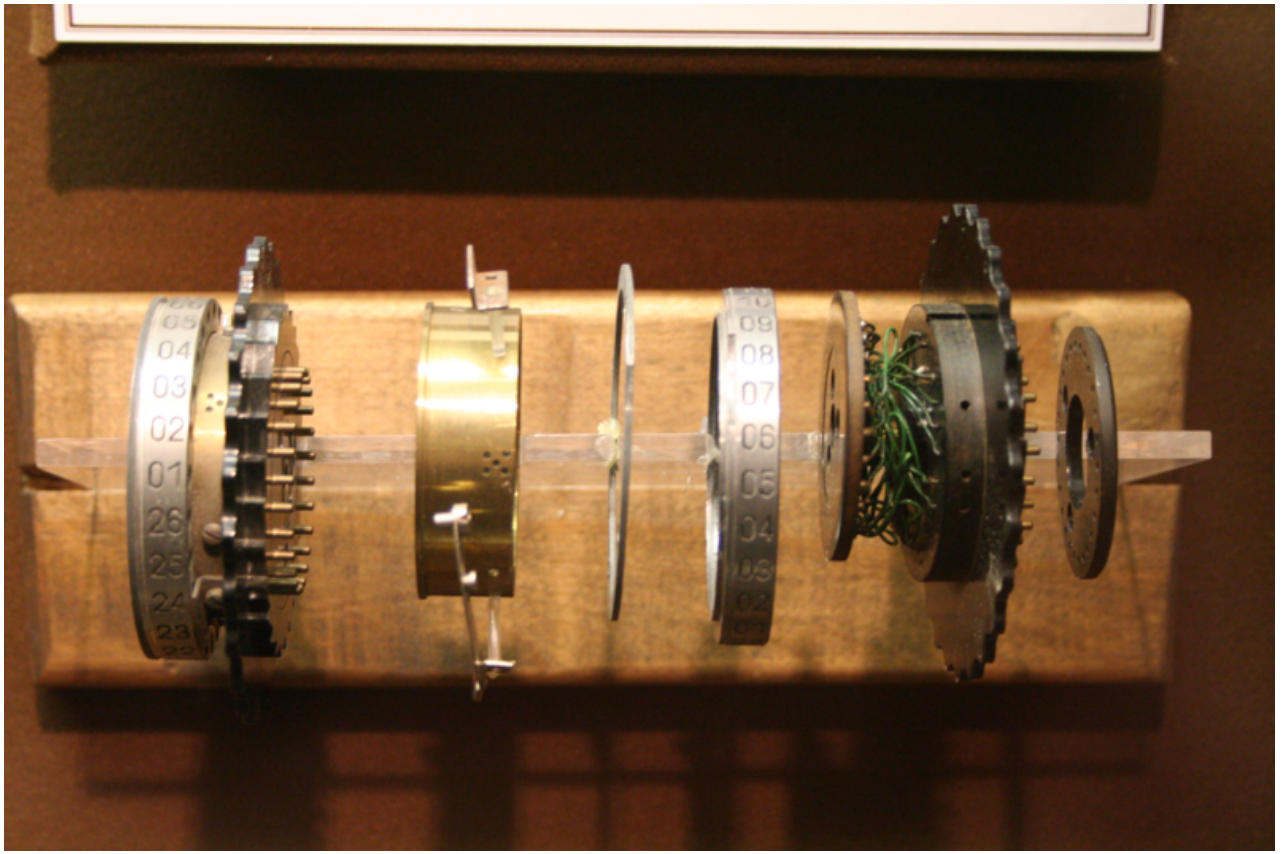
1 Key Press, 1 of 26 “wires”

- Important parts: Keyboard, Plugboard, Rotors, Reflector, Lightboard

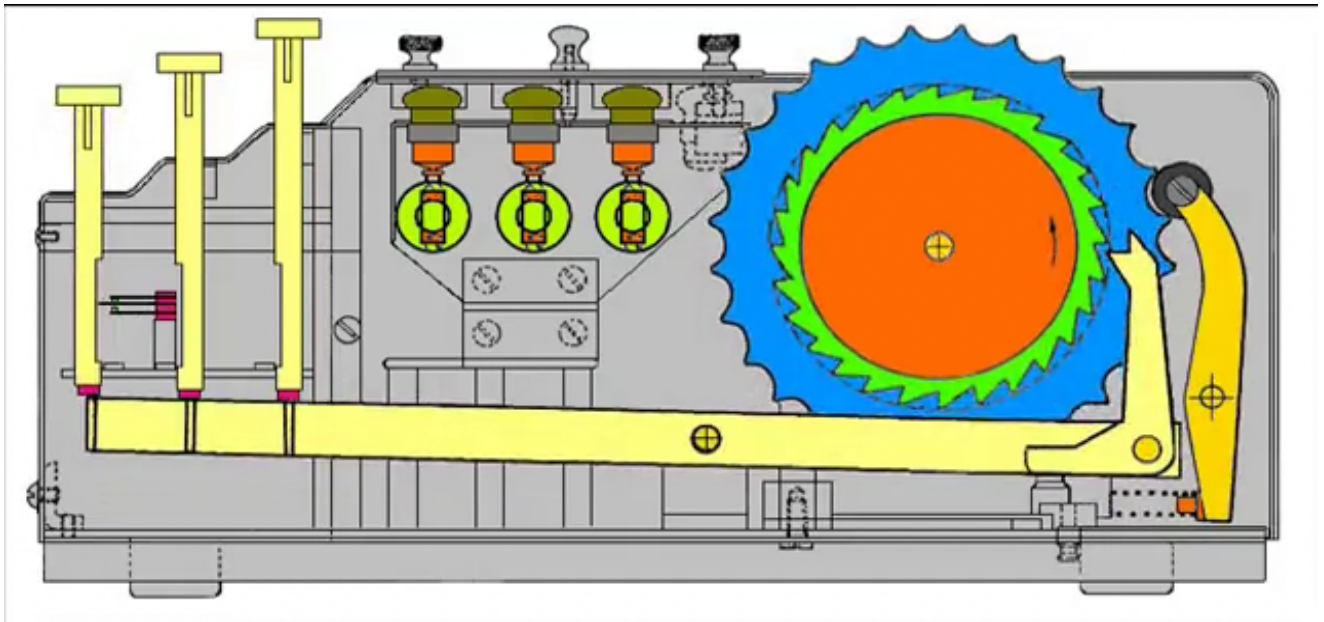


Rotor Encryption

- A rotor is a simple substitution cipher.
- The rotor rewires the alphabet, so scrambles the letters.
- BUT it also rotates by 1 letter each time a key is pressed. This makes frequency analysis useless.

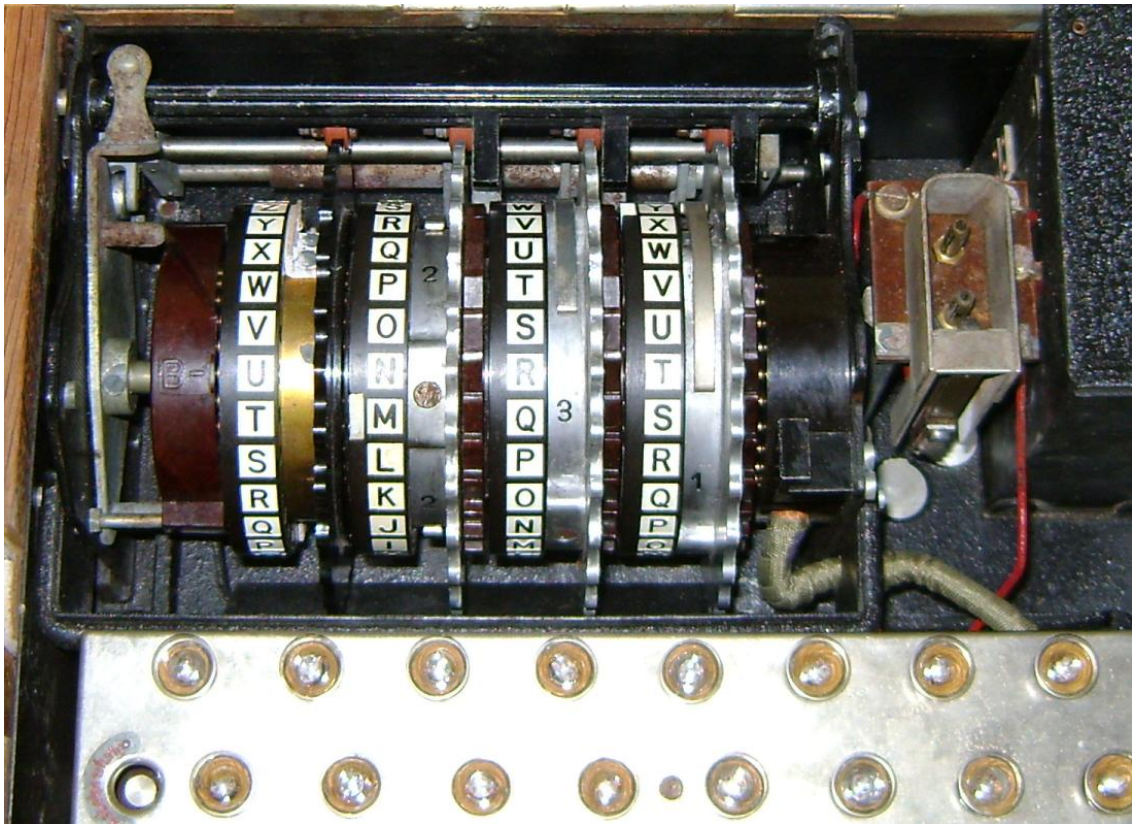


Side View



Rotor Drum

- The German military and air force enigma has 3 rotors.
- Navy has 4 rotors.
- A reflector is on left side of machine to redirect the electricity back into the rotors to go through more scrambling.



Plugboard

- So, the military enigma has those plugs on the plugboard.
- It's a cable that when plugged, swaps 2 letters.
- It swaps the letters straight after a key press.
- It also swaps the letter after scrambling the letters.

Bombe

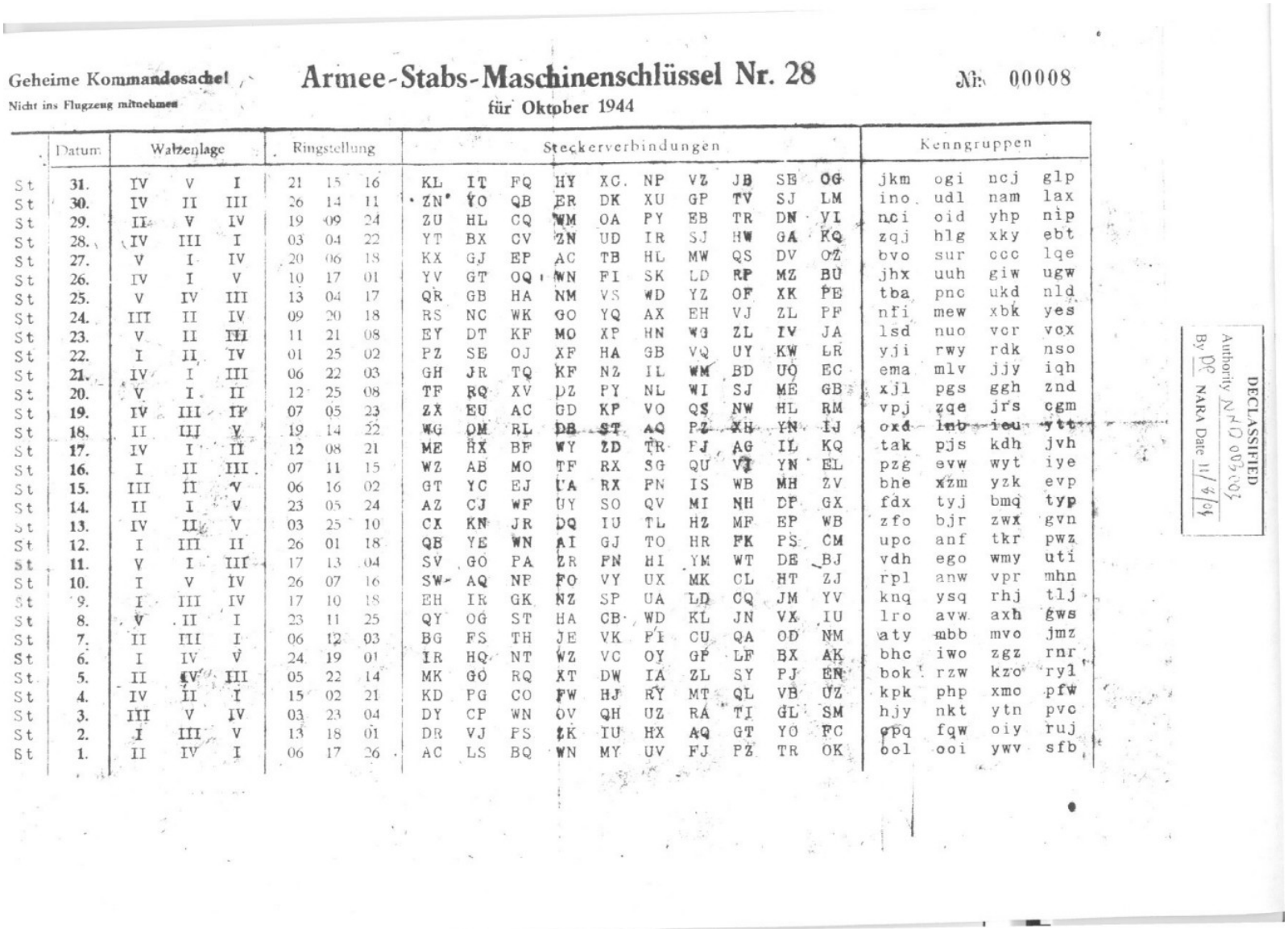
- There are this many possible ways to set up Enigma: 158,962,555,217,826,360,000
- The Nazis thought this is impossible to break.
- Guess what? They were wrong. The British cracked it with Bombe:

Alan Turing

- Bletchley Park was an secret organisation responsible for cracking German codes.
- Alan Turing was a very smart statistician hired by Bletchley Park to decipher the codes.
- The Bombe machine was designed by Alan Turing and improved by Gordon Welchman.
- Turing is widely considered to be the father of theoretical computer science and artificial intelligence. Without him, we're likely not to even have the internet today.

Now you try and operate Enigma

The Germans have this setting sheet issued every month. Each day they tear off part of the sheet, use the setting, then burn the torn piece away.



Geheime Kommandosache
Nicht ins Flugzeug mitnehmen

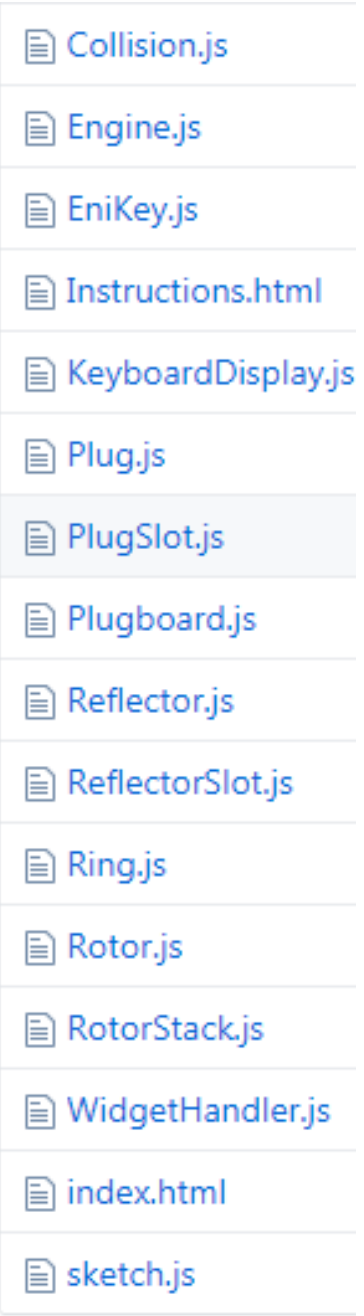
Armee-Stabs-Maschinenschlüssel Nr. 28
für Oktober 1944

Nr. 00008

	Datum	Walzenlage			Ringstellung			Steckerverbindungen										Kenngruppen			
St	31.	IV	V	I	21	15	16	KL	IT	FQ	HY	XC	NP	VZ	JB	SE	OG	jkm	ogi	ncj	glp
St	30.	IV	II	III	26	14	11	ZN	YO	QB	ER	DK	XU	GP	TV	SJ	LM	ino	udl	nam	lax
St	29.	II	V	IV	19	09	24	ZU	HL	CQ	WM	OA	PY	EB	TR	DN	VI	nci	oid	yhp	nip
St	28.	IV	III	I	03	04	22	YT	BX	CV	ZN	UD	IR	SJ	HW	GA	KQ	zqj	hlg	xky	ebt
St	27.	V	I	IV	20	06	18	KX	GJ	EP	AC	TB	HL	MW	QS	DV	OZ	bvo	sur	ccc	lqe
St	26.	IV	I	V	10	17	01	YV	GT	OQ	WN	FI	SK	LD	RP	MZ	BU	jhx	uuh	giw	ugw
St	25.	V	IV	III	13	04	17	QR	GB	HA	NM	VS	WD	YZ	OF	XK	PE	tba	pnc	ukd	nld
St	24.	III	II	IV	09	20	18	RS	NC	WK	GO	YQ	AX	EH	VJ	ZL	PF	nfi	mew	xbk	yes
St	23.	V	II	III	11	21	08	EY	DT	KF	MO	XP	HN	WG	ZL	IV	JA	lsd	nuo	vcr	vcx
St	22.	I	II	IV	01	25	02	PZ	SE	OJ	XF	HA	GB	VQ	UY	KW	LR	yji	rwy	rdk	nso
St	21.	IV	I	III	06	22	03	GH	JR	TQ	KF	NZ	IL	WM	BD	UO	EC	ema	mlv	jjy	iqh
St	20.	V	I	II	12	25	08	TF	RQ	XV	DZ	PY	NL	WI	SJ	ME	GB	xjl	pgs	ggh	znd
St	19.	IV	III	II	07	05	23	ZX	EU	AC	GD	KP	VO	QS	NW	HL	RM	vpj	zqe	jrs	cgm
St	18.	II	III	V	19	14	22	WG	OM	RL	DB	ST	AQ	PZ	XH	YN	IJ	oxd	lnb	ieu	ytt
St	17.	IV	I	II	12	08	21	ME	HX	BF	WY	ZD	TR	FJ	AG	IL	KQ	tak	pjs	kdh	jvh
St	16.	I	II	III	07	11	15	WZ	AB	MO	TF	RX	SG	QU	VI	YN	EL	pzg	evw	wyt	iye
St	15.	III	II	V	06	16	02	GT	YC	EJ	UA	RX	PN	IS	WB	MH	ZV	bhe	xzm	yzk	evp
St	14.	II	I	V	23	05	24	AZ	CJ	WF	UY	SO	QV	MI	NH	DP	GX	fdx	tyj	bmq	typ
St	13.	IV	II	V	03	25	10	CX	KN	JR	DQ	IU	TL	HZ	MF	EP	WB	zfo	bjr	zwx	gvn
St	12.	I	III	II	26	01	18	QB	YE	WN	AI	GJ	TO	HR	FK	PS	CM	upc	anf	tkr	pwz
St	11.	V	I	III	17	13	04	SV	GO	PA	ZR	FN	HI	YM	WT	DE	BJ	vdh	ego	wmy	uti
St	10.	I	V	IV	26	07	16	SW	AQ	NP	FO	VY	UX	MK	CL	HT	ZJ	rpl	anw	vpr	mhn
St	9.	I	III	IV	17	10	18	EH	IR	GK	NZ	SP	UA	LD	CQ	JM	YV	knq	ysq	rhj	tlj
St	8.	V	II	I	23	11	25	QY	OG	ST	HA	CB	WD	KL	JN	VX	IU	lro	avw	axh	gws
St	7.	II	III	I	06	12	03	BG	FS	TH	JE	VK	PI	CU	QA	OD	NM	aty	mbb	mvo	jmz
St	6.	I	IV	V	24	19	01	IR	HQ	NT	WZ	VC	OY	GP	LF	BX	AK	bhc	iwo	zgz	rnr
St	5.	II	IV	III	05	22	14	MK	GO	RQ	XT	DW	IA	ZL	SY	PJ	EN	bok	rzw	kzo	ryl
St	4.	IV	II	I	15	02	21	KD	PG	CO	FW	HJ	RY	MT	QL	VB	UZ	kpk	php	xmo	pfw
St	3.	III	V	IV	03	23	04	DY	CP	WN	OV	QH	UZ	RA	TI	GL	SM	hjy	nkt	ytn	pvc
St	2.	I	III	V	13	18	01	DR	VJ	FS	IK	IU	HX	AQ	GT	YO	FC	cpq	fqw	oiy	ruj
St	1.	II	IV	I	06	17	26	AC	LS	BQ	WN	MY	UV	FJ	PZ	TR	OK	ool	ooi	ywv	sfb

My Enigma on GitHub

- Many javascript files
- Does some file names sound like what we've discussed?
- Notice the Rotor.js, that's 1 file, but how many rotors are there in actual Enigma machine?
- Try it out (instructions included): https://nciccs.github.io/Ultra2/



Resources

- https://www.cryptomuseum.com/crypto/enigma/hist.htm
- https://en.wikipedia.org/wiki/History_of_cryptography
- https://www.revolvy.com/page/Timeline-of-cryptography
- http://pi.math.cornell.edu/~morris/135/timeline.html
- https://diy.org/wellfleet/1408552
- https://tex.stackexchange.com/questions/103364/how-to-create-a-caesars-encryption-disk-using-latex
- https://en.wikipedia.org/wiki/Frequency_analysis
- https://en.wikipedia.org/wiki/Enigma_rotor_details
- https://www.autodesk.com/products/eagle/blog/series-vs-parallel-circuits/
- http://enigma.louisedade.co.uk/howitworks.html
- https://en.wikipedia.org/wiki/File:EnigmaMachineLabeled.jpg
- http://users.telenet.be/d.rijmenants/pics/hires-m4inside.jpg
-