

Werftschlüssel

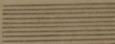
M. Dv. Nr. 103

Berlin 1940
Oberkommando der Kriegsmarine

Source: TICOM Document T-2750,
Bestand Rückgabe TICOM, S8,
Politisches Archiv des Auswärtigen Amts, Berlin.

URL: <https://cryptocellar.org/wmc/m.dv.nr.103-werftschluessel.pdf>

Editor: Frode Weierud, Crypto Cellar Research

Nr. 

Geheim!

Werftschlüssel

T-2750



Berlin 1940

Oberkommando der Kriegsmarine

M. Ov. Nr. 103

Ich genehmige den »Werftschlüssel« — M. Dv. Nr. 103. Er tritt am 15. Mai 1940 in Kraft.

Abänderungen des »Werftschlüssels« oder des vorgesehenen Ausrüstungsstreifens sind verboten.

Bei Nichtgebrauch ist der »Werftschlüssel« unter sicheren Verschuß zu nehmen. Liegt Gefahr vor, daß der »Werftschlüssel« in Feindeshand fällt, so ist er durch Feuer wirksam zu vernichten. Ist dies nicht möglich, so muß er auf andere Weise wirksam vernichtet oder auf tiefem Wasser versenkt werden.

Auf Dienststellen am Lande finden diese Bestimmungen sinngemäß Anwendung.

Berlin, im März 1940.

Der Oberbefehlshaber der Kriegsmarine

Verteiler.

Kriegsmarine:

Bordstellen:

Flottenkommando
Befehlshaber und Führer
Flottillenkommandos und gleichgeordnete Verbandsstäbe
Schlachtschiffe
Kreuzer
Zerstörer
Schulschiffe
Begleitschiffe
Minenschiffe, Minenräumschiffe
Trossschiffe
Werftfahrzeuge, Botenfahrzeuge und sonstige Fahrzeuge der Kriegsmarine mit Funkeinrichtung ohne militärisches Funkpersonal
Sonstige Fahrzeuge nur auf Befehl der Stationskommandos

Landstellen:

D. R. M.
Gruppenkommandos
Stationskommandos
Kmd. Adm.
N. J.
Kriegsmarinewerften
M. N. A.
M. N. D. mit M. F. S.
M. N. D. mit R. F. S.
R. S.

Luftwaffe:

Gen. d. Lw. b. Ob. d. M. — MM
Seenotzentralen
Seenotbezirksstellen
Flugsicherungsschiffe
See-Fl. H. N. S.

Schlüsselanleitung.

Allgemeines.

1. Der Werftschlüssel dient zum geheimen Nachrichtenverkehr mit Werft-, Votten- und sonstigen im Dienst der Kriegsmarine stehenden Fahrzeuge sowie Flugversicherungsschiffen ohne militärisches Funkpersonal.

Die Benutzung durch andere Fahrzeuge wird von Fall zu Fall befohlen.

2. Bei Verwendung des Werftschlüssels wird der vorbereitete Klartext unmittelbar mit Doppelbuchstaben-tauschtafeln verschlüsselt.
3. Die Funkprüche nach dem Werftschlüssel bestehen aus fünfstelligen Buchstabengruppen.

Kennung.

4. In den Fällen, in denen eine Unterscheidung der nach dem Werftschlüssel verschlüsselten Nachrichten von sonstigen Funkprüchen mit fünfstelligen Buchstabengruppen, die nach einem anderen Schlüsselverfahren verschlüsselt sind, notwendig ist, werden als Kennung die Buchstaben »gr« vor die Gruppenzahl gesetzt.

Tauschtafelplan.

5. Der Tauschtafelplan bestimmt die zum Ver- und Entschlüsseln der Kenngruppen zu benutzende Tauschtafel. Für jeden Monatstag ist eine Tauschtafel aus dem »Schlüsselheft zum Werftschlüssel« festgesetzt. Die Tauschtafeln wechseln um 0000 Uhr.

Tauschtafelweiser.

6. Der Tauschtafelweiser enthält die Zahlen 1 bis 20 in willkürlicher Folge. Diese Zahlen entsprechen den Tauschtafeln des Schlüsselheftes zum Werftschlüssel.
7. Die an der linken (rechten) Seite und oben (unten) stehenden Buchstabenpaare des Tauschtafelweisers dienen zur Bildung der Kenngruppe.
8. Zur Schlüsselung werden jedesmal fünf hintereinanderstehende Zahlen aus dem Tauschtafelweiser benötigt. Diese fünf Zahlen werden als Tauschtafelreihe bezeichnet. Die erste dieser fünf Zahlen ist die »Einsatzstelle«.
9. Beim **Verschlüsseln** wird die Einsatzstelle willkürlich gewählt und die an dieser Stelle stehende und die vier folgenden Zahlen herausgeschrieben.
10. Beim **Entschlüsseln** wird das aus dem ersten und zweiten Buchstaben gebildete Buchstabenpaar der entschlüsselten Kenngruppe in der linken (rechten) senkrechten Doppelbuchstabenreihe und das aus dem vierten und fünften Buchstaben gebildete Buchstabenpaar in der oberen (unteren) waagerechten Doppelbuchstabenreihe aufgesucht. Die im Schnittpunkt dieser beiden Buchstabenpaare stehende Zahl ist die Einsatzstelle, die zusammen mit den folgenden vier Zahlen die Tauschtafelreihe bildet.

11. Zur Erhöhung der Schlüsselsicherheit muß nach Möglichkeit verhindert werden, daß innerhalb kurzer Zeit für verschiedene Funksprüche die gleiche Einsatzstelle und damit die gleiche Tauschtafelserie benutzt wird. Daher ist für jeden Funkspruch eine andere Einsatzstelle zu wählen.

Von den M. J. S. ist bei jedem ausgehenden Funkspruch die gewählte Einsatzstelle leicht mit Blei anzuhaken. Soweit es möglich ist, sind auch die Einsatzstellen der eingehenden Funksprüche zu bezeichnen. Diese Bleistiftstriche sind erst dann zu entfernen, wenn alle im Tauschtafelreißer enthaltenen Zahlen angehängt sind.

Doppelbuchstabentauschtafeln.

12. Zum Verschlüsseln und zum Entschlüsseln werden die gleichen Tauschtafeln benutzt.
13. Das zu ver- bzw. entschlüsselnde Buchstabenpaar wird in der Tauschtafel aufgesucht und das hinter dem Gleichheitszeichen stehende Buchstabenpaar herausgelesen.

Kenngruppe.

14. Zur Bezeichnung der zum Verschlüsseln benutzten Tauschtafelserie dient eine Kenngruppe. Sie bezeichnet die Einsatzstelle (Ziffer 8).
15. Die Kenngruppe wird gebildet aus den links (rechts) neben und über (unter) der Einsatzstelle stehenden Buchstabenpaaren und einem willkürlich gewählten Buchstaben (Füllbuchstabe). Hierbei werden das links (rechts) stehende Buchstabenpaar als die beiden ersten Buchstaben, das oben (unten) stehende als die beiden letzten Buchstaben und der Füllbuchstabe als mittlerer Buchstabe der fünfstelligen Buchstabengruppe eingesetzt.

S. B. links (rechts) l m
oben (unten) d f
Füllbuchstabe k } ergibt Kenngruppe l m k d f

16. Unter die so gebildete Kenngruppe wird eine fünfstellige Buchstabengruppe gesetzt, bei der die Buchstaben willkürlich gewählt und zusammengefaßt sind.
17. Diese beiden Gruppen werden zusammengefaßt und mit der im Tauschtafelplan bezeichneten Tauschtafel verschlüsselt.

Die verschlüsselten Gruppen werden als **vorletzte** und **letzte** Funkgruppe in den Funkspruch eingesetzt.

18. Beim Verschlüsseln und Entschlüsseln werden je zwei untereinanderstehende Buchstaben der Kenngruppe und der willkürlich zusammengefaßten Gruppe zu einem Buchstabenpaar zusammengefaßt und durch das entsprechende Buchstabenpaar aus der Tauschtafel ersetzt.

S. B.: Kenngruppe:

l	m	k	d	f
1	2	3	4	5

willkürlich zusammengefaßte Gruppe:

k	c	y	w	b
---	---	---	---	---

 } verschlüsselt

h	a	x	f	w
1	2	3	4	5
p	s	e	b	q

Vorbereiten des Klartextes.

19. Der Funkspruch muß so kurz wie möglich, aber trotzdem klar verständlich sein.
20. Inhaltlich gleiche oder ähnliche Nachrichten sind durch Umstellen, Erweitern oder Kürzen des Wortlautes jedesmal anders zu gestalten.

Bei See-, Warn- und Wetternachrichten sind einleitende Überschriften fortzulassen.

21. a) Statt der **Umlaute** ä, ö und ü ist ae, oe und ue einzusetzen. A, o und u können statt der entsprechenden Umlaute dann eingesetzt werden, wenn die Nachricht dabei unmißverständlich bleibt.

b) Bei **Zahlen** werden die einzelnen Ziffern als Ziffernwörter ausgeschrieben, die bei mehrstelligen Zahlen aneinandergereiht werden, z. B. 8 = acht, 18 = eins acht, 108 = eins null acht. Folgende Zahlenwerte können jedoch als ein Wort geschrieben werden: Zehn, elf, zwanzig, dreißig usw., hundert, tausend usw.

Zwei unmittelbar aufeinanderfolgende Zahlen, zwischen die kein Komma gesetzt werden darf, sind durch yy voneinander zu trennen,

z. B. □ 8316 2 verschiedene Tonnen = ... acht drei eins sechs yy zwei

c) **Satzzeichen** werden ausgedrückt:

Punkt durch x	Trennungsstrich durch yy
Doppelpunkt durch xx	Fragezeichen durch ud
Komma durch y	Klammer durch kk (vor und nach dem Eingeklammerten)

Satzzeichen sind im allgemeinen nicht entbehrlich. Sie können weggelassen werden, wenn dadurch der Sinn der Nachricht nicht mißverstanden werden kann. Ein Schlüsselpunkt ist nicht einzusetzen.

d) Als **Hervorhebungszeichen** für nicht geläufige Eigennamen, Worte und Begriffe wird vor und hinter diesen Namen usw. der Buchstabe j gesetzt, z. B. j ... j. Besonders wichtige Worte können erforderlichenfalls zweimal hintereinander eingesetzt werden, dabei ist das Wort jedesmal einzeln zwischen j ... j zu setzen.

e) **Breiten- und Längenangaben** sind in der Regel nur durch die Zahlenwerte der Grade, Minuten und Sekunden auszudrücken, die hierfür in unmittelbarer Folge nebeneinander gestellt werden. Die Worte »Grad«, »Minuten« und »Sekunden« werden dabei weggelassen. Die Zahlenwerte von 0 bis 9 werden durch eine davorgesetzte Null zweifellig gemacht.

Die Breiten- und Längenangaben bei Graden unter 99° werden also als zwei-, vier- bzw. sechsstellige ganze Zahlen, bei Graden über 99° als drei-, fünf- bzw. siebenstellige ganze Zahlen in den Spruch eingesetzt.

Sind jedoch Zehntelminuten statt volle Sekunden angegeben, so sind sie von den vollen Minuten durch ein Komma zu trennen.

Sind Bruchteile von Sekunden angegeben, so werden die Bestenangaben in vollem unverändertem Wortlaut verschlüsselt.

Umwandlung von vollen Werten in Dezimalwerte und umgekehrt ist im Schlüsseldienst verboten.

Zur eindeutigen Unterscheidung ist »Ost« durch dreimal »o«, »West« durch dreimal »w« auszudrücken.

Beispiele:

70 Grad Nord	=	70 nord
170 Grad West	=	170 www
4 Grad 1 Min. Süd	=	0401 süd
31 Grad 0 Min. 7 sec West	=	310007 www
104 Grad 56 Min. 8 sec Ost	=	1045608 ooo
125 Grad 50,5 Min. Ost	=	12550,5 ooo

22. a) **Dienststellenbezeichnungen innerhalb des Funkspruchwortlautes sowie An- und Unterschriften** werden ausgeschrieben. Von Abkürzungen ist weitgehend Gebrauch zu machen; dabei ist jedoch zu beachten, daß der Name nicht verkürzt wird und keine Verwechslungen möglich sind.

Bei Abkürzungen der Dienststellen sowie An- und Unterschriften, die sich von anderen nur durch einen oder zwei Buchstaben unterscheiden und bei Schiffs- und Bootsnamen, bei denen Verwechslungsgefahr besteht, wird der unterscheidende Buchstabe **dreimal** eingesetzt;

z. B. B d R	=	bdkkk
F d M	=	fdmmm
U 10	=	uuu zehn
2. U. Gl.	=	zwote uuufi

Die Form der Abkürzung ist, soweit dies ohne Mißverständnisse hervorzurufen möglich ist, abwechselnd zu wählen, um hierdurch die Funksprachlänge und den Funksprachanfang verschieden zu gestalten;

z. B. Kriegsmarinewerft Kiel ist entweder voll auszuschreiben oder RMW Kiel, Werft Kiel, Kiel Werft usw. einzusetzen.

Folgen mehrere Dienststellenbezeichnungen oder Anschriften aufeinander, so ist darauf zu achten, daß keine Mißverständnisse möglich sind; erforderlichenfalls Trennung durch y (Komma).

b) **An- und Unterschriften** werden durch das Wort »von« getrennt und entweder an den Anfang, an eine beliebige Stelle des Wortlautes oder an das Ende der zu verschlüsselnden Nachricht gesetzt und mit verschlüsselt. Um die Schlüsselarbeit zu erleichtern, sind bei lebhaftem Funkverkehr die Anschriften vorwiegend an den Anfang oder an das Ende des Funkspruches zu setzen. Sie sind von dem Wortlaut der Nachricht durch yy zu trennen.

Die Buchstaben yy sind einzusetzen, wenn

An- und Unterschrift am Anfang	hinter der Unterschrift
An- und Unterschrift innerhalb des Wortlautes	vor der Anschrift und hinter der Unterschrift
An- und Unterschrift am Ende	vor der Anschrift

Ist die abgehende Funkstelle nicht die Funkstelle des Aufgebers und muß, um nötigenfalls den Aufgeber und die abgehende Funkstelle klar herauszustellen, neben der Unterschrift des Aufgebers auch der Name der abgehenden Funkstelle im Spruch genannt werden, so ist die abgehende Funkstelle im Anschluß an die Unterschrift getrennt durch das Wort »durch« einzusetzen.

z. B.: Anschrift: FdM, Unterschrift: V 1607,
abgehende Funkstelle: V 1609.

Dann ist einzusetzen: fdmmm von vvv eins sechs nul siben
durch vvv eins sechs nul neun

Ist der Wortlaut des Funkspruches auch ohne An- oder Unterschrift verständlich (z. B. bei Warnmeldungen u. dgl.), so ist die Anschrift fortzulassen. Unter Umständen kann auf beides verzichtet werden.

23. Der vorbereitete Klartext wird buchstabenweise in die Spalte »Buchgruppen« des Schlüsselzettels zu fünfstelligen Gruppen von links nach rechts eingetragen, und zwar zuerst in die 1. Zeile, dann in die 3. Zeile, 5. Zeile, 7. Zeile und 9. Zeile, danach in die 2. Zeile, 4. Zeile, 6. Zeile, 8. Zeile und 10. Zeile. Nach der 10. Zeile wird die Eintragung des Klartextes in laufender Reihenfolge der Zeilen fortgesetzt, und zwar in die 11. Zeile, 12. Zeile, 13. Zeile usw.
24. Enthält die letzte Gruppe des vorbereiteten Klartextes weniger als fünf Buchstaben, so ist sie mit beliebigen Konsonanten fünfstellig aufzufüllen. Dabei ist darauf zu achten, daß keine Mißverständnisse möglich sind. Jede Regelmäßigkeit in der Anwendung der Füllkonsonanten ist zu vermeiden.
25. Je zwei Buchgruppen sind zu Buchgruppenpaaren zusammenzufassen. Die Buchgruppenpaare sind durch einen dicken waagerechten Strich voneinander zu trennen.

Verlängerung von Funksprüchen.

26. Die Bestimmungen über das Umstellen, Erweitern oder Kürzen von gleichen oder ähnlichen Nachrichten werden durch die nachfolgenden Bestimmungen erweitert.
27. Die Nachricht wird durch Anhängen von Buchstaben und Wörtern auf unterschiedliche Länge gebracht. Unmittelbar an das letzte Wort des zu verschlüsselnden Klartextes sind drei oder vier gleichlautende **Buchstabenpaare** und daran anschließend ein oder mehrere beliebige, inhaltlich neutrale, im allgemeinen bekannte Worte anzufügen, z. B. Wassereimer, Fernsprecher, Kleiderschrank u. ä.;
z. B. . . . minenverseucht mfmfmf Kleiderschrank . . .
Worte, die gegen Zucht und Ordnung verstoßen, persönliche Mitteilungen u. ä. sind verboten. Bei der Wahl der Worte und der gleichlautenden Buchstabenpaare ist darauf zu achten, daß die Verlängerungsworte nicht mit dem eigentlichen Wortlaut der Nachricht in Zusammenhang gebracht werden können.
28. Das Einsetzen von bekannten Verlängerungswörtern der deutschen Sprache hat den Zweck, dem Schlüssel die Gewähr zu geben, richtig entschlüsselt zu haben.

Verschlüsseln.

29. Im Tauschtafelweiser wird eine beliebige Einsatzstelle gewählt (siehe Ziffer 8).
30. Die Zahlen der Tauschtafelserie werden nacheinander auf dem Schlüsselzettel über den Buchstaben der fünfstelligen Buchgruppen eingetragen.
Dabei ist die erste Zahl (Einsatzstelle) über dem ersten, die zweite Zahl über dem zweiten usw. und die fünfte über dem fünften Buchstaben der fünfstelligen Buchgruppen niederzuschreiben.
31. Die fünfstelligen Buchgruppen werden nur spaltenweise mit der Tauschtafel verschlüsselt, die der über der Spalte stehenden Zahl entspricht.
Zuerst wird die erste Spalte verschlüsselt.
32. Dabei werden zwei untereinanderstehende Buchstaben eines Buchgruppenpaares zu einem Buchstabenpaar zusammengefaßt, wobei der obenstehende Buchstabe der erste und der untenstehende der zweite Buchstabe des Buchstabenpaares ist.
33. Dieses Buchstabenpaar wird in der entsprechenden Tauschtafel aufgesucht und das danebenstehende Buchstabenpaar in die Spalte »Funktgruppen« eingetragen, und zwar der erste Buchstabe oben und der zweite Buchstabe darunter.
34. Wenn alle Buchstabenpaare der ersten Spalte verschlüsselt worden sind, werden die der zweiten, dann die der dritten, dann die der vierten und zuletzt die der fünften Spalte verschlüsselt.
35. Bei ungerader Buchgruppenzahl werden die ersten vier Buchstaben der letzten Buchgruppe zu zwei Buchstabenpaaren zusammengefaßt und mit der für die erste Spalte gültigen Tauschtafel verschlüsselt.
Der fünfte Buchstabe der Buchgruppe wird nicht verschlüsselt.
36. Anschließend werden die gem. Ziffern 15—18 gebildeten und verschlüsselten **Rennguppen** als die beiden letzten Funkgruppen eingefügt.
37. Die richtige Verschlüsselung ist durch Rückschlüsseln zu prüfen.
38. Dann wird der Funkspruch durch Einsetzen der Uhrzeitgruppe, nötigenfalls der Kennung (gr) und der Gruppenzahl abgabefertig gemacht.
Soll die verschlüsselte Nachricht, z. B. bei Benutzung zwischenstaatlicher Wellen, als Funktelegramm abgegeben werden, so ist der Telegrammkopf entsprechend einzusetzen.

39. **Beispiel:** (Tauschtafelserie, Renngruppe und Renngruppentauschtafel sind willkürlich gewählt.)
Folgende Nachricht soll verschlüsselt werden:

»1724. An Marbef. Dänemark, B. S. O. Geleit »Bollin« wegen Rebel geantert bei Kiel Feuerschiff
Reereburg.«

Tauschtafelserie: 6 2 15 9 7

Renngruppe: 1 m k d f

Renngruppentauschtafel gem. Plan: 17

Willkürlich zusammengefaßte Gruppe: r s p w b

1724					Uhrzeitgruppe						
gr 21					Gruppenzahl						
					6	2	15	9	7		
Zunfgruppen					Buchgruppen					Bedeutung	
g	m	o	w	a	q	u	a	d	r	1	An- und Unterschrift <

- Anmerkung: 1. Das Beispiel zeigt nur den Gang der Verschlüsselung an. Zunfgruppen, Laufstafel und die Kenngruppe sind willkürlich gewählt.
2. Die gem. Laufstafel zusammengehörenden Buchstabenpaare der Buch- und Zunfgruppen sind mit gleichen Ziffern bezeichnet.

Entschlüsseln.

40. Zuerst wird die Kenngruppe (letzten beiden Funkgruppen) entschlüsselt und durchgestrichen.
41. Je zwei Funkgruppen werden von oben nach unten zu einem Buchstabengruppenpaar zusammengefaßt. Die Gruppenpaare werden durch einen biden waagerechten Strich voneinander getrennt.
42. Im Tauschtafelweiser wird die durch die Kenngruppe bezeichnete Einsaßstelle aufgesucht und die Tauschtafelreihe entsprechend Ziffer 30 über den Buchstaben der fünfstelligen Funkgruppen eingetragen.
43. Der Funkpruch ist spaltenweise zu entschlüsseln.
44. Zwei untereinanderstehende Buchstaben sind gem. Ziffer 32 zu einem Buchstabenpaar zusammenzufassen.
45. Dieses Buchstabenpaar ist in der Tauschtafel aufzusuchen und das entsprechende Buchstabenpaar in die Spalte »Buchgruppen« einzutragen (s. Ziffer 33).
46. Bei ungerader Gruppenzahl sind je zwei Buchstaben der letzten Funkgruppe waagerecht zusammenzufassen und mit der für die erste Spalte gültigen Tauschtafel zu entschlüsseln. Der fünfte Buchstabe wird als solcher übernommen.
47. Aus der Spalte »Buchgruppen« sind nun die einzelnen Buchstaben zeilenweise von oben nach unten herauszuschreiben, sie ergeben den Klartext der verschlüsselten Nachricht.

48. Beispiel: Folgender Funkpruch wurde aufgenommen:
(Tauschtafelserie, Kenngruppe und Kenngruppentauschtafel sind willkürlich gewählt.)

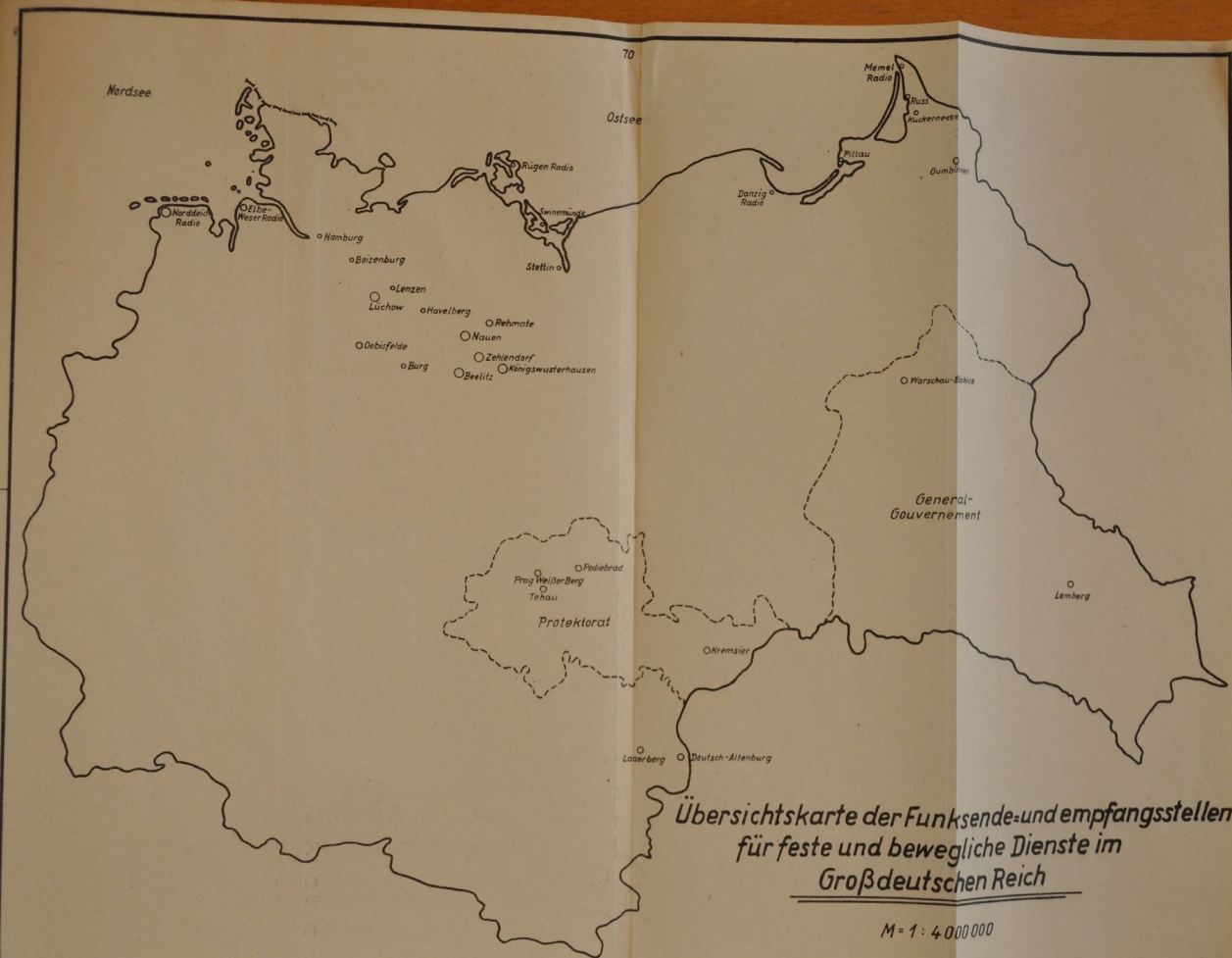
2256					Uhrzeitgruppe									
gr 17					Gruppengahl									
3	14	6	5	16										
Funkgruppen					Buchgruppen					Bedeutung				
c	s	w	r	l	v	e	r	a	b	1				
r	o	s	g	k	r	e	d	e	t	2				
m	l	a	x	h	e	n	t	r	e	3				
l	c	f	t	n	f	p	u	n	k	4				
k	t	v	u	b	t	g	e	h	e	5				
g	q	z	q	f	n	x	o	e	l	6				
u	y	j	e	k	u	b	e	r	n	7				
m	a	p	p	e	a	h	m	e	z	8				
h	d	e	i	u	w	o	x	d	r	9				
o	z	a	v	x	e	i	x	n	u	10				
d	z	j	h	h	l	a	c	h	t	11				
j	t	r	y	b	u	h	r	y	y	12				
x	u	f	c	p	w	o	l	l	i	13				
y	n	q	i	v	n	v	o	n	s	14				
x 1 i	g 2 a	r			c 1 h	e 2 e	r			15				
c	o	m	d	w	a	t	e	l	h	16				
x	f	t	i	g	p	j	u	q	s	17				

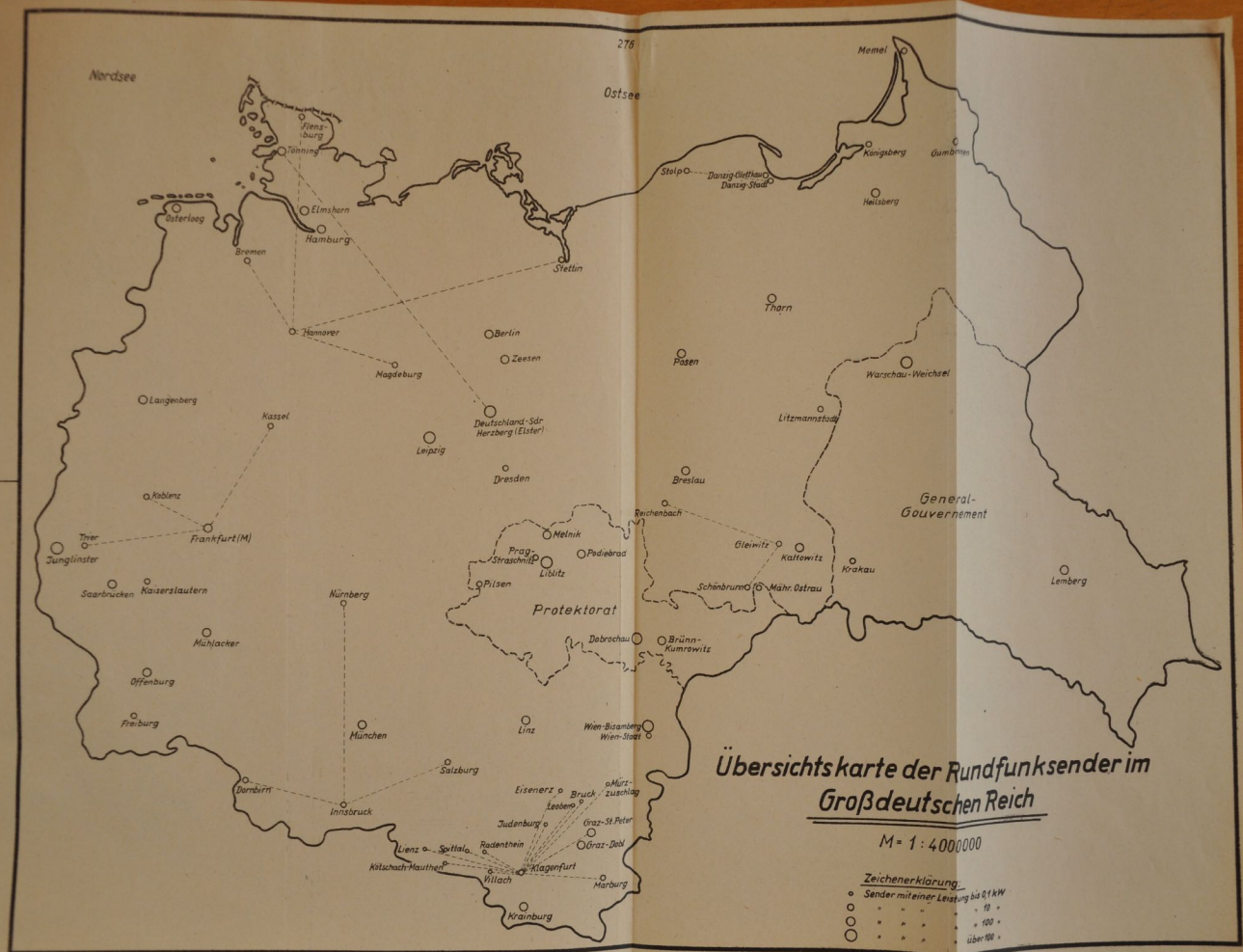
Kenngruppe atelh ergibt

Tauschtafelserie: 3 14 6 5 16

Nach der Entschlüsselung ergibt sich folgende Nachricht:

»2256. Verabredeten Treffpunkt gehen. Übernahme 2. 3. 0800 Uhr. An Wollin von Scheer.«





RECORD OF WORK DONE

TICOM NO. 2750

TITLE OF DOC.

Werkzeugschlüssel

DESCRIPTION:

Key for use by auxiliary
craft + shore installations
1940. From State Printing
Office Berlin.

Date	Job	By

erteiler.

gleichgeordnete Verbandsstäbe

Schiffe

zeuge und sonstige Fahrzeuge der Kriegs-
ung ohne militärisches Funkpersonal
auf Befehl der Stationskommandos

M. N. D. mit R. F. S.
R. S.

Luftwaffe:

- Gen. d. Lw. b. Ob. d. M. — RMW
- Seenotzentralen
- Seenotbezirksstellen
- Flugsicherungsschiffe
- See-Fl. S. N. S.