MENSCH UND MASCHINE TEIL I: VORTRAG

Der Krieg der Code-Brecher

DER EINBRUCH DER BRITEN UND AMERIKANER IN DAS MIT DER CHIFFRIER-MASCHINE ENIGMA GESICHERTE FUNKNETZ DER DEUTSCHEN KRIEGSMARINE IM 2. WELTKRIEG

BLETCHELEY PARK TRUST

Ein versteckter Landsitz zwischen London und Birmingham – Bletcheley Park, das Hauptquartier der britischen Dechiffrier-Spezialisten

VON RALPH ERSKINE

ENIGMA war der Markenname der von Arthur Scherbius 1918 erfundenen, von der Reichswehr und der Wehrmacht verwendeten Chiffriermaschine. Die baldmöglichste Bloßlegung des Chiffrierverfahrens der ENIGMA nach Beginn des Zweiten Weltkriegs, die unter dem höchst geheimen Decknamen „Ultra“ lief, war zweifelsohne für die Briten von entscheidender Wichtigkeit. Während dies dank Vorarbeiten polnischer Kryptologen für den Funkverkehr von Heer und Luftwaffe sehr rasch gelang, bot die Marine-ENIGMA größere Schwierigkeiten. Dass auch hier der Einbruch schließlich möglich war, rettete Großbritannien vor der Niederlage im U-Boot-Krieg und hat nach Harry Hinsley, dem offiziellen Historiker der britischen Geheimdienste, dazu beigetragen, den Zweiten Weltkrieg um etwa drei Jahre zu verkürzen.

Die 3-Rotor-ENIGMA M3 der deutschen Kriegsmarine funktionierte nicht anders als die von Heer und Luftwaffe verwendete, mit fünf auswechselbaren Rotoren ausgestattete, verfügte jedoch über drei zusätzliche Rotoren. Da jeweils drei der Rotoren in beliebiger Reihenfolge verwendet werden konnten, ergaben sich 8x7x6 = 336 Rotorlagen für die Marine-ENIGMA gegenüber 5x4x3 = 60 für die ENIGMAs der anderen Wehrmachtsteile. Nicht nur waren drei Rotor-Verschaltungen mehr aufzudecken, beim reinen Durchprobieren aller möglichen Rotorlagen ergab sich laufend ein mehr als fünffacher Aufwand. Überdies war das von der Kriegsmarine für die Deckung der Schlüssel-Vereinbarung verwendete Verfahren wesentlich sicherer als das von Heer und Luftwaffe benutzte.

Die drei Rotoren wurden zählerartig fortbewegt. Dies ergab eine polyalphabetische Chiffrierung mit der Periodenlänge16900. Eine Besonderheit, die nach einem Patent von Willi Korn schon die kommerzielle ENIGMA C von 1923 aufwies, war der Umstand, dass Chiffrieren und Dechiffrieren

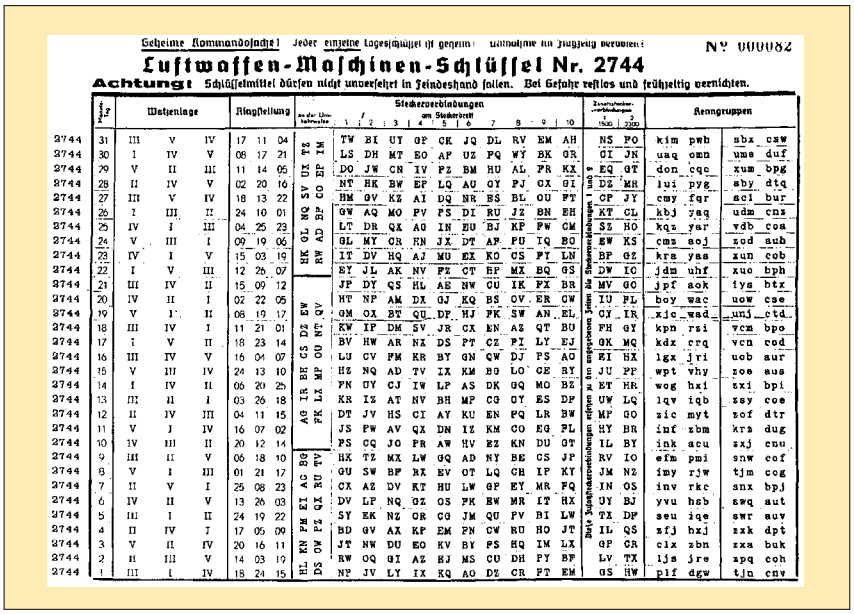
ohne Umstellung erfolgen konnte: Ging etwa bei irgendeiner Stellung der Rotoren der Buchstabe F in den Buchstaben P über, so ging bei der gleichen Stellung auch der Buchstabe P in den Buchstaben F über. Das war betrieblich sehr bequem, machte aber, wie sich zu spät herausstellte, die ENIGMA Chiffrierung angreifbar. Bewerkstelligt wurde diese Reziprozität durch eine Umkehrscheibe, die sich nach dem dritten Rotor befand und den Rückweg des Stromlaufs einleitete.

Während die Briten im Zentrum Bletchley Park bereits im Januar 1940 die ersten Funksprüche der Luftwaffe lesen konnten und schon im Frankreich-Feldzug die des Heeres, konnte das in Hut 8 arbeitende Team erst 1941 einige ENIGMA-chiffrierte Funksprüche der Kriegsmarine (für Februar und für April) lesen. Aber nur wenige dieser dechiffrierten Funksprüche waren zu dieser Zeit – wenn überhaupt – rechtzeitig verfügbar, um dem Operationszentrum der britischen Admiralität strategisch zu nützen.

Nicht nur der oben erwähnte größere Aufwand bedingte diese Verzögerungen, sondern auch weitere Vorsichtsmaßnahmen der Kriegsmarine: sie setzte zur Verkürzung der Funksprüche Codebücher mit Kurzsignalen ein, um Funkpeilungen ihrer Schiffe und stationären Sendestationen zu erschweren und verwendete auch sonst manuelle Codierung durch Codebücher. Die am häufigsten verwendeten waren das Kurzsignalheft für taktische Berichte wie etwa über gesichtete Geleitzüge und der Wetter-Kurzschlüssel für Wetterberichte. Die einschlägigen Codegruppen wurden mittels der ENIGMA vor der Übertragung überchiffriert.

Die ENIGMA-Chiffrierungen mussten variiert werden, schon zu Kriegsbeginn täglich: nicht nur durch einen Wechsel der Rotorlage, sondern auch der Anfangseinstellung (Grundstellung) jedes der drei Rotoren – jeweils durch einen der 26 Buchstaben des Alphabets gekennzeichnet. Das ergab für die Marine ENIGMA 336x26x26x26 = 5 905 536 Varianten der Chiffrierung – eine große Anzahl, die naive Betrachter leicht in Sicherheit wiegen konnte. Darüber hinaus konnten durch Steckerschnüre feste Auswechslungen der Buchstaben vorgenommen werden, wofür es etwa bei Verwendung von 10 Doppelschnüren 1.51×10^{14}, also über Hundert Billionen verschiedene Möglichkeiten dieser sogenannten Steckerverbindung gibt – was auf den ersten Blick an unendlich viele grenzt. Die Wahl dieser Möglichkeiten war durch Chiffrierunterlagen geregelt, die Grundstellung war Gegenstand der Schlüssel-Vereinbarung für den jeweiligen Spruch. Und jedes Funknetz hatte eigene Chiffrierungen. Das wichtigste Funknetz der Kriegsmarine, Heimische Gewässer genannt, war für Überwasserschiffe und U-Boote in der Ostsee und Nordsee einschließlich des Atlantik bestimmt; in Bletchley Park hatte es den Decknamen „dolphin“. Wenigstens 20 verschiedene Funknetze wurden im weiteren Verlauf des Krieges eingeführt.

Die meisten ENIGMA-Chiffrierungen hatten neben der Variante Allgemein eine Variante, Offizier genannt, bei der eine erste Chiffrierung des Klartextes (oder Codetextes) der Nachricht durch einen Offizier vorgenommen werden musste, mit einer für jeden Monat festgelegten Steckerverbindung. Eine Überchiffrierung erfolgte dann mit der Variante Allgemein. Für besonders schutzwürdige Nachrichten gab es in einigen



Geheime Kommandosache! Jeder einzelne Tagesschlüssel ist geheim! Kenntnisnahme durch Unbefugte verboten!

N° 000082

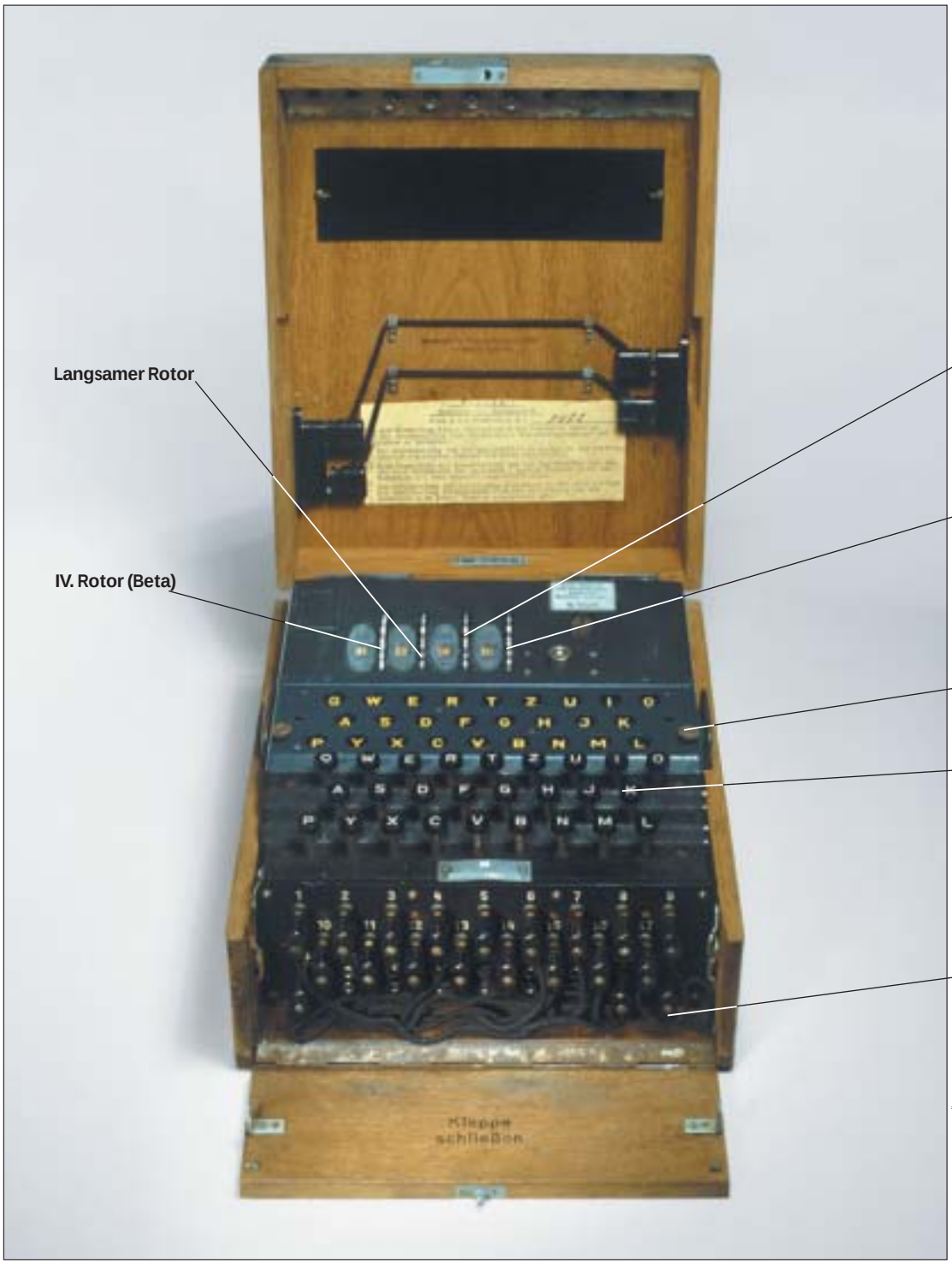
Luftwaffen-Maschinen-Schlüssel Nr. 2744

Achtung! Schlüsselmittel dürfen nicht unversehrt in Feindeshand fallen. Bei Gefahr restlos und frühzeitig vernichten.

Tag	Walzenlage			Ringstellung			Steckerverbindungen am Steckerbrett										Kenngruppen			
2744	31	III	V	IV	17	11	04	TZ	IM	TW	BI	UY	GP	CK	JQ	DL	RV	EM	AH	NS	FO	kim	pwb	sbx	csw
2744	30	I	IV	V	08	17	21			LS	DH	MT	EO	AF	UZ	FQ	WY	BK	GR	GI	JN	uaq	omn	ume	duf
2744	29	V	II	III	11	14	05	UX	EP	DO	JW	CN	IV	PZ	BM	HU	AL	FR	KX	EQ	GT	don	cqc	xum	bpg
28	II	IV	V	02	20	16	SV	CO	NT	HK	BW	EP	LQ	AU	OY	PJ	OX	GI	DZ	MR	lui	pyg	aby	dtq
2744	27	III	V	IV	18	13	22			HM	GV	KZ	AI	DQ	NR	BS	BL	OU	FT	CP	JY	cmy	fqr	aci	bur
26	I	III	II	24	10	01	NQ	BP	GW	AQ	MO	PV	FS	DI	RU	JZ	BN	EH	KT	CL	kbj	yaq	udm	cnz
2744	25	IV	I	III	04	25	23	GL	AD	LT	DR	QX	AG	IN	EU	BJ	KP	FW	GM	SZ	HO	kqz	yar	vdb	coa
24	V	III	I	09	19	06				GL	MY	OR	RN	JX	DT	AP	PU	IQ	BO	EW	KS	cmz	aoj	xod	aub
2744	23	IV	I	V	15	03	19	HK	RW	IT	DV	HQ	AJ	MU	EX	KO	CS	FT	LN	BP	GZ	krs	yaa	xun	cob
2744	22	I	V	III	12	26	07			EY	JL	AK	NV	FX	QT	BF	MX	BQ	GS	DW	IO	jdm	uhf	xuo	bph
2744	21	III	IV	II	15	09	12			JP	DY	QS	HL	AE	NW	CU	IK	FX	BR	MV	GO	jpf	aok	iys	btx
2744	20	IV	II	I	02	22	05			HT	NP	AM	DX	GJ	KQ	BS	OV	ER	GW	IU	FL	boy	wac	uow	cse
2744	19	V	I	II	06	19	17	EW	QV	GM	OX	BT	QU	DF	HJ	PK	SW	AN	EL	GI	IR	xie	wad	uni	ctd
2744	18	III	IV	I	11	21	01	DZ	NT	KW	IP	DM	SV	JR	CX	KN	AZ	QT	BU	PH	GY	kpn	rsi	vcm	bpo
2744	17	I	V	II	18	23	14	CS	OU	BV	HW	AR	NX	DS	PT	CZ	FI	LY	EJ	OK	MQ	kdz	crq	vcn	cod
2744	16	III	IV	V	16	04	07	BH	MP	LU	GV	FM	KR	BY	GN	QW	DJ	PS	AO	EI	HX	lgx	jri	ueb	aur
2744	15	V	III	IV	24	13	10			HZ	NQ	AD	TV	IX	KM	BO	LO	GS	BT	JU	PF	wpt	vhy	zoe	aus
2744	14	I	IV	II	06	20	25			FN	UY	CJ	IW	LP	AS	DK	GQ	MO	BZ	ET	HR	wog	hxi	zxi	bpi
2744	13	III	II	I	03	26	18	AG	LX	KR	IZ	AT	NV	BH	MF	CG	OY	ES	DP	UW	LQ	iqv	iqb	zsy	coe
2744	12	II	IV	III	04	11	15	IR	PK	DT	JV	HS	CI	AY	KU	EN	PQ	LR	BW	MF	GO	zic	myt	zof	dtr
2744	11	V	I	IV	16	07	02			JS	FW	AV	QX	DN	IZ	KM	CO	EQ	PL	HY	BR	inf	xbm	krs	dug
2744	10	IV	III	II	20	12	14			FS	CQ	JO	PR	AW	HV	EZ	KN	DU	GT	IL	BY	ink	acu	zxj	cnu
2744	9	III	II	V	06	18	10	BG	RV	HK	TZ	MX	LW	GQ	AD	NY	BE	CS	JP	KV	IO	efm	pmi	snw	cof
2744	8	V	I	III	01	21	17			GU	SW	BF	RX	EV	OT	LQ	CH	IP	KY	JM	NZ	imy	rjw	tjm	cog
2744	7	II	V	I	25	08	23	AC	BU	CX	AZ	DV	KT	HU	LW	GP	EY	MR	FQ	IN	OS	inv	rkc	snx	bpj
2744	6	IV	II	V	13	26	03	EI	QX	DV	LF	NQ	GZ	OS	PK	EW	MR	IT	HX	UY	BJ	yvu	hsb	zwq	aut
2744	5	III	I	II	24	19	22	PM	PZ	SY	EK	NZ	OR	CG	JM	QU	PV	BI	LW	TX	DP	seu	iqe	swr	auv
2744	4	II	IV	I	17	05	09	KN	OW	BD	GV	AX	KP	EM	PN	CW	RU	HO	JT	IL	QS	xfj	hxj	zxk	dpt
2744	3	V	II	IV	20	16	11			JT	NW	DU	EO	KV	BY	PS	HQ	IM	LX	GP	CR	clx	zbn	zxa	buk
2744	2	II	III	V	14	03	19	HL	DS	RW	OQ	GI	AZ	EJ	MS	CU	DH	PY	BP	LV	TX	ljs	jre	zpq	coh
2744	1	III	I	IV	18	24	15			NP	JV	LY	IX	KQ	AO	DZ	CR	FT	EM	GS	HW	plf	dgw	tjn	cnv

F.L. BAUER

Auszug aus einem Kurzsignalheft der Luftwaffe – links ist die Rotorlage („Walzenlage“) des Tages angegeben, in der Mitte die jeweilige Steckerverbindung



DEUTSCHES MUSEUM MÜNCHEN

4-Rotor-ENIGMA der Marine (1944): Die M4 war weitgehend baugleich mit der 3-Rotor-Ausführung (M3), denn der zusätzliche Rotor (Beta) ersetzte lediglich die Umkehrscheibe B der M3. Das heißt, der IV. Rotor konnte aufgrund der Konstruktion der ENIGMA nicht fortbewegt werden – im Gegensatz zu den anderen Rotoren. Zusätzliche Kombinationsmöglichkeiten wurden so verschenkt – auch die M4 blieb „angreifbar".

Funknetzen eine weitere Variante Stab, die zusätzliche Schikanen bot. Obwohl Bletchley Park häufig mit den chiffrierten Nachrichten in der Offizier-Variante fertig wurde, manchmal allerdings erst nach Wochen, wurde die Stab-Variante nur ein einziges Mal gebrochen.

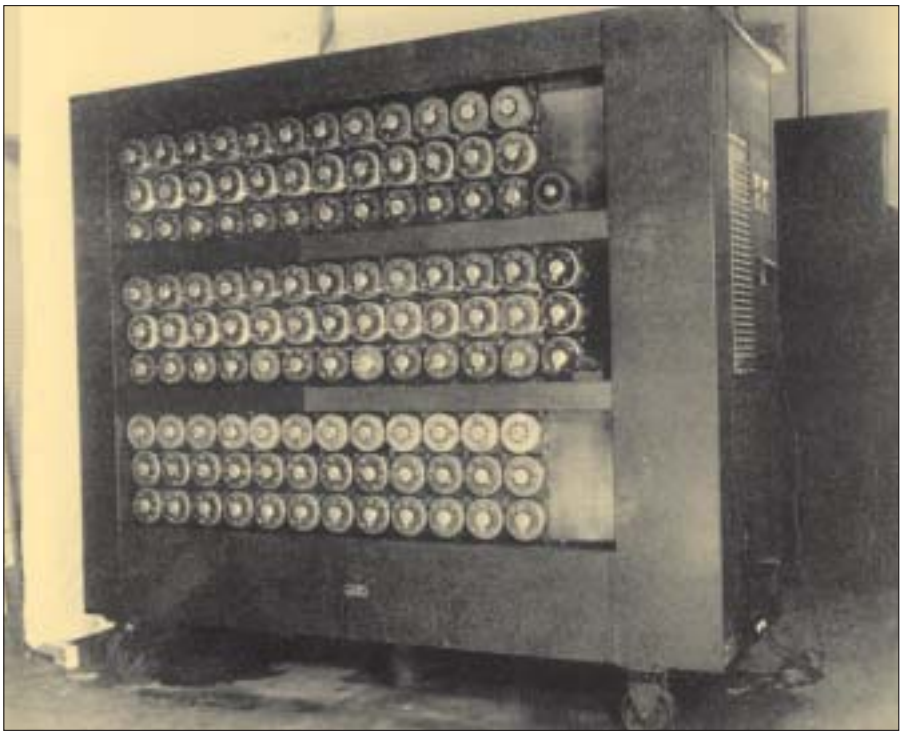
Bletchley Park erhielt im August 1939 einen ENIGMA-Nachbau und die Verschaltung der von Heer und Luftwaffe verwendeten Rotoren I bis V von den Polen. Marian Rejewski, der polnische Kryptanalytiker, hatte schon im Dezember 1932 die Verkabelung der bis dahin benützten ENIGMA-Rotoren I bis III mathematisch rekonstruiert. Die Briten erbeuteten die Rotoren VI und VII von der Besatzung des U-33 am 12. Februar 1940 und den Rotor VIII im August 1940. Hut 8 hatte nun alle acht Rotoren, konnte aber nur selten den ENIGMA-Marine-Code brechen.

Mai/Juni 1940 gelang es Hut 8, den ENIGMA-Funkverkehr der Marine von sechs Tagen im April zu dechiffrieren, nachdem sie aus einem zusammengehörigen Paar von Klartext und chiffriertem Text, die in dem Patrouillen-Schiff VP 26 erbeutet worden waren, hinreichend Einblick in das Chiffrierverfahren gewonnen hatten. Sie verwendeten bei dieser Dechiffrierung bereits die erste BOMBE, eine Hochgeschwindigkeitsmaschine mit einer komplizierten Suchschaltung zur Feststellung der relativen Lage der durch die drei Rotoren bestimmten polyalphabetischen Chiffrierschritte, wobei entscheidend war, dass die Suche von der Kenntnis der Billionen Steckerverbindungen völlig unabhängig war.

Diese BOMBE – das Geistesprodukt des mathematischen Genies Alan Turing, genannt „der Prof" – war noch nicht so leistungsfähig wie die von Gordon Welchman bald darauf erfundene BOMBE mit „diagonal board", welch letzteres die durch die Umkehrscheibe bewirkte Reziprozität – eine grundlegende innere Gesetzmäßigkeit der ENIGMA-Chiffrierung – geschickt ausnützte und damit „feinfühliger" war. Eine solche BOMBE war im August 1940 verfügbar. Sie leistete beim Aufbrechen von ENIGMA-chiffrierten Nachrichten des Heeres und der Luftwaffe ganze Arbeit.

Hut 8 sah sich vor drei Probleme gestellt bei dem Versuch, auch die ENIGMA-chiffrierten Nachrichten der Kriegsmarine zu brechen, sogar nachdem die nach Welchman verbesserten BOMBEN in Betrieb genommen worden waren:

1. Das System, das die Spruchschlüssel-Vereinbarung (die Grundstellung der Rotoren für die Übermittlung eines be-



BLETCHELEY PARK TRUST

Eine sogenannte BOMBE: Vorne sichtbar sind die Rotoren (analog zu denen der ENIGMA), im Inneren ist eine komplizierte Suchschaltung zur Feststellung der verwendeten Rotorlage und Anfangseinstellung. Sobald diese gefunden waren, konnte das Dechiffrieren auf einem ENIGMA-Nachbau beginnen.

stimmten Funkspruchs betreffend) angab, war „idiotensicher“ dadurch, dass es ein Buch-System war, d.h. welche Grundstellung verwendet wurde, hing nicht von der alleinigen Entscheidung des Funkers ab.

2. Die Durchmusterung mit der BOMBE aller 336 möglichen Rotorlagen dauerte mehr als fünfmal länger bei der ENIGMA der Kriegsmarine als bei den ENIGMA-Maschinen von Heer und Luftwaffe. Außerdem war nur eine BOMBE ausschließlich für die Dechiffrierung der Marine-ENIGMA verfügbar.
3. „cribs“, d.h. wahrscheinliche Floskeln und Bruchstücke, die die Suchschaltung der BOMBE steuerten, waren noch so gut wie überhaupt nicht verfügbar.

Hut 8 konnte den Verkehr im Funknetz Heimische Gewässer bis zum Juni/Juli 1941 nicht ohne beträchtliche Verzögerungen aufdecken. Dabei benutzte man Chiffrierunterlagen und cribs, die in eigens geplanten Überfällen auf die Wetterschiffe München und Lauenburg erbeutet wurden. Das so erworbene Wissen versetzte das Operationszentrum der britischen Admiralität schließlich in die Lage, mehrere Geleitzüge von Schiffen so umzuleiten, dass sie den wenigen (etwa 20) U-Booten im Nordatlantik entkommen konnten. Die neue Festlegung der Route dank Ultra rettete viele Leben und mehrere tausend Bruttoregistertonnen lebenswichtigen Schiffsbestands – auch wenn es unwahrscheinlich ist, dass es sich um 1,5 bis 2 Millionen Tonnen handelte, wie das manchmal für die zweite Hälfte des Jahres 1941 behauptet wird.

Die Entzifferungen der Monate Juni und Juli 1941 gaben Hut 8 genug Einblick in den Funkverkehr, um das Funknetz Heimische Gewässer ab August 1941 kryptoanalytisch vollständig zu knacken. Hilfreich dabei war, dass die Rotorlage nur jeden zweiten Tag gewechselt wurde. Am zweiten Tag genügte ein BOMBEN-Lauf von weniger als siebzehn Minuten, um auf der Basis der bereits festgestellten Rotorlage des ersten Tages die Einstellungen des zweiten Tages zu finden – falls eine crib, von der sich die Versuchsschaltung der BOMBE ableiten ließ, vorhanden war. Das halbierte die Arbeit von Bletchley Park an den Marine-Funksprüchen und sparte Bletcheley Park wertvolle BOMBEN-Zeit. Die Erbeutung eines Kenngruppenbuchs vom U-Boot 110 am 9. Mai 1940 half auch bei der Entwicklung einer Methode (im Jargon genannt Banburismus), mit der herausgefunden werden konnte, welcher Rotor als „schneller“ Rotor der Maschine, d.h. in der Position ganz rechts, eingesetzt wurde. Dies reduzierte die Anzahl der erforderlichen BOMBEN-Läufe beträchtlich. Ohne cribs oder Banburismus waren die BOMBEN praktisch unnütz gegen dolphin.

Obwohl die Kriegsmarine die ENIGMA in vielerlei Hinsicht sorgfältiger benutzte als andere Dienste, waren einige Einheiten nicht mit der ENIGMA ausgerüstet. Einige Nachrichten wurden also sowohl mit manuellen Systemen chiffriert wie mit der ENIGMA. Dechiffrierungen der handchiffrierten Funksprüche lieferten cribs, wenn die selben Funksprüche auch mit der ENIGMA chiffriert wurden. Manchmal führte die Royal Air Force Minenlege-Operationen durch (im Jargon „Gartenarbeit“ genannt), um Hut 8 so cribs zu beschaffen. Die Kriegsmarine musste Funksprüche senden, sobald die Seewege nach der Minenentschärfung wieder schiffbar waren. Die Funksprüche über die geräumten Kanäle wurden sowohl mit der ENIGMA der Marine chiffriert gesendet wie auch nach einer manuellen Chiffrierung (bekannt als „Werftschlüssel“). Als Bletchley Park den Werftschlüssel aufbrach, hatte Hut 8 den Klartext, sobald es einen identischen ENIGMA-Funkspruch gab. Ohne die Hilfe der Abteilung Hut 4 von Bletchley Park, die den Werftschlüssel dechiffrierte, hätte man wesentlich weniger Informationen über das Funknetz Heimische Gewässer bekommen. Manuelle Chiffren, die von Bletchley Parks Wetter-Abteilung Hut 10 gebrochen wurden, waren die zweite ergiebige Quelle für cribs. Kurz-Wettermeldungen wurden von U-Booten im Atlantik gesendet, was einen wesentlichen Teil der deutschen Kriegsanstrengungen darstellte. Ab Februar 1941 knackte Hut 10 den Wetterkurzschlüssel, den die U-Boote der Kriegsmarine verwendeten. Anfang Mai 1941 erhielt Bletchley Park eine Kopie des Wetterkurzschlüssel-Buches des Wetterschiffs München in der Ausgabe von 1940. Hut 8 konnte jetzt den exakten Text der chiffrierten U-Boot-Wettermeldungen rekonstruieren – und verfügte so über eine zweite Quelle für cribs.

Bletchley Park erlitt einen schweren Rückschlag am 1. Februar 1942, als eine neue, mit einem vierten Rotor versehene ENIGMA-Maschine M4 der Kriegsmarine mit dem Funknetz „Triton“ in Betrieb ging. Bletchley Park gab

DEUTSCHES MUSEUM MÜNCHEN

Die Rotoren der ENIGMA konnten herausgenommen und ausgetauscht werden

dieser Spezial-Chiffrierung für U-Boote in Atlantik und Mittelmeer den Decknamen „shark“. Obwohl Bletchley Park die Verdrahtung des neuen Rotors in M4 im Dezember 1941 herausfand, erwies sich die Kombination der Einführung eines zusätzlichen Rotors, eines eigenen Funknetzes shark und einer zweiten Auflage des Wetterkurzschlüssels als verheerend.
Nachdem man Bletchley Park seiner cribs beraubt hatte, waren die Briten blind gegen shark, und das in einer kritischen Phase des U-Boot-Krieges.

M4 war allerdings keine echte 4-Rotor-Maschine. Der vierte Rotor, mit Beta bezeichnet, war die rechte Hälfte der aufgespaltenen Umkehrscheibe B und war nicht mit den Rotoren I bis VIII austauschbar. Beta und eine restliche Umkehrscheibe B dünn ersetzten die frühere Umkehrscheibe B. Beta konnte nach Maßgabe der Chiffrierunterlagen in 26 Stellungen fest eingestellt werden, was M4 das Äquivalent von 26 verschiedenen Umkehrscheiben gab, aber die M4-Rotoren konnten immer noch auf nur 336 (8 x 7 x 6) verschiedene Arten kombiniert werden und nicht auf 3024 (9 x 8 x 7 x 6). Aber ohne cribs für den neuen Wetterkurzschlüssel zu besitzen, konnte Hut 8 das Funknetz shark nicht angreifen.

Bei einer gewissen „neutralen“ Stellung des Beta-Rotors war M4 jedoch komplett kompatibel mit M3. Am 30. Oktober 1942 wurde schließlich die zweite Auflage des Wetterkurzschlüssels aus dem U-Boot U 559 geschnappt, bevor es bei Port Said sank. Nach mehreren hundert BOMBEN-Läufen fand Hut 8 heraus, dass der Beta-Rotor bei der Verschlüsselung von Wetterberichten in „neutraler“ Stellung war: M4 wurde nur im M3-Modus benutzt. Ein 3-Rotor-BOMBEN-Lauf mit, sagen wir, 60 Rotorlagen würde folglich nur 17 Stunden brauchen statt der um den Faktor 26 größeren Zeit von 442 Stunden (mehr als 18 Tagen), die erforderlich gewesen wären, hätte man das Potenzial der M4 voll ausgeschöpft.

Am 13. Dezember 1942 schickte Bletchley Park ein Fernschreiben an das Operationszentrum der britischen Admiralität, in dem die Positionen von mehr als 12 U-Booten im Atlantik dargelegt wurden. Die Positionsbestimmung gründete auf den im Funknetz shark chiffrierten Wetter-Funksprüchen. Hut 8 war mit Hilfe der Wetter-Funksprüche, die Hut 10 geknackt hatte, endlich in das Funknetz shark der M4 eingedrungen. Die sich daraus ergebende Information über die Absichten des Befehlshabers der U-Boote hat, auch wenn sie manchmal schrecklich spät kam, ohne Zweifel eine entscheidende Rolle in der Schlacht auf dem Atlantik gespielt und vielleicht weit mehr als 100.000 Bruttoregistertonnen Schiffskapazität allein im Dezember 1942 und im Januar 1943 gerettet. Die Nutzung der Wetterkurzschlüssel gegen das „Triton“-Funknetz sollte nur von kurzer Dauer sein. Eine dritte Auflage des Wetterkurzschlüssel-Buches trat am 10. März 1943 in Kraft – wodurch Bletchley Park wieder seiner cribs beraubt wurde. Bletchley Park hatte befürchtet, durch diese Änderung für mehrere Monate blind zu werden. Aber Hut 8 verwendete die Kurzsignal-Sichtungsberichte als cribs (U-Boote, die in Kontakt mit Geleitschiffen standen erstellten diese Berichte,

die mit dem Kurzsignalheft chiffriert wurden) und drang am 19. März 1943 wieder in shark ein. Vor dem 30. Juni gelang es Hut 8, an 90 der folgenden 112 Tage die Chiffrierung zu knacken. Die Kurzsignal-Sichtungsberichte verwendeten ebenfalls die M4-ENIGMA im M3-Modus – und das U-Boot 559 hatte eine Kopie des Kurzsignalheftes eingebracht.

In den Vereinigten Staaten ging man nun ebenfalls zur Offensive im U-Boot Krieg über. 4-Rotor-BOMBEN der britischen und amerikanischen Marine gingen jeweils im Juni und im August 1943 in Betrieb, aber die Ermittlung einiger Juli- und August-Chiffrierunterlagen dauerte bis zu 26 Tagen, nachdem ein neuer Rotor (Gamma) bei der M4 eingeführt worden war. Wie auch immer, ab September 1943 konnte shark im allgemeinen innerhalb von 24 Stunden gelesen werden, auch wenn es selten leicht war. Ende 1943 wurde die Arbeit an shark in die Codebrecher-Abteilung Op-20-G der US-amerikanischen Kriegsmarine in Washington verlegt, denn die US-Marine besaß inzwischen hinreichend viele BOMBEN (50 bis Mitte November in Betrieb und 30 weitere im Bau) und sie waren weitaus verlässlicher als die britischen 4-Rotor-BOMBEN.

Hugh Alexander, ein Mathematiker und Schachgroßmeister, der Turing als Chef der Hut 8 Ende 1942 nachfolgte, war ein brillanter Organisator und eine herausragende Führungspersönlichkeit. Die Dechiffrierungen der Marine-ENIGMA wurden ins Englische übersetzt von den Leuten in Hut 4, die ihren vollen Text dann als Fernschreiben an das Operationszentrum der britischen Admiralität nach London schickten. Die Hauptaufgabe der mittels der Marine-ENIGMA gewonnenen Ultra-Informationen war defensiv, wie z.B. die Umleitung von Geleitschiffen. Aber sie hatte auch viele andere Verwendungszwecke: Sie führte zur Versenkung von acht Versorgungsschiffen Mitte 1941, des Zerstörers Atlantis im Dezember 1941 und des Schlachtschiffes Scharnhorst im Dezember 1943. Und die US-Navy benutzte Ultra-Informationen ab 1943 offensiv (obschon risikoreich) bei den vielen Versenkungen der wichtigen U-Tanker.

Aber ohne den Wagemut von Leutnant Anthony Fasson, des Vollmatrosen Colin Grazier und des 16-Jährigen Tommy Brown, der den Wetterkurzschlüssel und das Kurzsignalheft aus dem U-Boot 559 herausfischte, wäre shark viele Monate lang nicht gebrochen worden. (Fasson und Grazier wurde das George Cross posthum verliehen und Tommy Brown, der überlebte, erhielt die George Medal). Die Alliierten hätten nicht vor der zweiten Hälfte des Jahres 1943 die Vorherrschaft der Marine im Atlantik begründen können und die Invasion in der Normandie wäre vermutlich bis 1945 verschoben worden. Nur wenige mutige Handlungen von drei Individuen können jemals so weitreichende Konsequenzen haben. Ohne die aus shark gewonnenen Ultra-Informationen über die U-Boote in Atlantik und Mittelmeer wären diese am Ende immer noch besiegt worden, aber der Verlust von Menschenleben in diesem globalen Konflikt wäre sogar noch schrecklicher gewesen als er es ohnehin war.

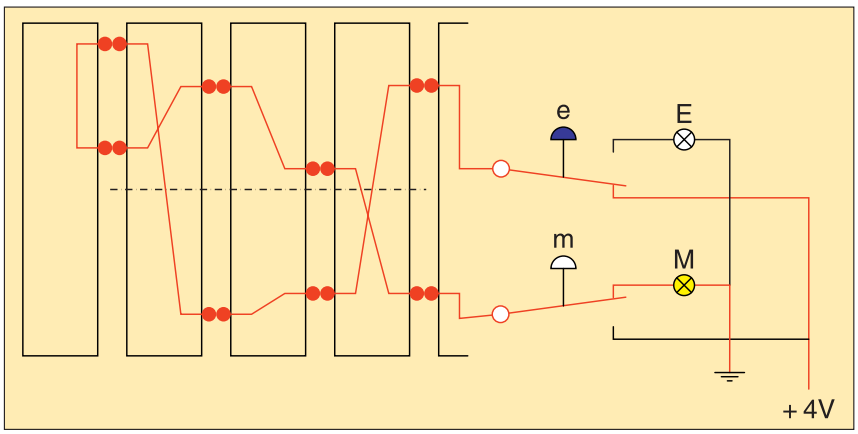
Übersetzung: Julia Müller
Überarbeitung und Ergänzung: Friedrich L. Bauer

Weiterführende Lektüre:

Friedrich L. Bauer: Entzifferte Geheimnisse – Methoden und Maximen der Kryptologie; 3. überarb. und erw. Auflage, Springer Verlag, Berlin 2000, XIV+503 S., 166 Abb., 26 Tabellen, 16 Farbtafeln, geb. 34,95 EUR ; ISBN 3 540 679316

Michael Smith, Ralph Erskine: Action This Day; Bantam Press, 2001, 560 S., geb. ca. EUR 39,– ; ISBN 0 593 04910 1

www. bletcheleypark.org.uk



Der Stromkreislauf in der ENIGMA: Die elektrisch oder mit Batterie betriebene Maschine „ersetzt“ hier den Buchstaben „m“ (Eingabe über die Tastatur) durch den Buchstaben „e“ (Ausgabe durch Lampenanzeige). Diese Substitution funktioniert analog in der Gegenrichtung („e“ zu „m“) – ein Schwachpunkt der Chiffrierung.