The Worshipful
Company of Scientific
Instrument Makers

Breaking Enigma & the U-boat Codes and the Legacy of Alan Turing

Tuesday 17th April 2012

Professor David Stupples

Centre for Cyber Security Sciences

BLETCHLEY PARK
National Codes Centre

CITY UNIVERSITY
LONDON

Route map of our journey this evening

THE WORSHIPFUL
COMPANY OF SCIENTIFIC
INSTRUMENT MAKERS

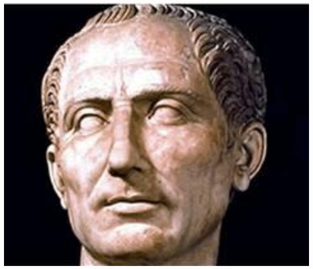
❖Ciphers - coming of age
❖The Enigma Machine
❖Poles and Spies
❖Dilly Knox and Bletchley Park
❖Alan Turing the Man - 100 years young this year
❖Breaking the Enigma Codes
❖Spying on the Airwaves
❖Battle with the U-boats
❖Codes and the Cold War
❖Codes and Ciphers Today - they are part of our every-day life
❖Legacy of Alan Turing

Centre for Cyber Security Sciences

BLETCHLEY PARK
National Codes Centre

Ciphers - coming of age

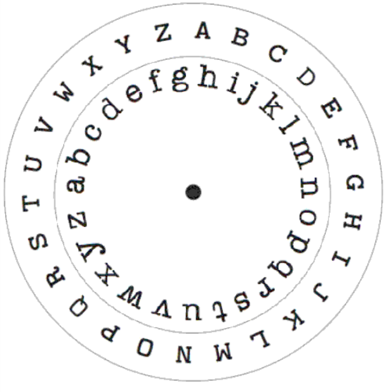
Our journey starts with the Caesar Cipher or ‘monoalphabetic’ substitution cipher



Alan Turing broke the U-Boat code

		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	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	B	C	D	E

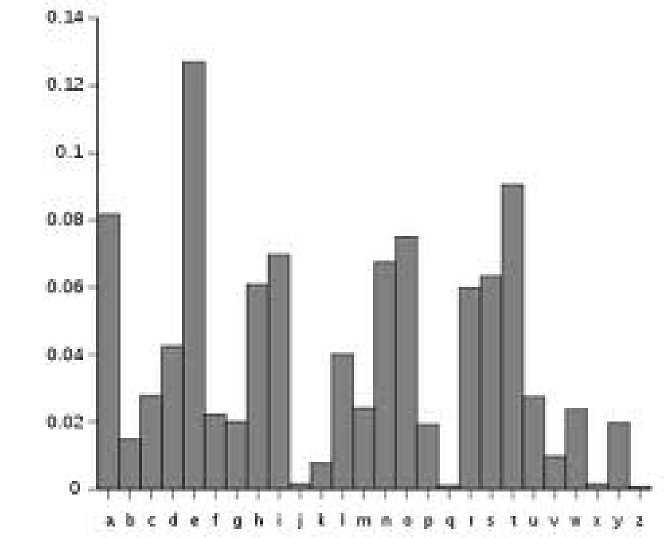
Cncp Vwtkpi dtqmg vjg Wdqcv eqfg


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 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

Letter frequency analysis and analysis of bigrams and trigrams make the cipher useless.

Bigrams – th, he, and in

Trigrams – the, &and tha



Ciphers - coming of age

Codebooks became the preferred communications method of Napoleon but were used throughout history for practising the art of secret writing. The Great Paris Cipher was based on Louis XIV's Grand Chiffre, adapted for use by the military, relying on identical copies of a table containing many numbers in the possession of both the sender and the receiver. It should be noted that this "Cipher" was actually a hybrid between a code and a cipher.

Using the single-number code:1253 could mean "Mississippi".
But it could be enciphered letter-by-letter: 10.42.300.428.69.808.746.478 giving
"m" "i" "s" "s" "i" "p" "p" "i"

Or we can encipher it using bigrams and single letters: 820.5.203.19.746.553
giving "mi" "ss" "is" "si" "p" "pi"

If "m" can be enciphered with three different numbers, "i" with ten, "s" with eight, and "p" with two, we can calculate the number of ways the whole word can be ciphered using just single-letter substitutions:
3 x 10 x 8 x 8 x 10 x 8 x 8 x 10 x 2 x 2 x 10 = 491,520,000

Ciphers - coming of age

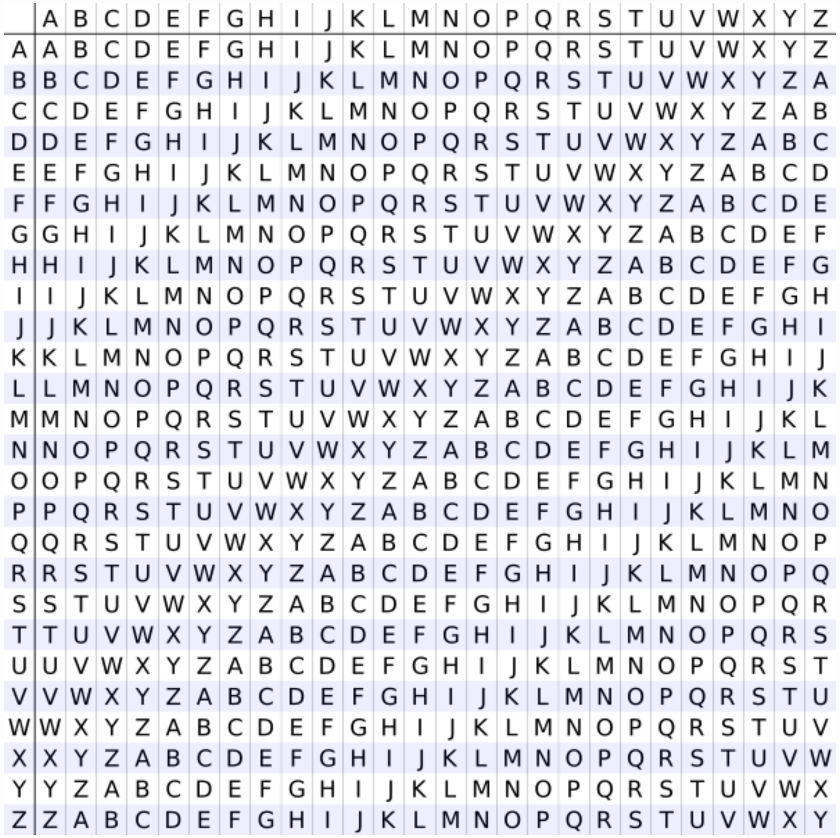
Codebooks are important for our story of Enigma as they were also used by Nazi Germany with the Enigma machine; e.g. Short-weather Codebook.

Major Scovell (English Cryptographer working for Wellington) needed a crib to break the code.
"I received your letter of – July: it is unfortunate that you were not able to attack 1214.609.656.803. occupied 58.850.112.1168.13.1388.1153.820."

Decoded to "I received your letter of – July: it is unfortunate that you were not able to attack the English army while they were occupied with the siege of 1168 of Salamanca."
Such a breakthrough was possible because of the partial enciphering of the message. Scovell's ability to decipher this and other messages came not from frequency analysis or mathematical calculation but from his knowledge of the French language. Using his understanding French syntax, grammar and behavioural characteristics, he could determine what the code numbers represented in context.

Ciphers - coming of age

The **Vigenère cipher** is a method of encrypting alphabetic text by using a series of different Caesar ciphers based on the letters of a keyword. It is a simple form of polyalphabetic substitution. This cipher is important to understanding Enigma!



	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

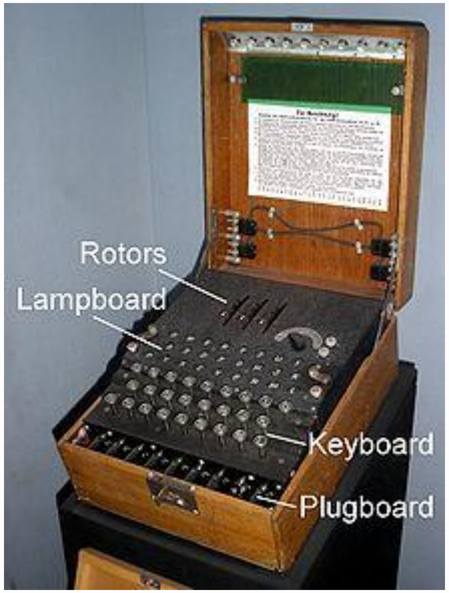
Plaintext:	*ATTACKATDAWN*
Key:	*LEMONLEMONLE*
Ciphertext:	*LXFOPVEFRNHR*

So long as the keyword is secret and is as long as the message the cipher is reasonably good – much better if it were unique ‘lemonisgreat’!

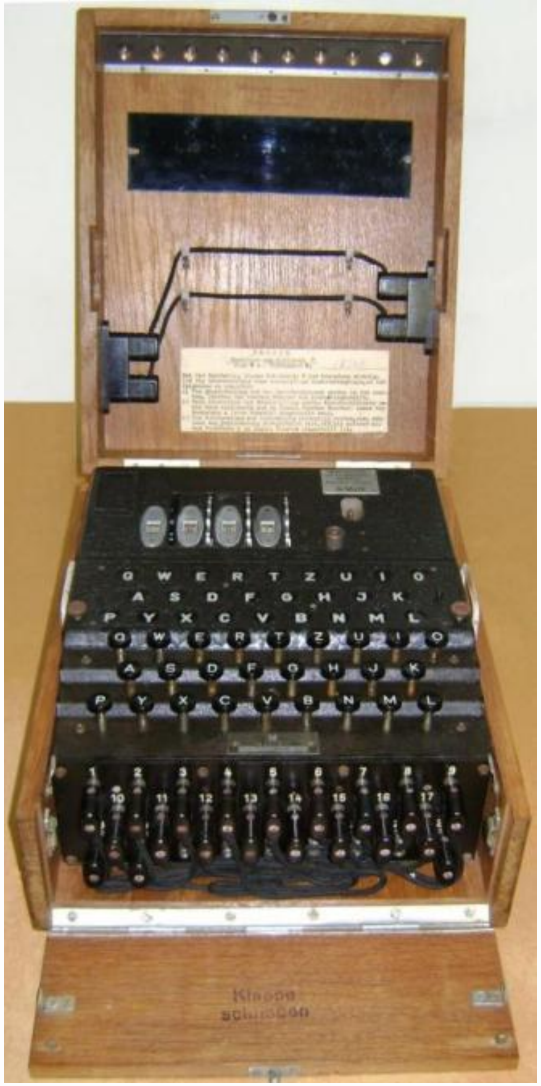
Our last part of basic theory – the key is symmetric – it must be know at both ends!

The Enigma Machine

Three-rotor Enigma machine used by the Wehrmacht and the Luftwaffe



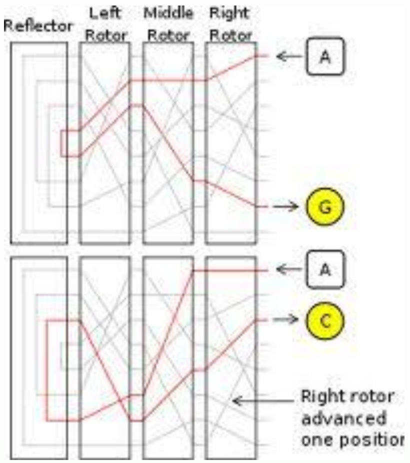
The Enigma Machine

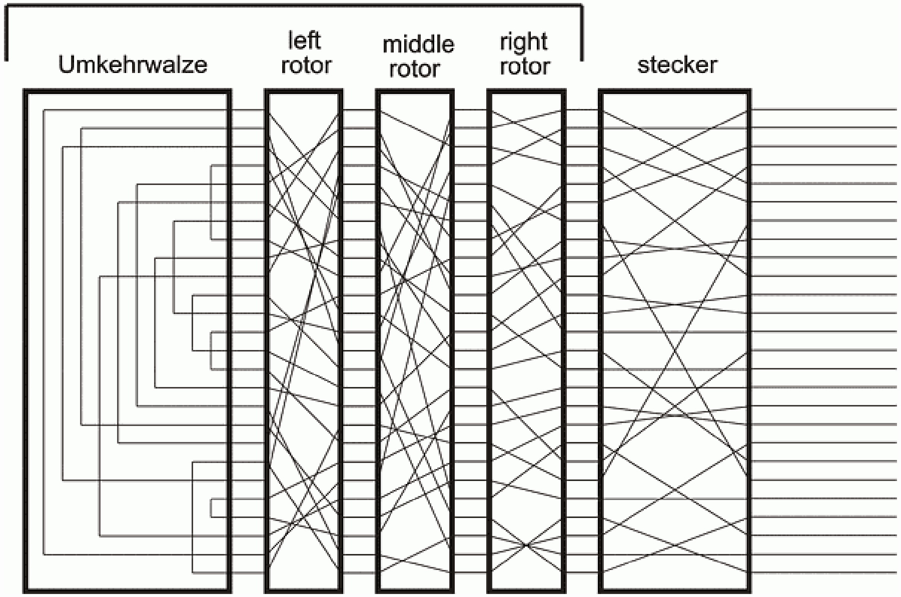


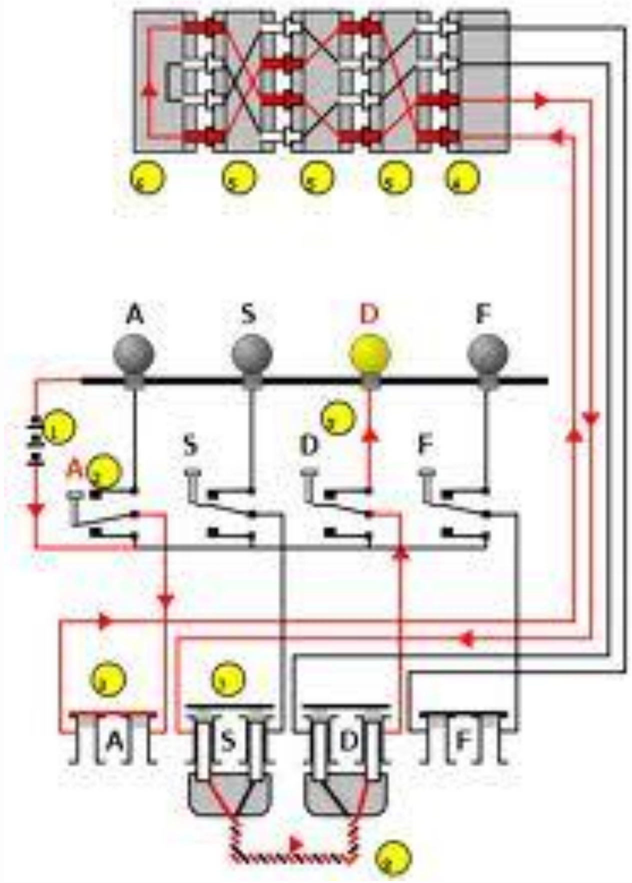
The Kreigsmarine 4-rotor machine

The Enigma Machine

Complexity of the three rotor Enigma machine







The Enigma Machine

Mathematics of the three and four rotor Enigma machines

Step 1 – plugboard (Stekkerboard) combinations (where p is the number of plugs)

$26!/((26\text{-}p)! \text{ x } p! \text{ x } 2^p) = 26!/((26\text{-}10)! \text{ x } 10! \text{ x } 2^{10}) = 150{,}738{,}274{,}937{,}250$

Step 2 – initial rotor (cipher wheel) settings

26^3 = 17,576 possible values – three-rotor Enigma

26^4 = 456,972 possible values - four-Rotor Enigma

Step 3 – possible rotor (cipher wheel) combinations

5!x3!/3!(5-3)!=5x4x3=60 – for the three-rotor Enigma

8!x4!/4!(8-4)!=8x7x5=336 – for the four rotor Enigma

Step 4 – possible rotor notch (ring) combinations

26^2=676 - same for both three and for rotor Enigma

Step 4 – possible practical combinations; theoretical combustions are higher

Plugboard x Initial rotor settings x rotor combinations x notch combinations

150,738,274,937,250 x 17,576 x 60 x 676 = $1.075\text{x}10^{23}$ for the three rotor

150,738,274,937,250 x 456,972 x 336 x 676 = $1.56\text{x}10^{25}$ for the four rotor

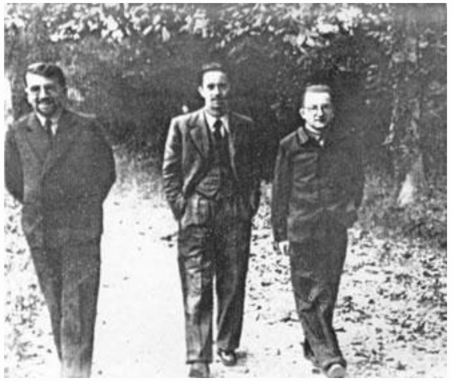
or - **one hundred thousand billion billion (three rotor)**

and – **15 million billion billion (four rotor)**

Poles and Spies

Polish Intelligence (***Biuro Szyfrów)*** needed to break the Enigma traffic driven by the imperative of finding what the Germans were up to. The Bureau's deputy chief, and the chief of its German section (BS-4), was **Captain Maksymilian Ciężki.** In 1932 a team of young mathematicians was set up with **Henryk Zygalski**, **Jerzy Rozycki** and **Marian Rejewski**.

…from left to right

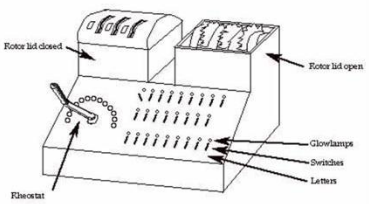


Rejewski made one of the greatest advances in cryptographic history in December 1932 by applying mathematical group theory, to breaking the German military Enigma ciphers. Together they overcame the ever-growing structural and operating complexities of the evolving Enigma with plugboard in the 1930s. They laid the foundations of the science of cryptanalysis and have only recently received their just recognition.

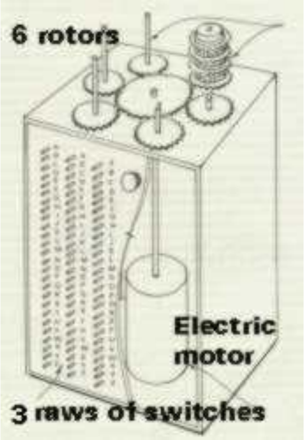
Poles and Spies

The Cyclometer" measured the Enigma cycles. In a few years they were able to set up a library of more than 80,000 typical set ups for Enigma. By mid-1938 they reached the peak of their operation.

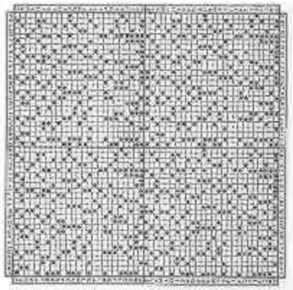
Cyclometer
(Figure 4)



Rejewski developed a faster and more powerful approach comprising six Enigma machines connected together and driven by a single motor - the **Bomba**, a term later used at Bletchley Park. Using the Bomba, all combinations could be examined in two hours. By November 1938 the system was operating and German messages were again being decrypted.



Zygalski developed a method using perforated sheets. Each sheet had 51x51 squares and about 1000 holes arranged in a pattern. Twenty-six sheets, one for each rotor position, were required. As the sheets were superimposed and adjusted on each other, light was passed through giving possible solutions. Six sets of these were required for finding possible Enigma settings. This substantially reduced demand on the "Bomba".

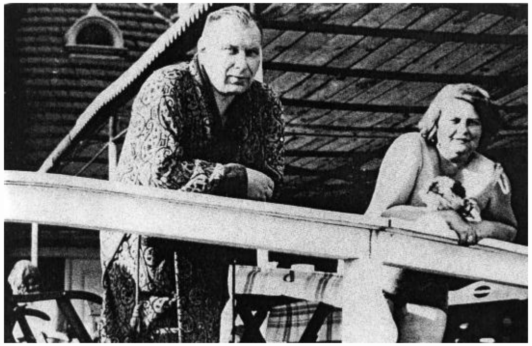


BLETCHLEY PARK
National Codes Centre

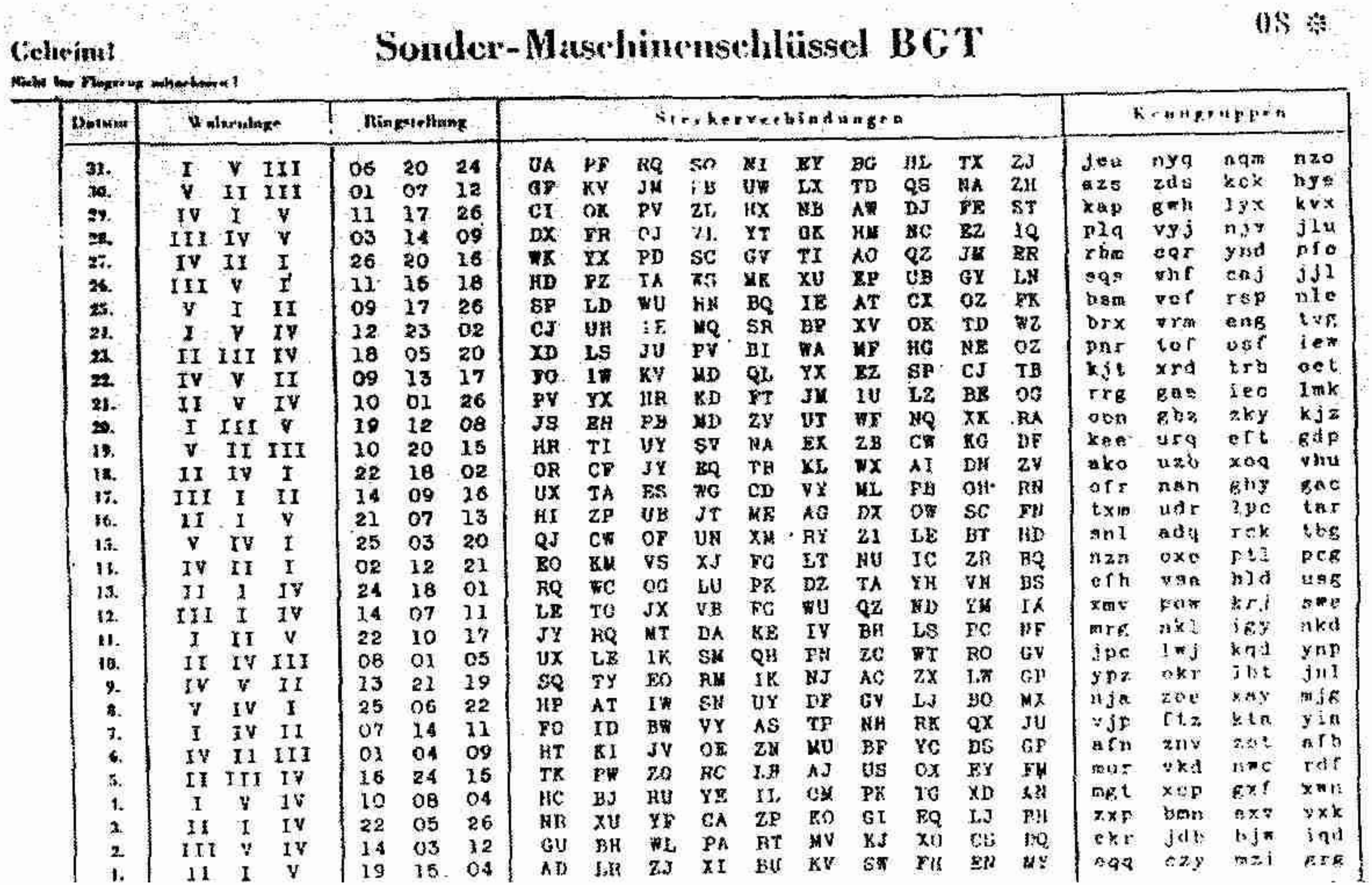
Poles and Spies

In the early 1930s, Schmidt (a serving officer) at the German Armed Forces' cryptographic headquarters. Shortly after the military version of the Enigma machine was introduced, he contacted French intelligence and offered to supply information about the new machine (for money). His offer was accepted by Captain Gustave Bertrand of French Intelligence, and he received from the French the codename *Asche*, and was assigned a French contact, codenamed *Rex*. For the next several years, until he left his position in Germany, he met with French agents at various European cities and supplied them copies of the Enigma machine's instruction manual, operating procedures, and lists of key settings. Even with this information, however, French Intelligence was unable to break messages encrypted on the Enigma. Nor were the British cryptologists whom Bertrand contacted able to make any headway.

Figure 41: Hans-Thilo Schmidt.



Poles and Spies



Geheim!

Nicht ins Flugzeug mitnehmen!

Sonder-Maschinenschlüssel BGT

08

Datum	Walzenlage			Ringstellung			Steckerverbindungen										Kenngruppen			
31.	I	V	III	06	20	24	UA	PF	RQ	SO	KI	EY	BG	HL	TX	ZJ	jeu	nyq	nqm	nzo
30.	V	II	III	01	07	12	GP	KV	JM	IB	UW	LX	TD	QS	NA	ZH	azs	zdu	kck	hye
29.	IV	I	V	11	17	26	CI	OK	PV	ZL	HX	NB	AW	DJ	FE	ST	xap	gwh	lyx	kvx
28.	III	IV	V	03	14	09	DX	FR	CJ	VL	YT	GK	HM	NC	EZ	IQ	plq	vyj	njv	jlu
27.	IV	II	I	26	20	16	WK	YX	PD	SC	GV	TI	AO	QZ	JM	ER	rbm	eqr	ynd	pfo
26.	III	V	I	11	16	18	HD	PZ	TA	WS	MK	XU	EP	UB	GY	LN	sqs	whf	caj	jjl
25.	V	I	II	09	17	26	SP	LD	WU	HN	BQ	IE	AT	CX	OZ	FK	bsm	vcf	rsp	nle
24.	I	V	IV	12	23	02	CJ	UH	IE	MQ	SR	BP	XV	OK	TD	WZ	brx	vrm	eng	tvg
23.	II	III	IV	18	05	20	XD	LS	JU	PV	BI	WA	MF	HG	NE	OZ	pnr	tof	usf	iew
22.	IV	V	II	09	13	17	FO	IW	KV	MD	QL	YX	EZ	SP	CJ	TB	kjt	xrd	trb	oet
21.	II	V	IV	10	01	26	PV	YX	HR	KD	FT	JM	IU	LZ	BK	OG	rrg	gas	iec	lmk
20.	I	III	V	19	12	08	JS	EH	PB	MD	ZV	UT	WF	NQ	XK	RA	oon	gbz	zky	kjz
19.	V	II	III	10	20	15	HR	TI	UY	SV	NA	EK	ZB	CW	KG	DF	kee	urq	eft	gdp
18.	II	IV	I	22	18	02	OR	CF	JY	EQ	TH	KL	WX	AI	DN	ZV	ako	uzb	xoq	vhu
17.	III	I	II	14	09	16	UX	TA	ES	WG	CD	VY	ML	FB	OH	RN	ofr	nan	ghy	gac
16.	II	I	V	21	07	13	HI	ZP	UB	JT	ME	AG	DX	OW	SC	FN	txm	udr	lpc	tar
15.	V	IV	I	25	03	20	QJ	CW	OF	UN	XM	RY	ZI	LE	BT	HD	snl	adq	rck	tbg
14.	IV	II	I	02	12	21	EO	KM	VS	XJ	FC	LT	NU	IC	ZR	RQ	nzn	oxe	ptl	pcg
13.	II	I	IV	24	18	01	RQ	WC	OG	LU	PK	DZ	TA	YH	VN	BS	cfh	vsa	hld	usg
12.	III	I	IV	14	07	11	LE	TG	JX	VB	FC	WU	QZ	ND	YM	IA	xmv	pow	krj	swe
11.	I	II	V	22	10	17	JY	HQ	MT	DA	KE	IV	BH	LS	FC	PF	mrg	nkl	igy	nkd
10.	II	IV	III	08	01	05	UX	LE	IK	SM	QH	FN	ZC	WT	RO	GV	jpc	lwj	kqd	ynp
9.	IV	V	II	13	21	19	SQ	TY	EO	RM	IK	NJ	AC	ZX	LW	GP	ypz	okr	jbt	jnl
8.	V	IV	I	25	06	22	HP	AT	IW	SN	UY	DF	GV	LJ	BO	MX	nja	zoe	xay	mjg
7.	I	IV	II	07	14	11	FO	ID	BW	VY	AS	TP	NH	RK	QX	JU	vjp	ftz	ktn	yin
6.	IV	II	III	01	04	09	HT	KI	JV	OE	ZN	MU	BF	YC	DS	GP	afn	znv	zot	afb
5.	II	III	IV	16	24	15	TK	PW	ZO	RC	LB	AJ	US	OX	EY	FM	mur	vkd	nwc	rdf
4.	I	V	IV	10	08	04	HC	BJ	RU	YE	IL	CM	PK	TG	XD	AN	mgt	xcp	gxf	xwn
3.	II	I	IV	22	05	26	NB	XU	YF	CA	ZP	EO	GI	EQ	LJ	PH	zxp	bmn	axv	vxk
2.	III	V	IV	14	03	12	GU	BH	WL	PA	RT	MV	KJ	XO	CE	DQ	ekr	jdb	bjw	iqd
1.	II	I	V	19	15	04	AD	LR	ZJ	XI	BU	KV	SW	FU	EN	MY	oqq	czy	mzi	zrg

Bletchley Park – Station X

In 1939, Bletchley Park received the work from the Poles and combined it with work already undertaken. Dilly Knox and his team (Mavis Batey, nee Lever, being one) were able to make substantial progress on the non-stekkered enigma machines including the 'K' (used by the Italians at the Battle of Matapan) and the 'G' used by the German Secret Service (Abwehr).

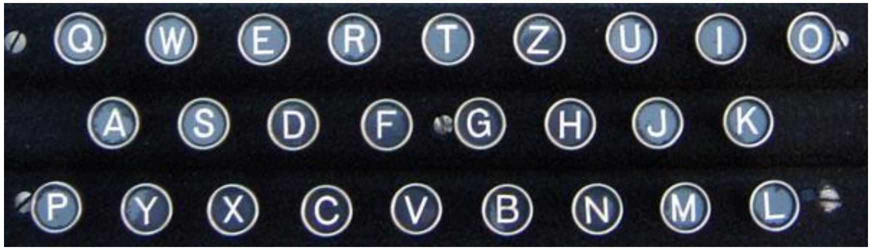
The technique used was 'rodding' invented by Dilly Knox. 'Rodding' required a crib with which to begin, however this technique did not provide a complete sequence of characters from the plain text and considerable linguistic skill was required to fill in the gaps, not unlike that required for solving crossword puzzles. Every correct inference made about the content of a message obtained in this way could then be used as an extension of the crib, and this would enable the process to be continued.

Bletchley Park – Station X

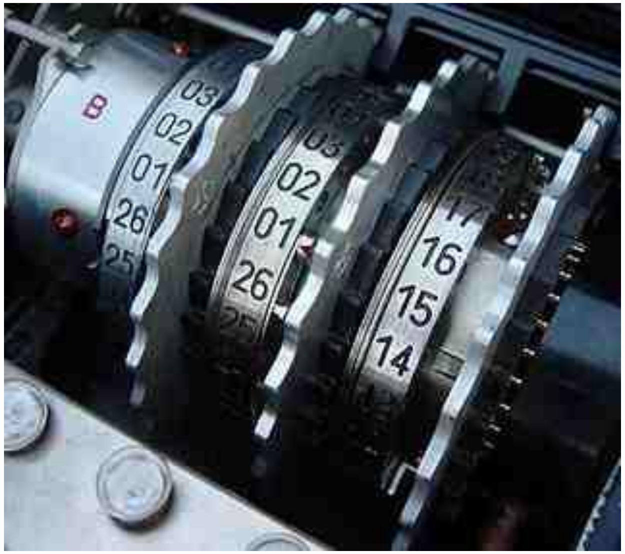
Help from the Germans in deciphering Enigma!

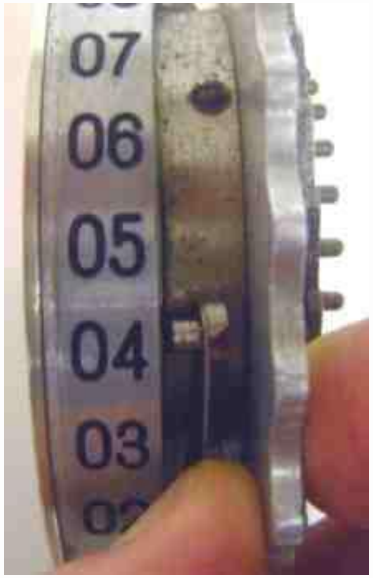
Cillies

When army/airforce operators were setting wheel start positions they often used the keyboard as an aid memoire, or part of a well known saying, etc



Herivel Tip





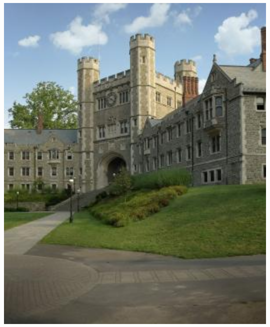
The ring settings could be adjusted before or after inserting the rotors into the machine. Herivel assumed that at least some of the operators would adjust them after. In the normal course of things, adjusting the rotors inside the machine would likely leave the correct ring setting at the top, or near the top, of the rotors.

Alan Turing the Man - 100 years young

Alan Mathison Turing, OBE, FRS, 23 June 1912 – 7 June 1954, was an English mathematician, logician, cryptanalyst, and computer scientist.

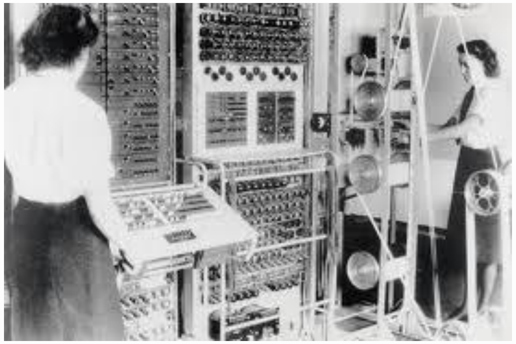
Sherborne School, Dorset,1926-30

Kings College, Cambridge
1931-34; Mathematics

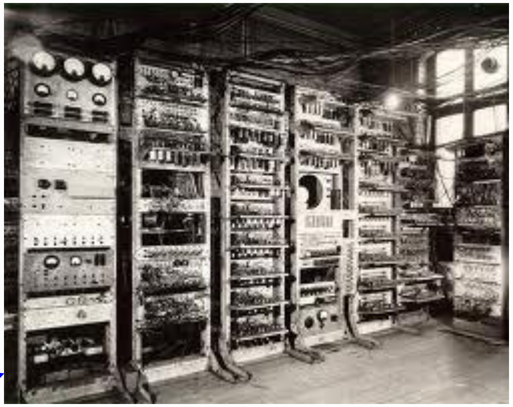


Princeton, New Jersey
1936-38; PhD Mathematics

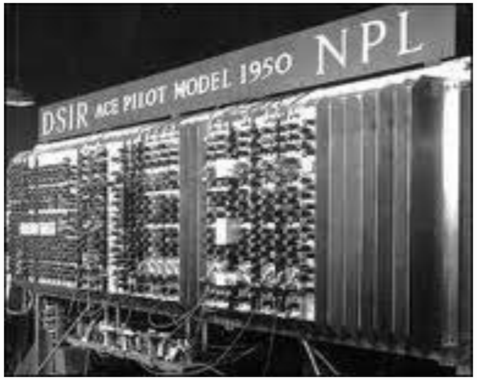
Alan Turing the Man - 100 years young



Bletchley Park - GC&CS
Bombe 1940-45



Electronic Delay Storage
Automatic Calculator –Manchester
University 1948-54



Automatic Computing Engine at the
National Physical Laboratory 1945-48

Cray
Supercomputer
2010

Centre for Cyber Security Sciences

BLETCHLEY PARK
National Codes Centre

Breaking the Enigma Codes

Alan Turing devised a procedure for breaking the Enigma based on a ‘crib’ known by codebreakers (cryptanalysts) and a plaintext attack. This procedure reduces the key space to a little over one million combinations and does not need prior knowledge of the plugboard (stekker) connections.

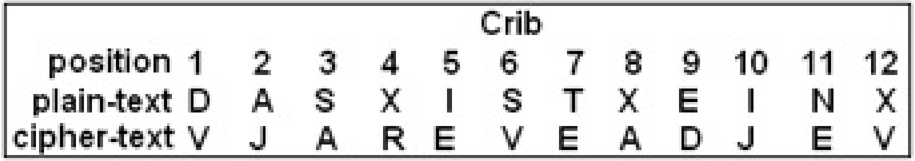
For our example – part of a common W/T test transmission often had the plain text DASXISTXEINXABSTIMM - this text uses X to represent a space.

The cipher text could be: ADVJAREVEADJEVGHRQNNDMCPA
Slide the plain-text crib to avoid encryption of a letter to itself!

A	**D**	**V**	**J**	**A**	**R**	**E**	**V**	**E**	**A**	**D**	**J**	**E**	**V**	**G**	**H**	**R**	**Q**	**N**	**N**	**D**	**M**	**C**	**P**	**A**
		D	**A**	**S**	**X**	**I**	**S**	**T**	**X**	**E**	**I**	**N**	**X**	**A**	**B**	**S**	**T**	**I**	**M**	**M**				

Move the plaintext to fit

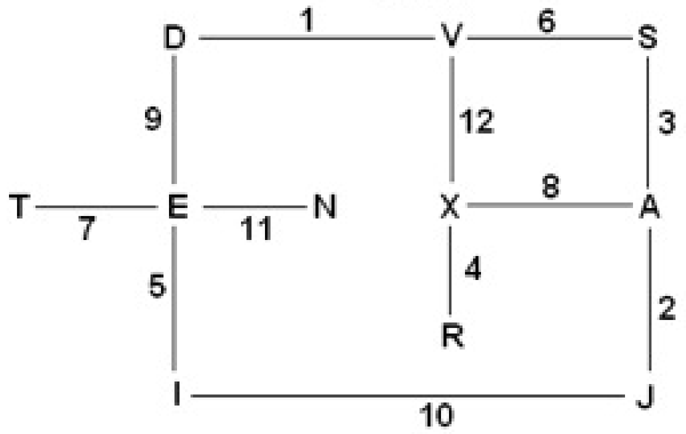
For my example I will shorten the crib slightly to develop a Bletchley menu.



Crib

position	1	2	3	4	5	6	7	8	9	10	11	12
plain-text	D	A	S	X	I	S	T	X	E	I	N	X
cipher-text	V	J	A	R	E	V	E	A	D	J	E	V

Menu



Note that this menu has two loops

D→V→ S→ A →J →I →E →D

S →A→X→V

Also note relative positions of the rotors as the cipher text proceeds

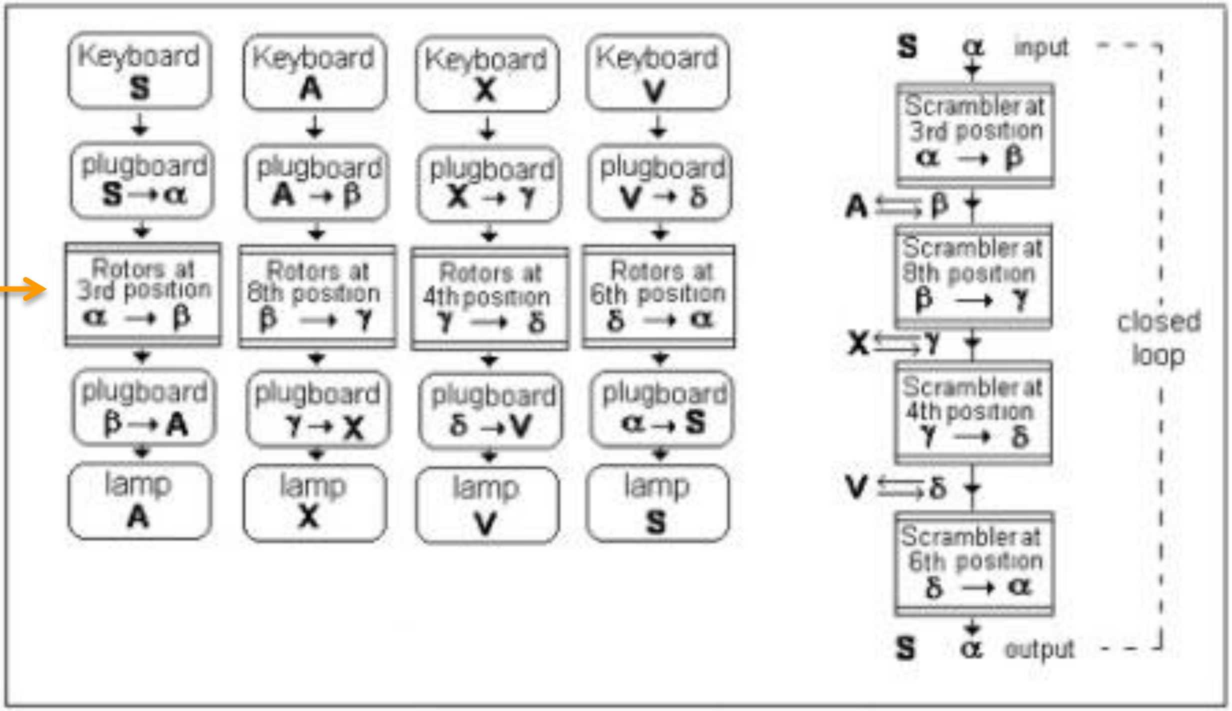
Using the smaller loop, we shall see that we have enough information to begin our break of Enigma code

Courtesy of the Rutherford Journal

Breaking the Enigma Codes

Turing used logic and hypothesis testing and contradictions to identify the first of stekker connections.

Replicas of the Enigma rotors (cipher wheels) each of these represent one Enigma machine.


Keyboard S
Keyboard A
Keyboard X
Keyboard V
plugboard S→α
plugboard A→β
plugboard X→γ
plugboard V→δ
Rotors at 3rd position α→β
Rotors at 8th position β→γ
Rotors at 4th position γ→δ
Rotors at 6th position δ→α
plugboard β→A
plugboard γ→X
plugboard δ→V
plugboard α→S
lamp A
lamp X
lamp V
lamp S
S α input
Scrambler at 3rd position α→β
A ⇆ β
Scrambler at 8th position β→γ
X ⇆ γ
Scrambler at 4th position γ→δ
V ⇆ δ
Scrambler at 6th position δ→α
S α output
closed loop

This procedure exploits the symmetrical relationship between the stekker pairs; if S is stekkered to ‘a’ then ‘a’ is stekkered to S.

Courtesy of the Rutherford Journal

Breaking the Enigma Codes

Turing had made a very important breakthrough but the method was still impractical timewise. A serious operational difficulty with the first (prototype) Bombe was that the menu should contain at least three loops and hence the crib needed to be long. Most German wartime messages were relatively short.

Gordon Welchman, another Cambridge mathematician, realised that the symmetry property of the stekker board could be exploited further and developed a diagonal board addition for the Bombe. Briefly it worked like this;

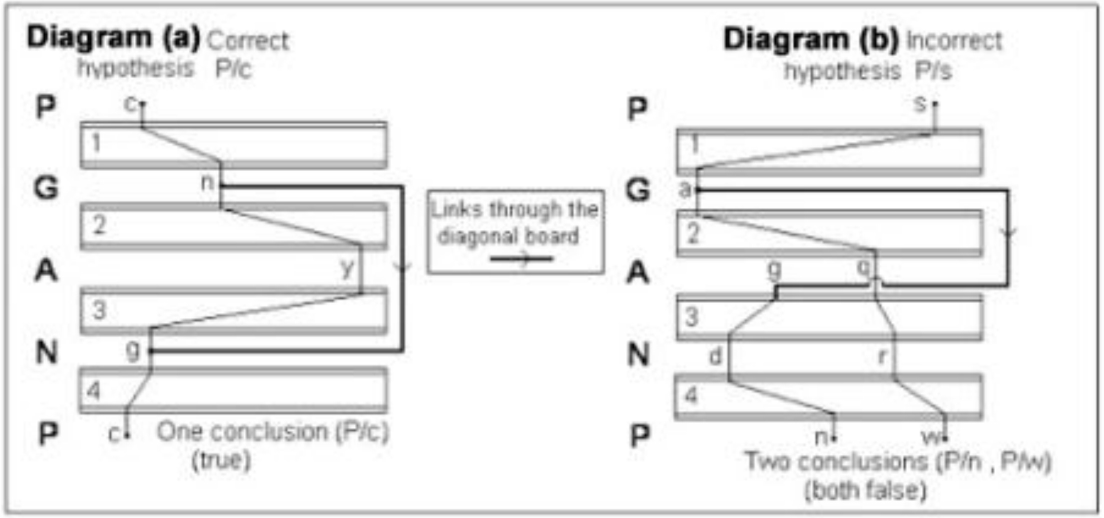
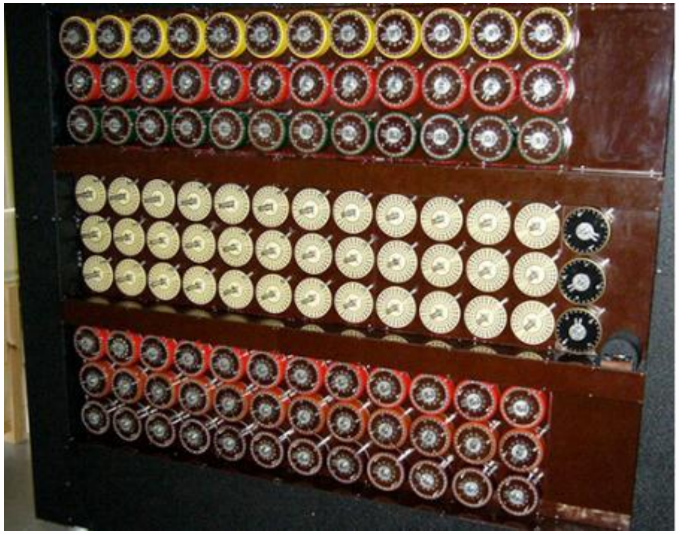
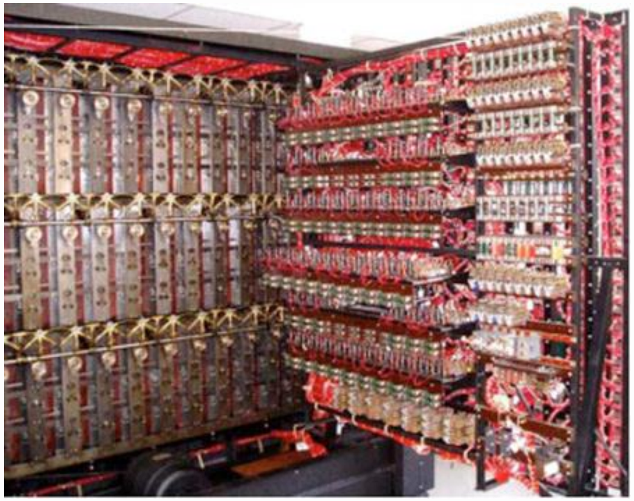


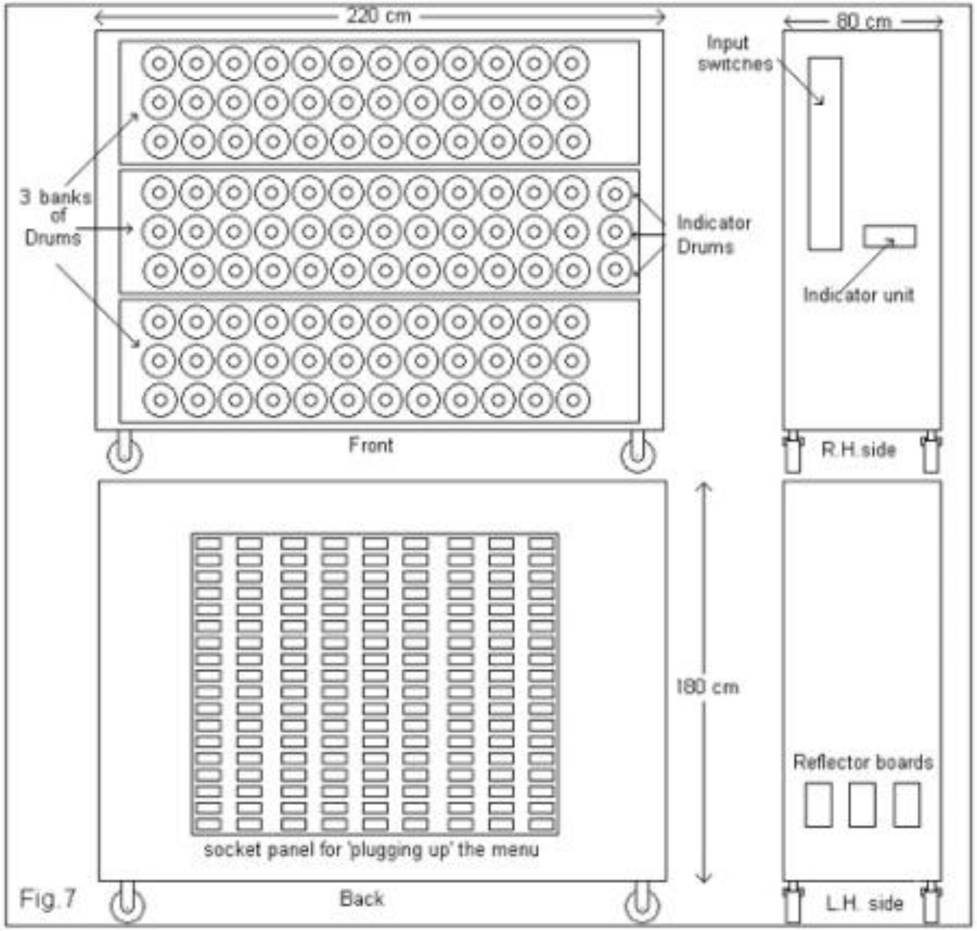
Diagram (a) Correct hypothesis P/c
P
c
1
G
n
2
A
y
3
N
g
4
P
c
One conclusion (P/c)
(true)
Links through the diagonal board
Diagram (b) Incorrect hypothesis P/s
P
s
1
G
a
2
A
g
q
3
N
d
r
4
P
n
w
Two conclusions (P/n , P/w)
(both false)

Breaking the Enigma Codes

The physical characteristics of the Turing/Welchman Bombe





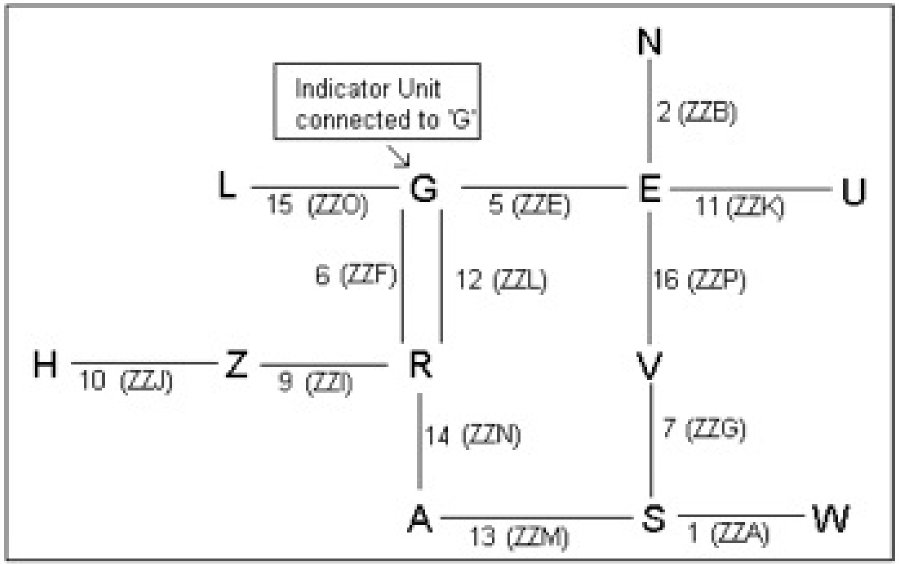


Centre for Cyber Security Sciences

Breaking the Enigma Codes

A worked simple example from Bletchley Park – used to test the rebuilt Bombe

Positions	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Cipher	S	N	M	K	G	G	S	T	Z	Z	U	G	A	R	L	V
Plain	W	E	T	T	E	R	V	O	R	H	E	R	S	A	G	E



Positional No	**Drum Letter Positions**	**Positional No**	**Drum Letter Positions**
0	ZZZ	26	ZAZ
1	ZZA	27	ZAA
2	ZZB	28	ZAB
3	ZZC	29	ZAC
--	--	--	--
25	ZZY	51	ZAY

Breaking the Enigma Codes

A worked simple example - continued

After several runs the rotor order was found to be II, V and III

The starting position of the rotors (the indicator) DKK

The stekker pair was G/Q used for the hypothesis

A checking machine found the other stekkers to be to A/D, E/T, H/M, L/J, N/V, U/F, Z/P with no stekkers R/R, S/S, and W/W.

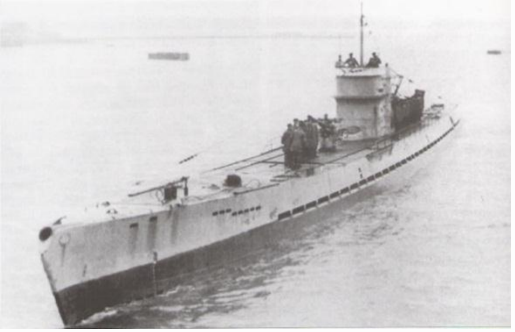
The ninth and tenth stekker pairs were found from letters from the crib that were not used.

Since the set up was found for the day – the only thing that would change from message to message during the that day was the three letter indicator – which was relatively easy to find.

Spying on the Airwaves

Wehrmacht radio operations

Radio operator on board of U-124.



Luftwaffe Radio operations

Every U-boat & surface ship, every Wehrmacht unit and every Luftwaffe unit and squadron would be equipped with radio and Enigma for secure radio communications

Spying on the Airwaves

Y-Intercept Stations

Beaumanor Hall

Wireless operators (Wops)- the unsung heroes of the signals war!

Spying on the Airwaves

Beachy Head, Sussex
Beaumanor Hall, near Loughborough
Beeston Bump, Beeston Regis, Norfolk
Bishop's Waltham, Hampshire
RAF Canterbury, Kent
Cheadle, Staffordshire
RAF Chicksands, Bedfordshire
RAF Clophill, Bedfordshire
Cromer, Norfolk
G.P.O. Radiophone Station Kemback
Foreign Office Denmark Hill, Camberwell
Met Office Dunstable, Bedfordshire
Felixstowe, Suffolk
Gilnahirk, Belfast
Gorleston, Norfolk
Harpenden, Hertfordshire (Army, No. 1 Special Wireless Group)
HMS Flowerdown, Winchester, Hampshire
HMS Forest Moor, Harrogate, Yorkshire
Kedleston Hall, Derbyshire
RAF Kingsdown, West Kingsdown, Kent
RAF Monks Risborough, Buckinghamshire
Foreign Office Knockholt, Kent
Army Markyate, Hertfordshire
North Walsham, Norfolk
Foreign Office Sandridge, Hertfordshire
Saxmundham, Suffolk
Army Shenley Hertfordshire
South Walsham, Norfolk
Southwold, Suffolk
Stockland Bristol Nr Bridgwater, Somerset
Stockton-on-Tees, Cleveland
RAF Waddington, Lincolnshire

Battle with the U-boats

The difficulty with the Naval Enigma (Shark) was that the messages were very short and that ‘codebooks’ were used to add security and increase efficiency of communication.

Two messages received by Scarborough:

SC28/04/43 0940 7369 A348
LQB 0910/28/04/43 QGMI VVEE SERQ YGBW IAHK HW…….BHB

SC28/04/43 1140 7369 A356
TMF 1110/28/04/43 MLWP EOIG VUWY USNT AHFT WW…….LLG

Without knowledge of the codebook and the message indicator (setting of the rotor wheels) this message would be impossible to read – ie there is no crib to work on.

Battle with the U-boats

This is how the naval operator set the wheels (*Kenngruppenbuch* Indicator System). Select two trigrams from the *Kenngruppenbuch* – say ***BFA*** and ***LXZ***, add two random letters and lay out as follows.

C B F A
L X Z B

The operator turned his wheels to the ground settings (given in his setting list for the day) and tapped out ***LXZ*** to get and enciphered indicator – say ***RGL.*** The operator then turned his wheels to this setting and enciphered his message. The fourth wheel was set as part of the daily settings.

Before sending the enciphered text the operator had to disguise the key setting for the recipient. Procedure is as follows:

C B F A
L X Z B

Bigram tables

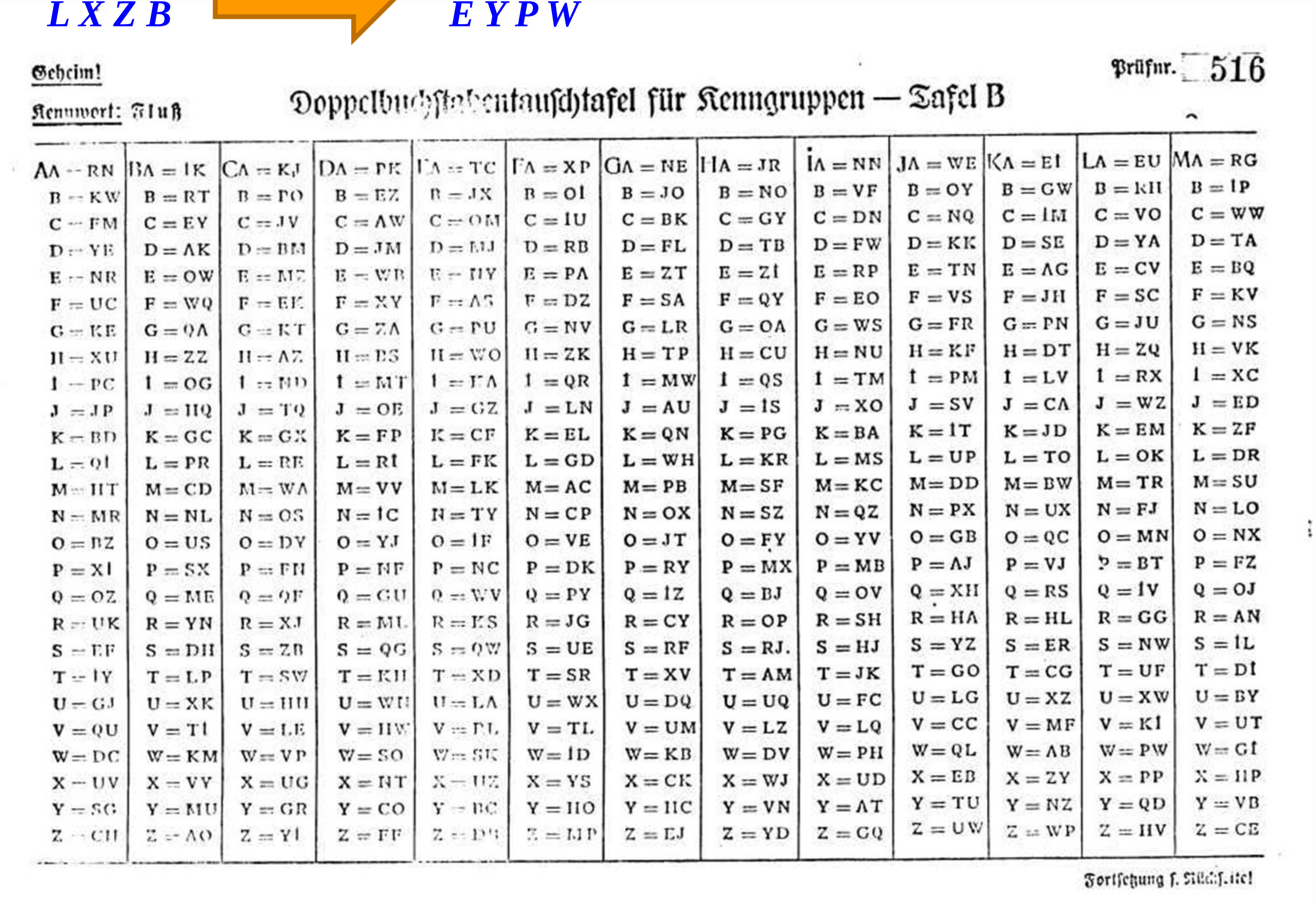
R V M K
E Y P W

The indicator ***RVMK EYPW*** was then sent in plaintext before the encrypted message

With non-naval Enigma the indicator was simply encoded with the base setting from 1938.

Battle with the U-boats

C B F A → R V M K
L X Z B → E Y P W



Geheim!

Prüfnr. 516

Kennwort: Fluß

Doppelbuchſtabentauſchtafel für Kenngruppen — Tafel B

AA = RN	BA = IK	CA = KJ	DA = PK	EA = TC	FA = XP	GA = NE	HA = JR	IA = NN	JA = WE	KA = EI	LA = EU	MA = RG
B = KW	B = RT	B = PO	B = EZ	B = JX	B = OI	B = JO	B = NO	B = VF	B = OY	B = GW	B = KH	B = IP
C = FM	C = EY	C = JV	C = AW	C = OM	C = IU	C = BK	C = GY	C = DN	C = NQ	C = IM	C = VO	C = WW
D = YE	D = AK	D = BM	D = JM	D = MJ	D = RB	D = FL	D = TB	D = FW	D = KK	D = SE	D = YA	D = TA
E = NR	E = OW	E = MZ	E = WB	E = HY	E = PA	E = ZT	E = ZI	E = RP	E = TN	E = AG	E = CV	E = BQ
F = UC	F = WQ	F = EK	F = XY	F = AS	F = DZ	F = SA	F = QY	F = EO	F = VS	F = JH	F = SC	F = KV
G = KE	G = QA	G = KT	G = ZA	G = PU	G = NV	G = LR	G = OA	G = WS	G = FR	G = PN	G = JU	G = NS
H = XU	H = ZZ	H = AZ	H = BS	H = WO	H = ZK	H = TP	H = CU	H = NU	H = KF	H = DT	H = ZQ	H = VK
I = PC	I = OG	I = ND	I = MT	I = EA	I = QR	I = MW	I = QS	I = TM	I = PM	I = LV	I = RX	I = XC
J = JP	J = HQ	J = TQ	J = OE	J = GZ	J = LN	J = AU	J = IS	J = XO	J = SV	J = CA	J = WZ	J = ED
K = BD	K = GC	K = GX	K = FP	K = CF	K = EL	K = QN	K = PG	K = BA	K = IT	K = JD	K = EM	K = ZF
L = QI	L = PR	L = RE	L = RI	L = FK	L = GD	L = WH	L = KR	L = MS	L = UP	L = TO	L = OK	L = DR
M = HT	M = CD	M = WA	M = VV	M = LK	M = AC	M = PB	M = SF	M = KC	M = DD	M = BW	M = TR	M = SU
N = MR	N = NL	N = OS	N = IC	N = TY	N = CP	N = OX	N = SZ	N = QZ	N = PX	N = UX	N = FJ	N = LO
O = BZ	O = US	O = DY	O = YJ	O = IF	O = VE	O = JT	O = FY	O = YV	O = GB	O = QC	O = MN	O = NX
P = XI	P = SX	P = FH	P = NF	P = NC	P = DK	P = RY	P = MX	P = MB	P = AJ	P = VJ	P = BT	P = FZ
Q = OZ	Q = ME	Q = QF	Q = GU	Q = WV	Q = PY	Q = IZ	Q = BJ	Q = OV	Q = XH	Q = RS	Q = IV	Q = OJ
R = UK	R = YN	R = XJ	R = ML	R = KS	R = JG	R = CY	R = OP	R = SH	R = HA	R = HL	R = GG	R = AN
S = EF	S = DH	S = ZB	S = QG	S = QW	S = UE	S = RF	S = RJ.	S = HJ	S = YZ	S = ER	S = NW	S = IL
T = IY	T = LP	T = SW	T = KH	T = XD	T = SR	T = XV	T = AM	T = JK	T = GO	T = CG	T = UF	T = DI
U = GJ	U = XK	U = HH	U = WH	U = LA	U = WX	U = DQ	U = UQ	U = FC	U = LG	U = XZ	U = XW	U = BY
V = QU	V = TI	V = LE	V = HW	V = PL	V = TL	V = UM	V = LZ	V = LQ	V = CC	V = MF	V = KI	V = UT
W = DC	W = KM	W = VP	W = SO	W = SK	W = ID	W = KB	W = DV	W = PH	W = QL	W = AB	W = PW	W = GI
X = UV	X = VY	X = UG	X = NT	X = UZ	X = YS	X = CK	X = WJ	X = UD	X = EB	X = ZY	X = PP	X = HP
Y = SG	Y = MU	Y = GR	Y = CO	Y = BC	Y = HO	Y = HC	Y = VN	Y = AT	Y = TU	Y = NZ	Y = QD	Y = VB
Z = CH	Z = AO	Z = YI	Z = FF	Z = DB	Z = MP	Z = EJ	Z = YD	Z = GQ	Z = UW	Z = WP	Z = HV	Z = CE

Fortſetzung ſ. Rückſeite!

Battle with the U-boats

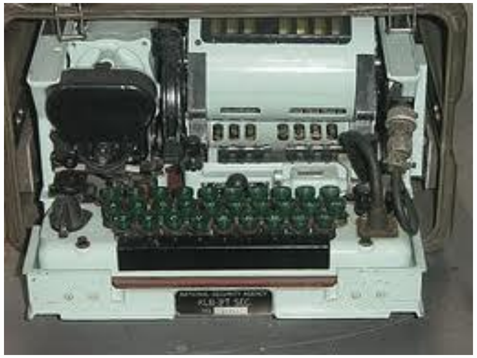
Turing developed a system he called Banburismus to derive the indicators. The aim of Banburismus was to reduce the time required of the electromechanical Bombe machines by identifying the most likely right-hand and middle wheels of the Enigma. BP performed the procedure continuously for two years, stopping only in 1943 when sufficient bombe time became readily available. The principle behind Banburismus was similar ideas to the to the Index of Coincidence within language.

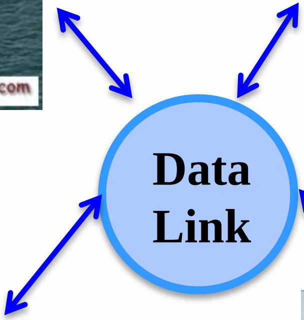
However, BP also relied on ‘pinches’ to recover Cryptographic ‘key’ and ‘codebook’ material. Here are some of the operations.

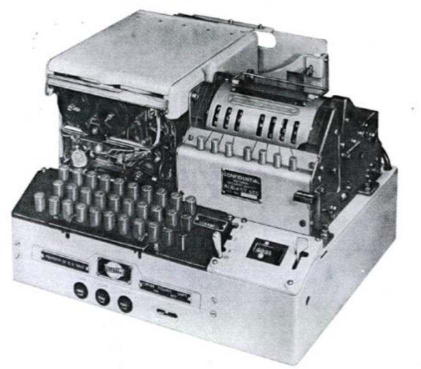
26/4/1940 Polares, a German trawler captured – Enigma logs/settings/Naval indicators
12/09/1940 proposed daring pinch in the English Channel by Ian Fleming
4/3/1941 Krebs, German trawler captured – Naval Enigma settings
7/5/1941 Munchen, German weather ship captured – Naval Enigma settings
9/5/1941 U-110 captured – Enigma settings, codebooks and Offizier settings
28/6/1941 Lauenburg weather ship – Enigma settings, codebooks, bigram tables
27/8/1941 U-570 captured – Enigma settings
20/1/1942 Germans replace short weather codebook; now unable to read Naval Enigma
30/10/1942 U-559 capture – Enigma settings, short-weather codebooks etc available

After Enigma and the Cold War

Were all the lessons learned on how to secure cryptographic keys?





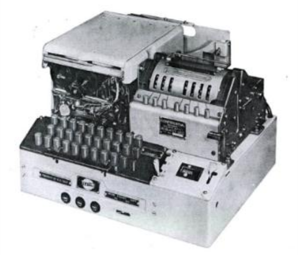


Protected by the encryption devices – KL47 and KL7

US Navy (1968-84)

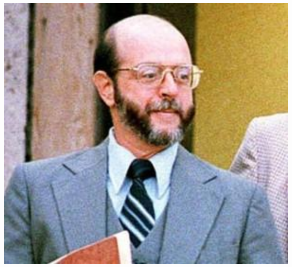
After Enigma and the Cold War

In January 1968, USS Pueblo (Signals Intelligence Ship) was captured off North Korea



24 hours later

From 1968 to 1985 the Walker Spy Ring Passed to Cryptographic key data to the Soviets.

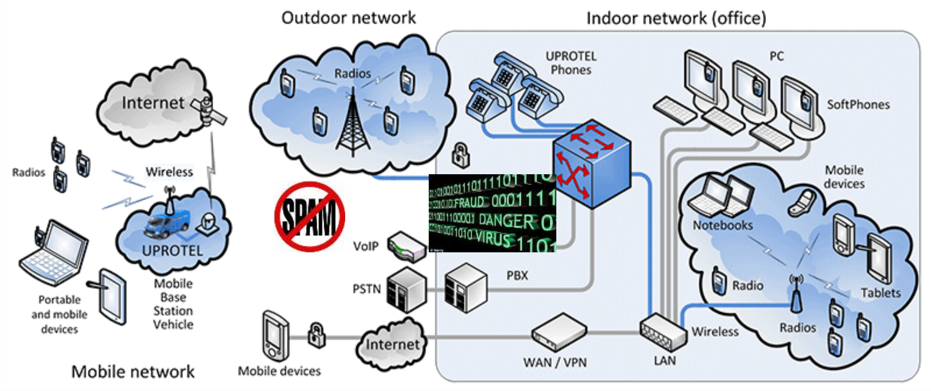


Codes and Ciphers Today

………ciphers are part of our every day life they protect our privacy and our personal secrets …..Turing has taught to look after the cipher – it will then look after us!

Follow us on twitter

ebay
Visit Our Ebay Shop



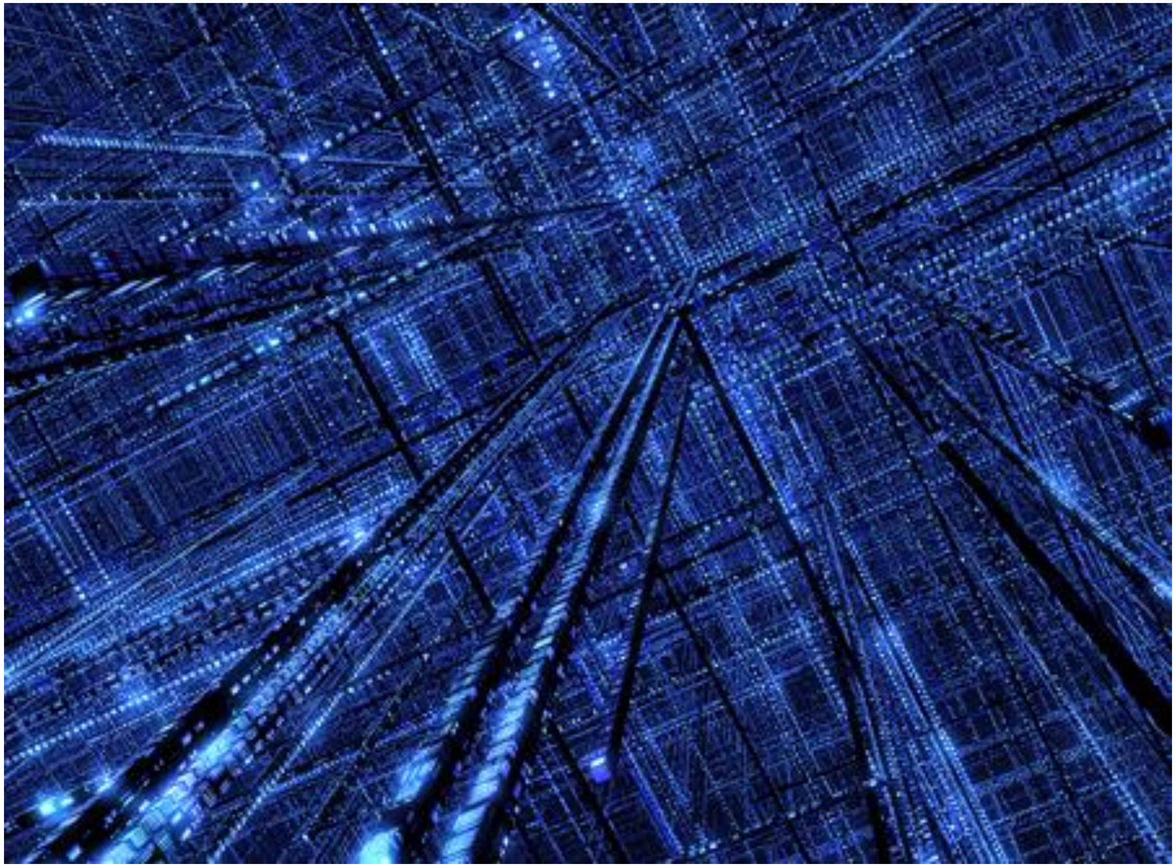
eset McAfee PANDA
KASPERSKY ANTI-VIRUS AVIRA
bitdefender secure your every bit
AVG TREND MICRO

Centre for Cyber Security Sciences

BLETCHLEY PARK
National Codes Centre

Legacy of Alan Turing

Alan Turing set the foundations for the World-Wide Web and how we can make it secure



Thank you!

Centre for Cyber Security Sciences

BLETCHLEY PARK
National Codes Centre