Eingangstor zu den Stallungen in Bletchley Park. Das Haus durchs Tor gesehen ist die >Cottage<.

Obwohl die Briten den >Enigma<-Schlüssel noch brechen mußten, enthüllte eine einfache Funkverkehrsanalyse, die Welchman mit Hilfe der geheimen >Y<-Horchstelle der Marine vornahm, den riesigen Umfang und die ineinandergreifende Vielfalt der Nachrichtenorganisation der deutschen Wehrmacht. Sie besaß 1939 das mit Abstand perfekteste und umfangreichste militärische Fernmeldenetz der Welt. Ohne ein schnelles, leicht bedienbares und sicheres Schlüsselsystem konnte es keinen Funk geben und ohne Funk auch keinen >Blitzkrieg<. So einfach war das. (Die einzige Alternative zu >Enigma<, die völlige Sicherheit bot, dürfte die Wegwerfchiffriertafel zum einmaligen Gebrauch gewesen sein. Abgesehen davon, daß sie viel mehr Zeit zum Ver- und Entschlüsseln erforderte, hat man errechnet, daß alle Druckerpressen in Deutschland, selbst wenn sie Tag und Nacht nichts anderes als diese Art Chiffriertafeln gedruckt hätten, nicht in der Lage gewesen wären, die Bedürfnisse der deutschen Wehrmacht zu decken, weil der Anfall an verschlüsselten Funksprüchen derart umfangreich war.)

>Enigma< war die Lösung. Als Welchman die Funksprüche deutscher Truppenverbände auswertete und anhand ihrer Kenngruppen daraus deren Bewegungen feststellte, begriff er, sofern erst einmal die ehernen Geheimnisse der Fünfergruppen, die den Inhalt der abgehörten Funkmeldungen bildeten, aufgedeckt werden konnten, daß eine gewaltige Organisation erforderlich war, die auch zahlenmäßig dem Hauptteil der deutschen Nachrichtentruppe entsprechen mußte, um mit der Unmasse von >Enigma<-Sprüchen fertig zu werden. Es war eine kryptologische Analyse in einem bisher noch ungeahnten Ausmaß.

Als Welchman diese Aufgabe überdachte, sah er plötzlich einen möglichen Ansatzpunkt, der zur Lösung der Schlüsselverfahren führen könnte.

> Ach rannte rüber zur >Cottage<, wo mein Chef Knox arbeitete, und meldete mich bei ihm, um dann nur zu hören, daß andere Leute sich schon vorher mit dem Problem befaßt hätten und tatsächlich die Rechengeräte schon entwickeln, mit deren Hilfe wir in der Lage wären, >Enigma< zu >knacken<.«

Weit davon entfernt, enttäuscht zu sein, daß seine Ideen schon von anderen vorweggenommen worden waren, wußte Welchman jetzt wenigstens, was getan wurde, weil er >Kenntnis< hatte. Ohne sein Gespräch mit Knox hätte es Monate dauern können, bevor man ihm die Möglichkeit eines bevorstehenden durchschlagenden Erfolges mitgeteilt hätte. Getreu der strengen Anwendung des Sicherheitsgrundsatzes: »Kenntnis nur wenn nötig!« Auf jeden Fall konnte er sich jetzt, aufgrund seiner Funkverkehrsanalysen, den Umfang der Aufgabenstellung, die Bletchley Park bevorstand, sehr gut vorstellen:

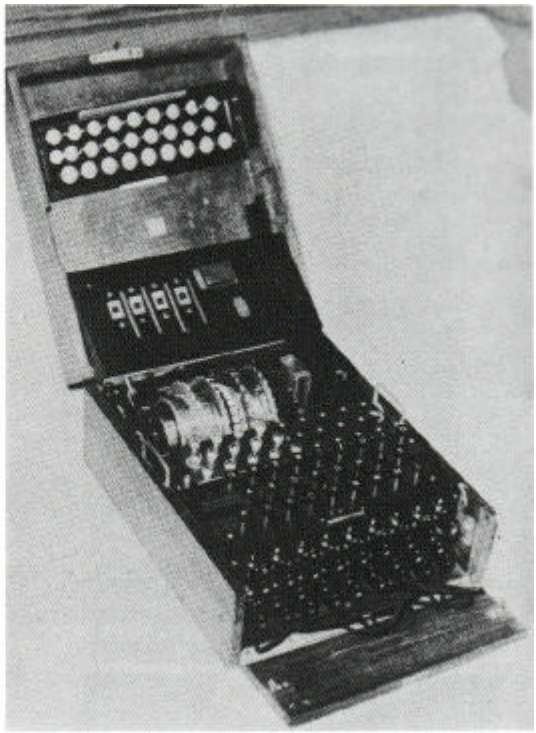
> »Ich dachte viel darüber nach, entwickelte einen Organisationsplan, legte ihn Travis vor, bekam ihn genehmigt und wurde ermächtigt, sofort mit der Anwerbung geeigneten Personals zu beginnen ...«

Es wurden viele Fachleute und Spezialisten benötigt: Funker, um die Abhörstationen zu besetzen; Mädel vom Frauenhilfskorps der Royal Navy (WRNS — Women's Royal Naval Service) als Entschlüsselungspersonal; Techniker, Statistiker, Mathematiker, Nachrichtendienstler, also eine umfangreiche Organisation, die schließlich 10 000 Leute, Männer und Frauen, umfaßte, die alle zu strengster Geheimhaltung verpflichtet wurden.
Binnen weniger Wochen stand die Organisation in ihren Grundzügen. Alles wartete auf den Augenblick, bis die >Schriftgelehrten, die Kryptologen, den Fünfwalzen->Enigma<-Schlüssel gebrochen hatten. Doch es war entmutigend. Die militärische >Enigma<, wie sie deutscherseits von Heer und Luftwaffe eingesetzt wurde, hatte 10^{21} mögliche Anfangseinstellungen. Für die Marine->Enigma<Schlüsselmaschine, die vier Chiffrierwalzen aus acht wählbaren einsetzte, ergab sich ein Wert von 10^{23}.
Selbst der Besitz einer >Enigma< bedeutete nur eine geringe Hilfe. Die Deutschen mußten die Möglichkeit, daß eine oder mehrere >Enigma<Maschinen erbeutet werden könnten, vorausgesehen haben. Der Versuch, alle mathematisch denkbaren Kombinationen der Maschinen zu errechnen, selbst unter Einsatz heutiger Computer, konnte bis zu fünfzig Jahre dauern. Kein Wunder, daß die Deutschen absolutes Vertrauen in die Sicherheit ihrer Geheimkodes setzten.

Und doch gelang es, sie zu brechen. Wichtigstes Hilfsmittel war dabei die >Bombe<. Dies war ein gefährlicher Deckname. Wenn der deutsche Geheimdienst ihn aufgeklärt hätte, müßte er daraus schließen, daß in Bletchley eine Atombombe in Entwicklung stehe, und Bletchley lag in Reichweite deutscher Kampfgeschwader. Abgesehen vom Namen >Bombe< gibt es keine Hinweise auf eine geistige Verwandtschaft der britischen Ausführung mit der polnischen >Bomba<.
Dr. I. J. Good, einer jener Mathematiker aus Bletchley, erklärte im Verlauf eines Vortrages >Pionierleistungen an Rechnern in Bletchley<, den er 1976 vor auserlesenem Publikum im >National Physical Laboratory< hielt, folgendes:

> »... es mußte also einige weitreichende sinnvolle Verbesserungen der britischen >Bombe< (im Vergleich zu der polnischen >Bombe) gegeben haben. Ich vermag das hier nicht näher zu erläutern. Ich kann nur sagen, daß Gordon Welchman einen der grundsätzlichen Gedanken gehabt hat und Turing einen weiteren. Meines Erachtens nach waren Turings Gedankengänge derart, daß in absehbarer Zeit niemand jemals darauf gekommen wäre. Er hat damit das Leistungsvermögen des Rechengerätes >Bombe< entscheidend verbessert ...«

Was diese beiden umwälzenden Ideen genau besehen beinhalteten, ist nicht bekannt: Turing ist tot, und Welchman ist noch an die amtliche Geheimhaltungs-

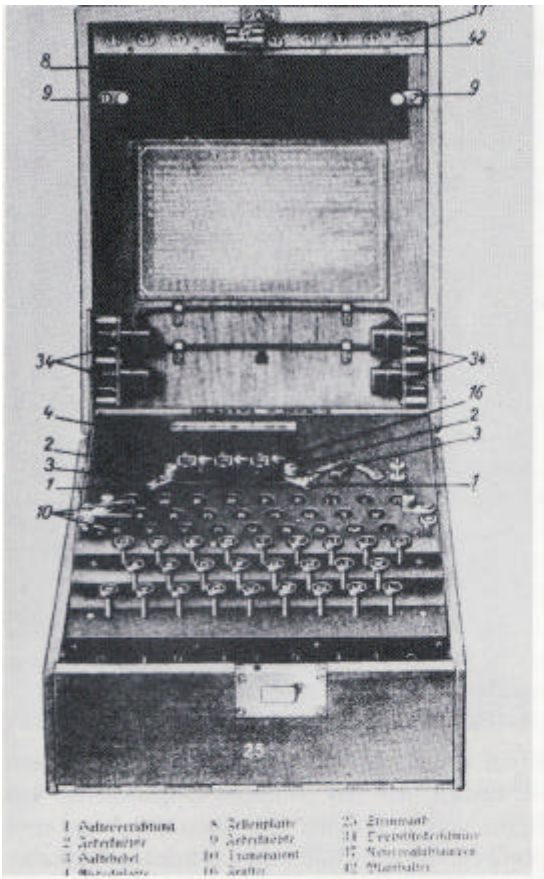


Links: Funk war für die Luftwaffe und U-Boote-Führung wichtig. Verschlüsselte >Enigma<-Sprüche wurden in Morsegruppen übermittelt.

Rechts: Vierwalzen->Enigma<, wie sie von der Marine für die >Triton<-Schlüssel benutzt wurden. Dieser Kode konnte von Bletchley Park erst 1943 nach intensivsten Entschlüsselungsbemühungen gebrochen werden.

verpflichtung gebunden, die er vor vielen Jahren unterschrieben hatte. Es kann jedoch durchaus angenommen werden, daß das polnische Originalgerät, und entsprechend die britischen Geräte, sehr groß waren. Dr. Good sprach von etwa drei Metern Höhe. Es waren gewiß die >Bronze-Göttinnen<, von denen Winterbotham in seinem Buch >The Ultra Secret< berichtet. Nach Recherchen bei Leuten, die sie gebaut und bedient hatten, gelang es, ein Modell der >Bombe< für die BBC-Fernsehsendungen nachzubauen, um eine allgemeine Vorstellung zu vermitteln. nach welchem Prinzip sie arbeitete. Sie wurde nicht elektronisch, sondern elektromechanisch betrieben. In gewisser Hinsicht waren die Bombe-Rechengerate in umgekehrter Richtung arbeitende Enigma-Geräte, aber weitaus umfangreicher. weil sie die drei Chiffrierwalzen mehrfach simulieren und durchlaufen lassen mußten. Sie hatten auch Steckerverbindungen, auf der ein sogenanntes >Menü< vorgewählt werden konnte. Dieses >Menü< war nichts anderes als ein Programm elektromagnetischer Voreingaben an die >Bombe<. wodurch die Anzahl der möglichen Anfangseinstellungen einer >Enigma<-Maschine von 10^{21} auf wesentlich kleinere, besser überschaubare Werte verringert werden konnte. Dieses >Menü<. das vorwählbare Programm, wurde in >Baracke 6< für Heer und Luftwaffe und in >Baracke 8< für die Marine aufgestellt. Die Krvptologen bezogen die Informationen hierfür aus abgehörten Funksprüchen. Entscheidende Hilfe erhielten sie von den Deutschen selbst. Ohne sie wären diese Aufgaben unlösbar geblieben.

Man muß sich vor Augen halten. daß in der deutschen Wehrmacht eine sehr große Zahl von >Eniema<-Schlüsselmaschinen im Einsatz waren. Man vermutet eine Zahl von etwa 200 000, die täglich gewaltige Mengen von Funksprüchen verschlüsselten. Das bedeutete, daß alle Meldungen immer wieder die gleichen



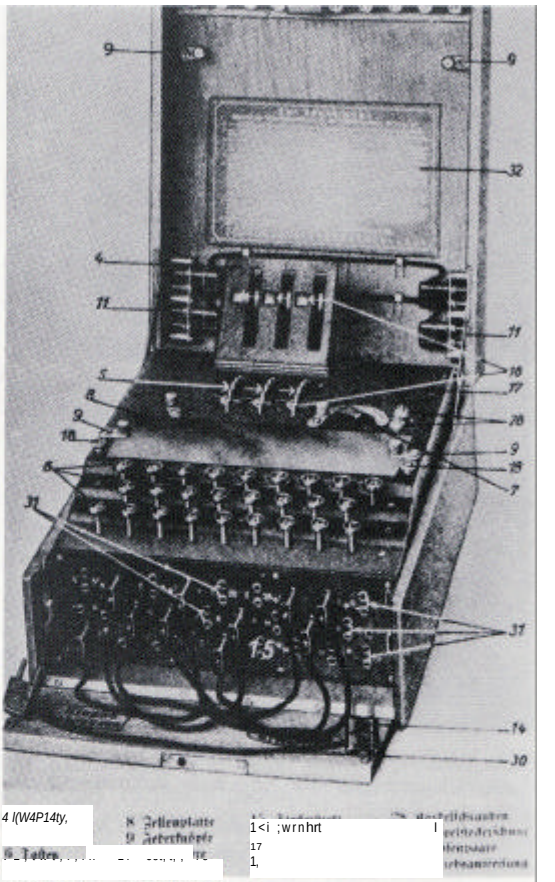
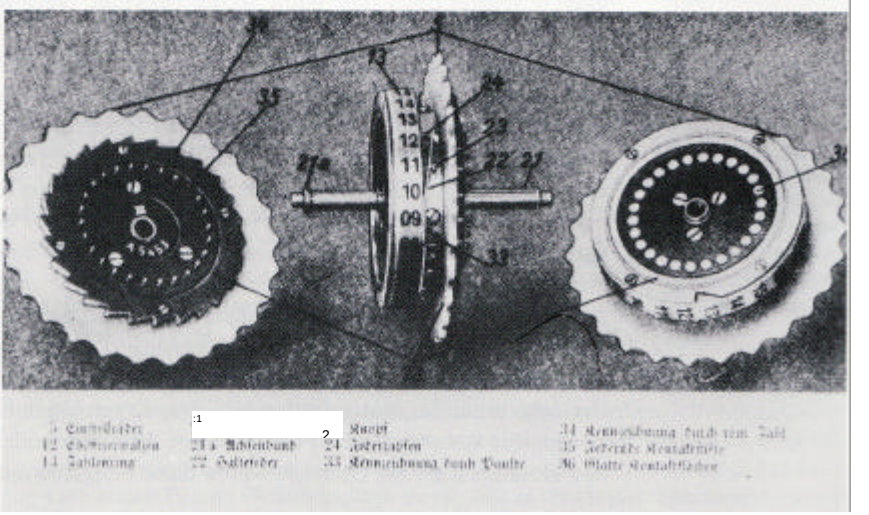


Abbildung einer >Enigma, aus einem deutschen Heereshandbuch. Diese spezielle Maschine verwendete 26 Ziffern auf den Walzen anstelle von

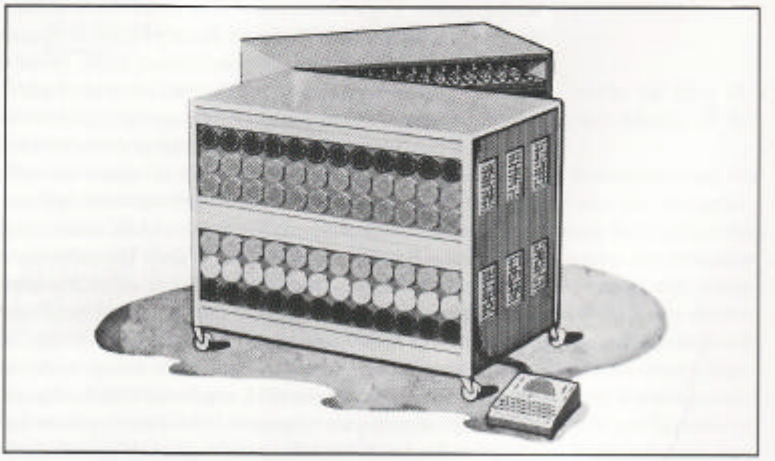


stereotypen Wortwendungen enthielten, wie >Betreff/Bezug<, >Kommandeurssache<, >Führerbefehl< bis hin zu Heil Hitler<. Derartige Wiederholungen sind Speise und Trank für den Kryptologen, er lebt davon und ist darauf angewiesen. Sobald nämlich eine dieser stereotypen Wortwendungen einmal dechiffriert war.

Bedeutung der Zahlen:

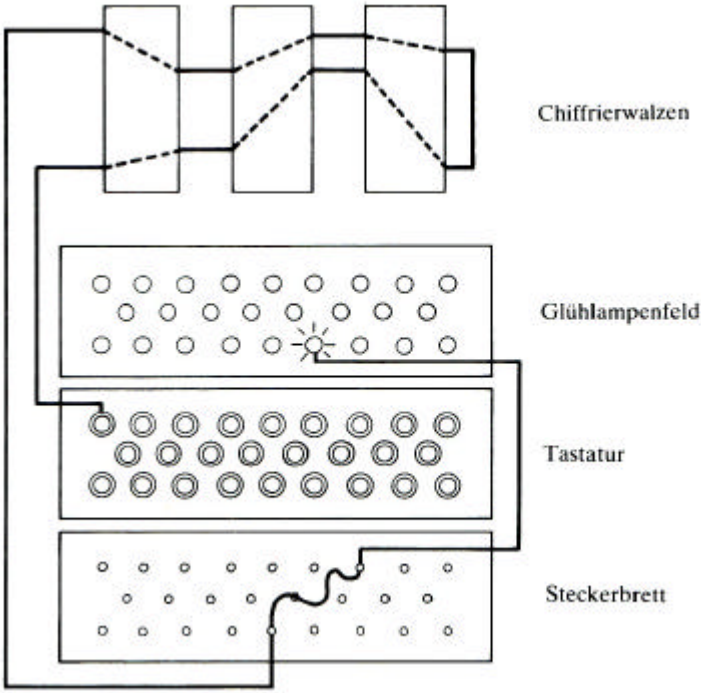
1 Haltevorrichtung
2 Federknöpfe
3 Haltehebel
4 Abdeckplatte
5 Einstellräder
6 Tasten
7 Schaltergriff
8 Zellonplatte
9 Federknöpfe
10 Transparente
11 Scharniere
12 Chiffrierwalzen
13 Zahlenringe
14 Doppelstecker
15 Steckerbrett
16 Fenster
17 Metalldeckel
18 Halteschrauben
19 Haltehebel
20 Umkehrwalze
21 Achse
21a Achsenbund
22 Haltefeder
23 Knopf
24 Federzapfen
25 Stirnwand
26 Haken
27 Batteriekasten
28 Kordelschrauben
29 Tastenbolzen
30 Doppelsteckerschnur
31 Buchsenpaare
32 Betriebsanweisung
33 Punktzeichen
34 Walzenkennzeichen
35 Federkontaktstifte
36 Glatte Kontaktflächen
37 Reserveglühbirnen
38 Glühlampenfeld
39 Lampenprüfer
40 Kabelprüfer
41 Kabelprüfbuchsen
42 Blatthalter

Zeichnung des britischen ›Bombe‹-Gerätes nach dem Gedächtnis von Leuten, die das Original kannten. Im Verhältnis zur danebenstehenden Schreibmaschine müßte es 1,80 Meter hoch gewesen sein.



diente sie als Schlüssel für die anderen. Auch Wettermeldungen waren aufschlußreich. Das europäische Wettergeschehen verläuft zumeist von West nach Ost. So wußten die Briten im voraus, welche Wettervorhersagen von den Deutschen insbesondere an die Luftwaffe ausgegeben werden würden.

Vereinfachtes Schema über die innere Verdrahtung einer Dreiwalzen->Enigma<.



Auch deutsches Schlüsselpersonal half unbeabsichtigt in mehrfacher Hinsicht. Häufig hatte der Nachrichtenoffizier eines höheren Stabes einen gleichlautenden Funkspruch an mehrere Einheiten herauszugeben, jeden auf einem besonderen Schlüsselnetz mit besonderer Kenngruppe, wobei jede wiederum ihren eigenen charakteristischen >Enigma<-Schlüssel hatte. Das Heer benutzte viele dieser Kenngruppen. Unglaublich zwar, aber es gab Verschlüßler, die eine gleichlautende Meldung unter verschiedenen Kenngruppen herausschickten. Als Bletchley nun einen dieser Funksprüche entschlüsselt hatte, besaß es eine Klartextvorlage für alle anderen Verschlüsselungen, und zwar nicht nur für diesen einen Funkspruch, sondern für alle weiteren, solange der Schlüssel nicht gewechselt wurde. Die Wahl des Spruchschlüssels verleitete zu Nachlässigkeiten, die den Kodebrechern wertvolle Hinweise lieferten. Es sei daran erinnert, daß die Verschlüßler drei beliebig wählbare Buchstaben zweimal hintereinander in die Maschine einzutasten hatten. Viele wählten >XYZ< oder >ABC< oder entgegen den Anweisungen ihre eigenen Namensinitialen oder die ihrer Freundin – immer und immer wieder. Die Einheiten dieser Leute wurden durch ihre Funkrufzeichen bald ausfindig gemacht, wodurch >Baracke T in Bletchley bald den Tagesschlüssel herausgefunden hatte. Es gab auch noch andere übliche Kniffe, die beim Entschlüsseln weiterhalfen. Zum Beispiel ist >Q< ein selten vorkommender Buchstabe im Deutschen; andererseits ist >CH< wiederum sehr häufig; viele Einheiten benutzten daher >Q< anstelle des längeren >CH<. Ferner gab es kein Punktzeichen in der >Enigma<-Tastatur, deshalb wurde gern >YY< als >Ende<- oder Punktzeichen benutzt.

Die Kryptologen verließen sich weitgehend auf >Löcher<, die oft in den Schlüsseln vorkamen. Angenommen, >XYZXYZ< sei die frei zu wählende Buchstabengruppe, die ein Verschlüßler benutzt hatte, und die nach Durchlauf durch die Chiffrier-

walze zum Beispiel als >PAQPAB< verschlüsselt herauskam. Hierin erscheint >P< zweimal. Diese Wiederholung eines Buchstabens in der Schlüsselgruppe wurde >Loch< genannt. Wenn etwa um die dreißig dieser >Löcher< im gleichen Schlüssel empfangen wurden, so konnte das Programm der >Bombe< damit gespeist werden. und es bestand gute Aussicht auf Erfolg, die Meldung zu dechiffrieren. Die Polen scheinen die Technik erfunden zu haben, nicht jedoch die Bezeichnung dafür. Sie wurde in Bletchley typisch englisch geprägt und war ursprünglich auf die Anordnung der Stanzlöcher in den großen Lochkartenblättern bezogen, die auf Leuchttischen ausgewertet wurden. Turing war es, wie schon erwähnt, der die Verbesserungen an der ursprünglichen Leuchttischtechnik vornahm und sie dem >Bombe<-Verfahren anpaßte.

Die >Enigma<-Maschine trug selbst dazu bei. Weil sie die Stromimpulse durch alle drei Chiffrierwalzen zurückleitete, konnte sie nie einen gleichlautenden Buchstaben selbst verschlüsseln (falls sie es dennoch tat, mußte Walze >Eins< in den beiden anderen einen Kurzschluß auslösen). Selbst dieser Mangel wurde von den Briten funkmäßig aufgeklärt und auf Stichhaltigkeit überprüft. Sie schickten ein Flugzeug an die französische Küste, um eine bekannte deutsche Leuchtboje zu zerstören; vielleicht eine, die eine ausgebaggerte Fahrrinne für Schnellboote vor der Küste von Calais kennzeichnete. Funkabhörstellen wurden nun angewiesen, insbesondere auf Funksprüche der zuständigen deutschen Kommandobehörde zu horchen. Alsbald mußte ein Funkspruch folgen, der die Schiffe warnte. Die britischen Kryptologen konnten ziemlich sicher sein, daß die Angabe: »Erloschen ist Leuchttonne« in dem Text erscheinen würde. Dann wurde durch Vergleich des erwarteten deutschen Ausdrucks im Klartext mit den verschlüsselten Gruppen nach einem Teil der Meldung gesucht, der keinen der deutschen Klartextbuchstaben enthielt. Wegen des Unvermögens der >Enigma<-Maschine, einen gleichlautenden Buchstaben selbst zu verschlüsseln, mußte die Textstelle, wenn man Glück hatte, die verschlüsselten Buchstaben der üblichen Redewendung enthalten:

Schlüsselgruppe:	FQZPA MSLOK
Klartext:	LEUCH TONNE

Sofern eine derartige Meldung tatsächlich erhältlich war. wurde sie über die rückseitig angebrachte Steckerverbindung als Teilprogramm des >Menüs< in die >Bombe, eingegeben.
Die britische Großrechenmaschine >Bombe< bestand aus fünfundzwanzig bis dreißig Dreiwalzengeräten. die genauso verdrahtet waren wie die >Enigma<-Maschinen und über die gleichen. eingestanzten sechsundzwanzig Buchstaben des Alphabets auf dem Rand verfügten. Die Dreiwalzensätze waren übereinander angeordnet, wobei der oberste Walzensatz der ersten Chiffrierwalze des >Enigma<-Gerätes entsprach, der mittlere der zweiten und der unterste der dritten >Enigma<-Chiffrierwalze. Sie waren farblich unterschieden und wurden jeweils auf Anweisung von >Baracke 6< oder Baracke 8< von den Marinehelferinnen ausgetauscht. Die Kryptologen konnten festlegen, welche drei der fünf Walzen jeweils genutzt werden sollten. Wahrscheinlich wurde es entweder durch mathematische Berechnung und Auswertung der Schlüssel oder durch das Vorhandensein von >Löchern< im Schlüssel festgelegt.
Die Schalttafel hatte mehrere Reihen von Buchsen, wie in einer Telefonvermittlung, nur mit dem Unterschied, daß die Buchsen jeweils in Linien von je sechsundzwanzig angeordnet waren, jede mit einem Buchstaben des Alphabets