Enigma machine and cryptography

by Chris Davis

Greeks

rearranging words
Hello world -> ehlol owrdl

Caesar Cipher

Hello Charlie
qmttw Kpiztqm

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
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
i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h

Advanced substitution Cipher

Mix letters
Hello Charlie
85ccf 381ic95
Conng Hcisnqo

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
1	2	3	4	5	6	7	8	9	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q
i	p	h	b	o	s	f	c	q	z	j	n	t	w	g	l	m	y	r	x	d	k	e	u	v	a

Vigenere Cipher

tbshsmathsphysicssociety- 24
key: robin
robinrobinrobinrobinrobi

Vigenere Cipher

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

Vigenere Cipher

tbshsmathsphysicssociety- 24
key robin
robinrobinrobinrobinrobi
kptpfdoupfgvzavtgtwpzsug

Long Cipher

Crowd of generally working classes were gathered from around greater manchester to protest for parliamentary representation. The Local Magistrates panicked and read riot act to crowd, but little of the crows could hear them.

600 Hussars (light infantry), several hundred infantrymen, 400 men of Cheshire cavalry, an artillery unit with 2 6 pounder guns, some local Yeomanry and 400 special constables. These forces were given the task of arresting the protesters, but some of the Yeomanry had grudges with Protesters and many were drunk. So they charged, and slashed at protesters and banners. The soldiers though this was the crowd attacking the Yeomanry and charged. Many attacked but a few resisted and tried to take the swords of the yeomanry crying ‘for shame gentlemen’.

11–15 killed and 400–700 injured. Members of the protesters put on trial, Hussars and Magistrates cleared of any wrong, received congratulations from Prince regent

Long Cipher

crowdofgenerallyworkingclasseweregatheredfromaroundgreatermanchestert
oprotestforparliamentaryrepresentationthlocalmagistratespanickedandreadrio
tacttocrowdbutlittleofthecrowscouldhearthemsixhundredhussarslightinfantrys
everalhundredinfantrymenfourhundredmenofcheshirecavalryanartilleryunitwi
thtwosixpoundergunssomelocalyeomanryandfourhundredspecialconstablesthes
eforceweregiventhetaskofarrestingtheprotestersbutsomeoftheyeomanryhadg
rudgeswithprotestersandmanyweredrunksotheychargedandslashedatprotesters
andbannersthesoldiersthoughtthiswasthecrowdattackingtheyeomanryandcharg
edmanyattackedbutafewresistedandtriedtotaketheswordsoftheyeomanrycryin
gforshamegentlemeneleventofifteenkilledandfourhundredtosevenhundredinju
redmembersoftheprotestersputontrialhussarsandmagistratesclearedofanywron
greceivedcongratulationsfromprinceregent

Key: mrhows

Long Cipher

oivkzgrxlbajmcsmsgdbpbcuxrzgakivyscsfylfavrivawjalurcjqrasnemejvakfvyhkh
dfasolrfydwjxzhaaffrymnwbilgaffrawkffyscysxdhuekfihhakbruwycquhbzjqrkfeg
frjhpgoivkztgkswplxvvtpzqtycskofbzzzqryhdwyjpldmzuyszzgjzonkxznvpazwhbp
jkjljajmcoijvdvkwjxmeafueqemcqjtlurnwpdlbkxoylgdadvjorsxifojsdkpzhwdpb
belizavpoajpllggeksnygezgkeqcvqwdkvvawfdphbzxalyvqfpilrohqtpohuaezhwtx
vzhdwevmcnuqjdsnwszcsjltvaoocawhfnwekpbcltvwfklqjasnknlagkeqfmhdwkvv
awfdpoozydlkuakizavljaklgpwdjhbzemefkajquyijcefavaqoyhfcwprurodmjoszsf
gycpweklfoszuiojfqizhdwefsrewdjavkmsyahdaenhgpzqtycsvmkaoycuenhdwkvv
awfdphbzutryuavyrumwlfrjyavnlaobwiilgekfvkojvfipszlakhyaltvzkkjpjvtpzqplci
szifqnquentkjeyhaayqeazaeqelzanqeacbarklsjcucsszszumcqjtlurnwpkvganqeoi
jvdvkwjbgilriwyslfogrkosljaklgpwdjwipgzkywwdtlzgwjerurisszzhnsfvzqhwmilrk
xmefkngzxysywumlrygzxyopmxrawkfewycihdzuqajqxlbp

The Perfect Vigenere Cipher

Remove space
Minimal words
Random words and letters
Use Shorthand
Never give away key

Advancing the Cipher

I apply Cipher
Send
They put on a Cipher
They send it back
I remove my Cipher
Send it to them
They remove their Cipher
Decoded message

Enigma machine

Arthur Scherbius
companies transferring ‘trade secrets’
Chiffriermaschinen Aktiengesellschaft
Soon used by German navy, army and air force by 1933

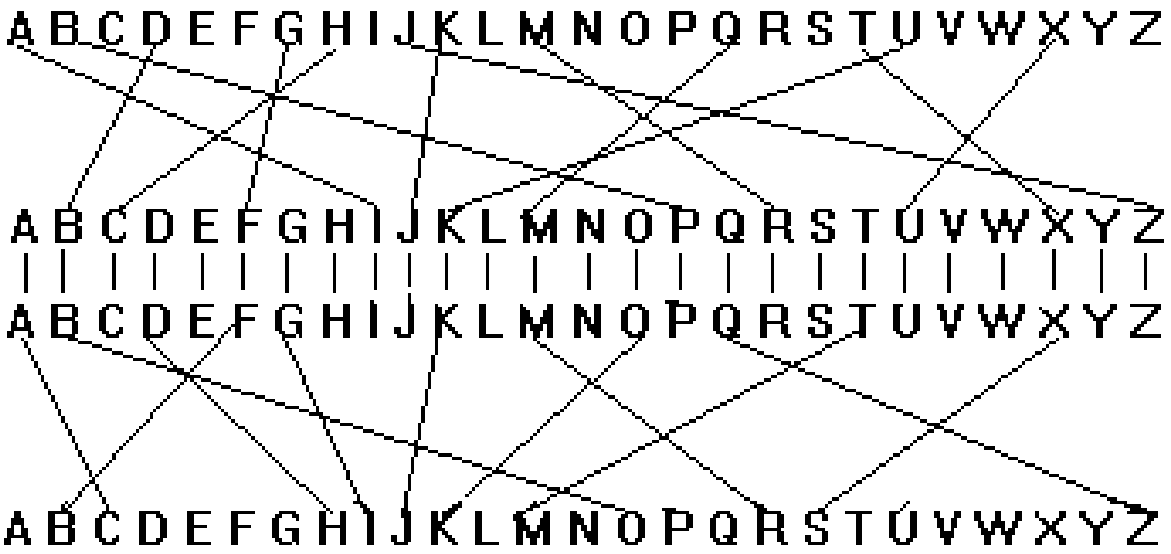
How it works

How it works

Electrical connections

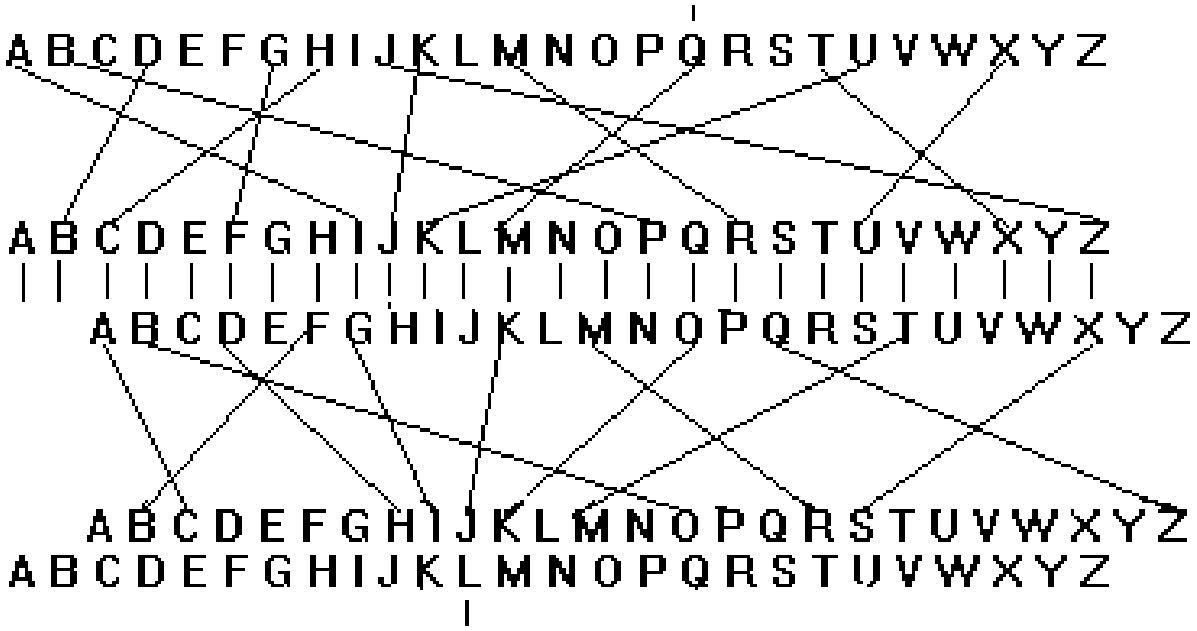
Voltage when trigger at top moves to the bottom

403,291,461,126,605,635,584,000,000 in one

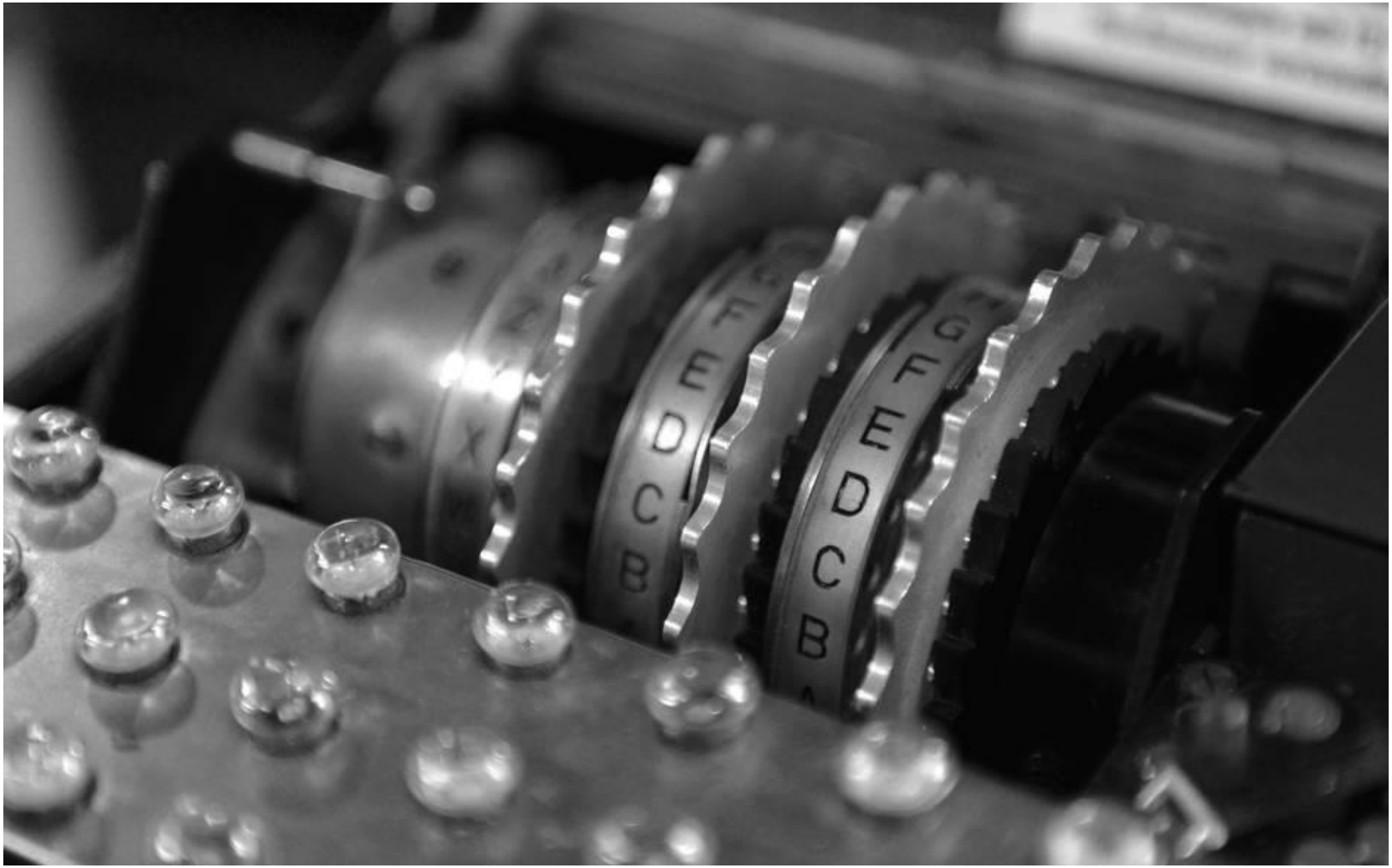


How it works

Caesar shift
Completely new set of conections

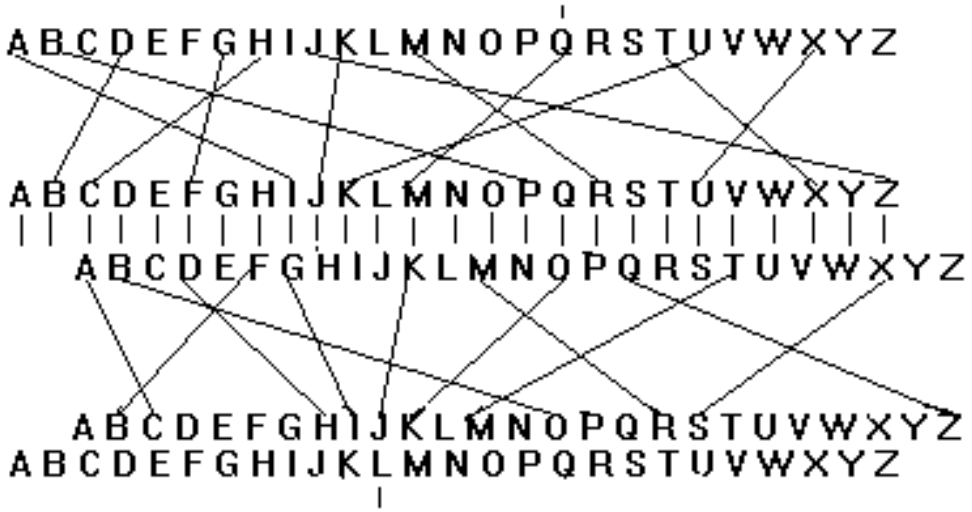


How it works



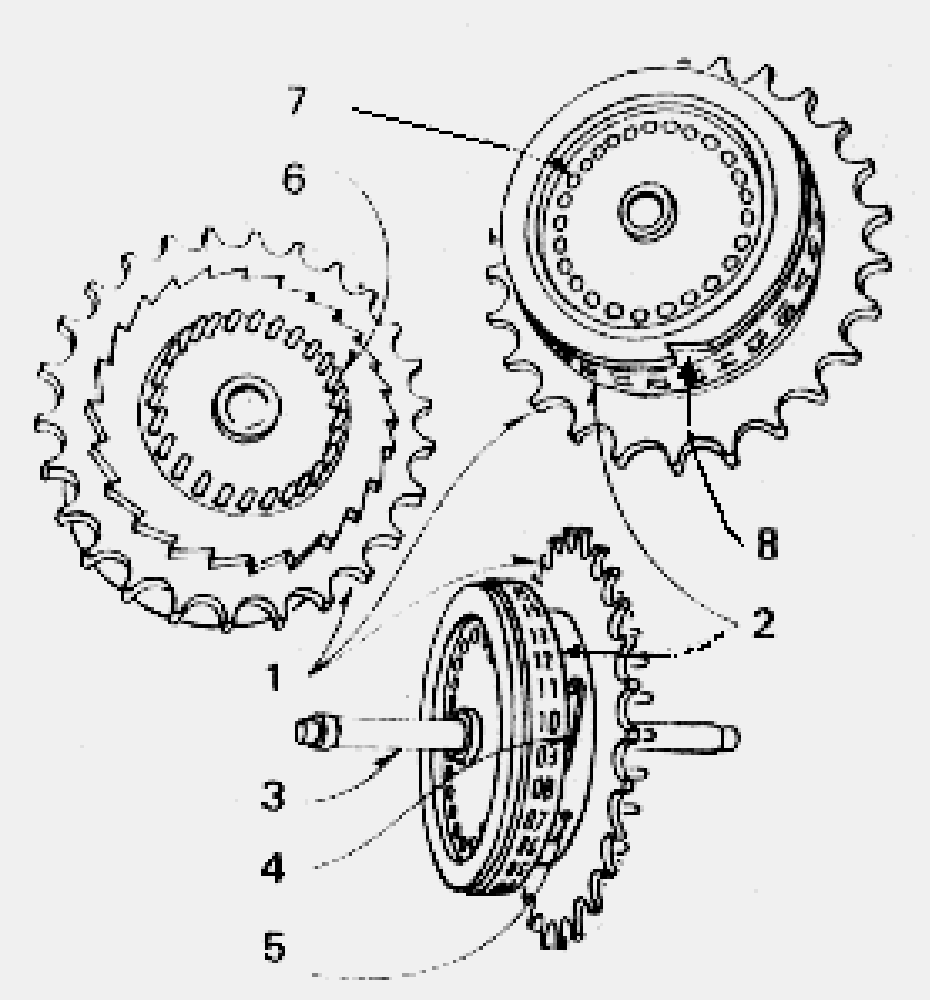
Reflector

Willi Korn
Connects back to another point
Passed back through, 7 total shifts
Made it simpler, no letter can remain the same
Reciprocal



Construction

3 basic wheels
Same buried wiring
4 and 5 added later



Construction

Use

Day

Wheel order

Ring settings

Reflector settings

150,738,274,937,250 possible states

Geheim!

Nicht ins Flugzeug mitnehmen!

Sonder-Maschinenschlüssel BGT

Datum	Walzenlage			Ringstellung			Steckerverbindungen										Kenngruppe		
31.	I	V	III	06	20	24	UA	PF	RQ	SO	NI	EY	BG	HL	TX	ZJ	jeu	nyq	aqm
30.	V	II	III	01	07	12	GF	KV	JM	?B	UW	LX	TD	QS	NA	ZH	azs	zds	kck
29.	IV	I	V	11	17	26	CI	OK	PV	ZL	HX	NB	AW	DJ	FE	ST	kap	gwh	lyx

Breaking the code

Intercepting key
Reciprocal
No repeated letter
Broken by Polish
Breaking green
Breaking red