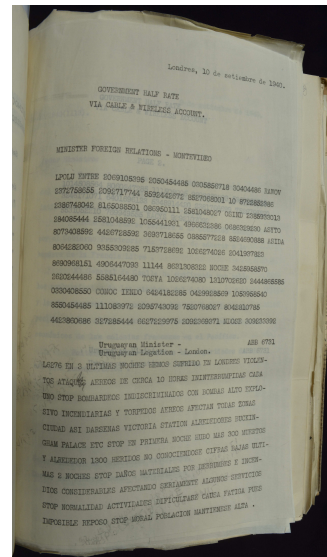
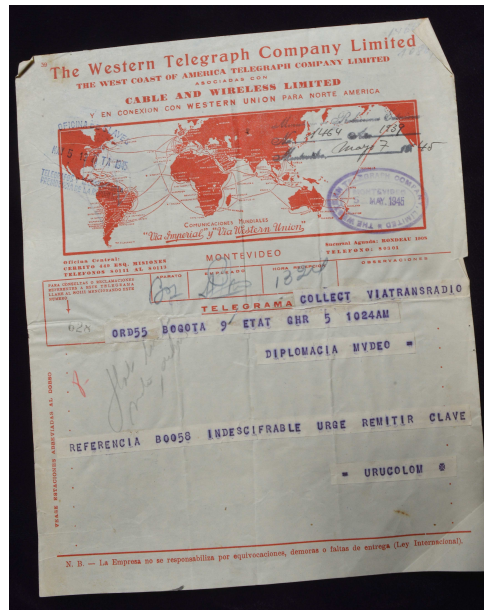


# Cryptography in Relaciones Exteriores





## Cryptography in Relaciones Exteriores



## Relaciones Exteriores: two rulers "Saint-Cyr", 1981



## Relaciones Exteriores: Gretacoder 805, c. 1975



Cryptography in Relaciones Exteriores: Gretacoder 805, c. 1975



Cryptography in Relaciones Exteriores: Gretacoder 906, c. 1976



Cryptography in Relaciones Exteriores: Gretacoder 906, c. 1976

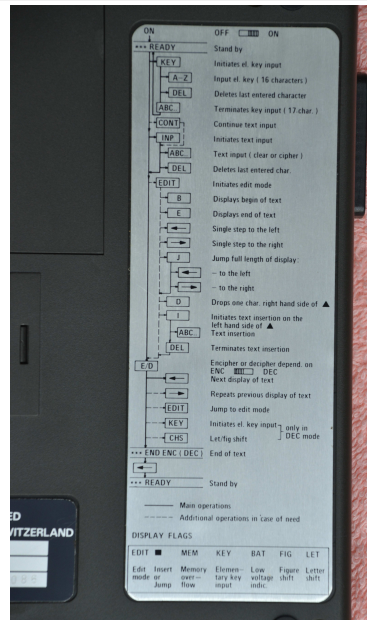




Cryptography in Relaciones Exteriores: Gretacoder 906, c. 1976



# Cryptography in Relaciones Exteriores: Gretacoder 906, c. 1976



## The Zimmermann telegram of 1917, overview

- ▶ The First World War, trench warfare
- ▶ The telegram
- ▶ Encryption and transmission
- ▶ British interception and decipherment
- ▶ Consequences

## Prehistory

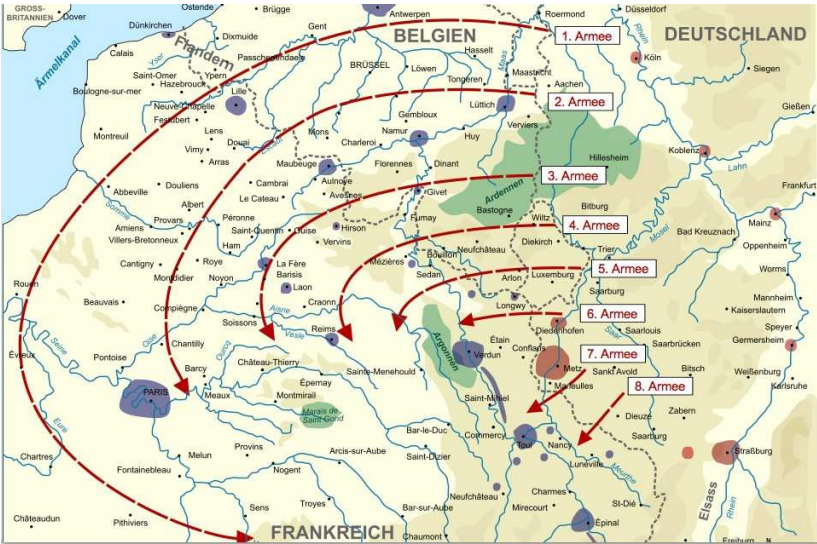
**Mexican-American War** 1846–1848: USA gain large tracts of Mexican territory, *Alta California* and *Santa Fe de Nuevo México* (including California, Texas, Arizona, New Mexico).

**Franco-German War** 1870–1871: German troops occupy Paris within a few weeks. Germany gains Alsace-Lorraine and becomes unified under Emperor Wilhelm I.

## The First World War (in the West)

- ▶ 28 July 1914 to 11 November 1918. Central powers (Germany, Austria-Hungary, and others) against the Entente (France, Great Britain, Russia, and others).
- ▶ 1 August 1914: German troops march through Belgium towards Paris (Schlieffen plan), but are stopped by the French and British forces.
- ▶ The ensuing trench war exhausts both sides morally, militarily, and financially.

# The Schlieffen plan



French attack on German trench



## The Zimmermann telegram, Januar 1917

- ▶ The leading German generals, Paul von Hindenburg (1847–1934) and Erich Ludendorff (1865–1937) convince Emperor Wilhelm II.: we can only win the war if we enter unrestricted U-boat warfare.





## The Zimmermann telegram, Januar 1917

- ▶ Worry: the US enter the war on the side of the Entente.
- ▶ Arthur Zimmermann (1864–1940), German foreign minister, starts an inept attempt to stop the US: Mexico shall reconquer the lost territories of Texas, New Mexico, and Arizona.



## The Zimmermann telegram, January 1917

9 January	Imperial U-boat decision
13 January	Zimmermann signs message
16 January	telegram(s) from Berlin to Washington in 0075
19 January	telegram from Washington to Mexico in 13040
31 January	Germany declares unrestricted U-boat warfare
3 February	US president Wilson breaks relations with Germany
10 February	Room 40 receives 13040 message from Mexico
22 February	Reginald Hall gives decrypt to Walter Page
24 February	President Wilson receives the telegram
1 March	story published in US newspapers
3 March	Zimmermann admits responsibility
6 April	US congress declares war on Germany

## 100 years Zimmermann telegram

**Cinvestav**

### SIMPOSIO EN CONMEMORACIÓN DE LOS 100 AÑOS DEL ENVÍO DEL TELEGRAMA DE ZIMMERMANN

El Departamento de Computación del Cinvestav organiza el presente Simposio en conmemoración del centenario del envío del telegrama en clave de Arthur Zimmermann, secretario de Asuntos Exteriores alemán al gobierno de México, invitando a científicos, académicos y funcionarios del Cinvestav del Estado Político de Zacatecas y de otras instituciones de Educación Superior, y posgrado en ciencias.

#### POENCIAS

Prof. Dr. Joachim von zur Gathen  
Profesor emérito  
Bonn Aachen International Center for Information Technology

Dr. Guillermo Morales Luna  
Investigador Titular en el Departamento de Computación en Cinvestav-IPN  
Escuela de Ciencias Exactas, Ingeniería y Tecnología de Zacatecas, Zacatecas, México

Captán 2da. Habilidad: Sergio Martínez Torres  
Esc. Pol. de Aviac. y Espaciales - IPN

**Lunes  
16 enero 2017  
10:00 am**

Auditorio del edificio de Ingeniería Eléctrica y Computación, CINVESTAV-IPN, Zacatecas, CDMX  
<https://www.cs.cinvestav.mx/SimposioZimmermann2017>

## Sending the telegram

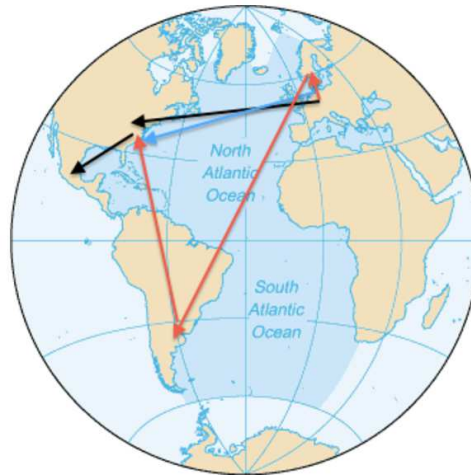
**Codebooks** for encryption:

- ▶ 13040: 11 000 words, broken by the British cipher bureau *Room 40* in 1915. This was guessed at by the Germans.
- ▶ 0075: more secure construction, not broken in early 1917. The commercial U-boat *Deutschland* had brought it to the German embassy in Washington in December 1916, but it was not available in Mexico.

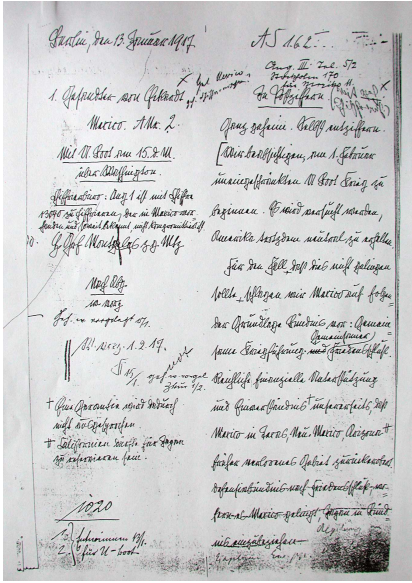
The British *HMS Telconia* had cut all transatlantic cables out of Germany on 5 August 1914. The Germans had the following four options for **transmission**:

- ▶ Another U-boat.
- ▶ Transmission between the high-power radio station at Nauen near Berlin and at Sayville on Long Island NY.
- ▶ The *Swedish roundabout*, via Stockholm and Buenos Aires.
- ▶ On US diplomatic cable from Berlin to Washington, which US ambassador James Gerrard had allowed for messages concerning peace negotiations.

## Possible transmission routes



The Zimmermann telegram: the original text



## The Zimmermann telegram in English

Most secret. Decipher yourself.

We intend to begin on the first of February unrestricted submarine warfare. We shall endeavour in spite of this to keep the United States of America neutral.

In the event of this not succeeding, we make Mexico a proposal of alliance on the following basis: Conduct war jointly. Conclude peace jointly. Substantial financial support and consent on our part for Mexico to reconquer lost territory in Texas, New Mexico, and Arizona. The settlement in detail is left to your Excellency. Your Excellency will inform the President of the above most secretly as soon as the outbreak of war with the United States of America is certain, and add the suggestion that he should, on his own initiative, invite Japan to immediate adherence, and at the same time mediate between Japan and ourselves.

Please call the President's attention to the fact that the ruthless employment of our submarines now offers the prospect of compelling England in a few months to make peace.

# The Zimmermann telegram: a closer look

AS162 pr. 12. Januar 1917, p.m. 000001 Eili sehr.  
 Berlin, den 13. Januar 1917. AS 162 I

1. Gesandter von Eckardt <sup>mit Mexico</sup> <sup>Stockholm 130</sup> <sup>Ang. III. Teil. 5/2</sup>  
<sup>als Chiffretelegramm</sup> <sup>für Mexico</sup> <sup>In Postziffern</sup> <sup>Mit geh.</sup> <sup>(Chiffre Text.)</sup>

Mexico ANr. 2. Ganz geheim. Selbst entziffern.

Mit U-Boot am 15.d.M. über Washington. Wir beabsichtigen, am 1. Februar uneingeschränkten U-Boot Krieg zu

<sup>Chiffretext</sup> Ang. I ist mit Chiffre 13040 zu chiffrieren, der in Mexico vor- <sup>beginnen. Es wird versucht werden,</sup>  
<sup>handen mit demselben nicht komprimiert ist.</sup> Amerika trotzdem neutral zu erhalten.

H. Graf Montgelas z.g. Mtz Für den Fall, daß dies nicht gelingen sollte, schlagen wir Mexico auf folgen

Nach Ag. W. WIZ der Grundlage Bündnis vor: Gemeinsame Kriegführung und Friedensschluß

W. vorz. 1.2.17. <sup>Reichliche finanzielle Unterstützung</sup>

† Eine Garantie wird dadurch und Einverständnis unsererseits, daß nicht ausgesprochen. Mexico in Texas, Neu-Mexico, Arizona †

‡ Californien dürfte für Japan früher verlorenes Gebiet zurückerobern. zu reservieren sein. Defensivbündnis nach Friedensschluß, wo

1020 fern es Mexico gelingt, Japan in Bündnis einzubeziehen. Regelung im Einzelnen Ew. pp. überlassen.

1. Entnommen 11.
2. für U-Boot



## Transmission and interception

Four possible routes: U-boat, German radio stations, Swedish roundabout, US diplomatic cable.

- ▶ U-boat: trip cancelled.
- ▶ Radio: no encrypted messages allowed.
- ▶ Sweden or US?

How to prove it did not go via Sweden? “co-NP”.

My stroke of luck: Maria Keipert, the knowledgeable director of the archive of the German Foreign Office, showed me the log book of encrypted messages (“*Geheime Ausgänge*”) to Sweden. Several entries in January 1917, but **not** the Zimmermann telegram.

The British **intercepted** all transatlantic cable transmissions, including US diplomatic messages and the Zimmermann telegram in 0075.

## Transmission and interception

Conclusion: The Zimmermann telegram (in German: *Mexiko-Depesche*) went in code 0075 on the undersea cable connecting the US embassy in Berlin to Washington. It was handed to the German ambassador, Graf Johann Heinrich Andreas Hermann Albrecht von Bernstorff, decrypted, re-encrypted in code 13040, and sent via Western Union to the German minister, Heinrich von Eckardt, in Mexico.

This shows the difficulty of transmitting secret keys over a public line. Is this possible at all?

Computer science enters cryptography: yes, it is possible. Diffie & Hellman 1976. Public-key cryptography.

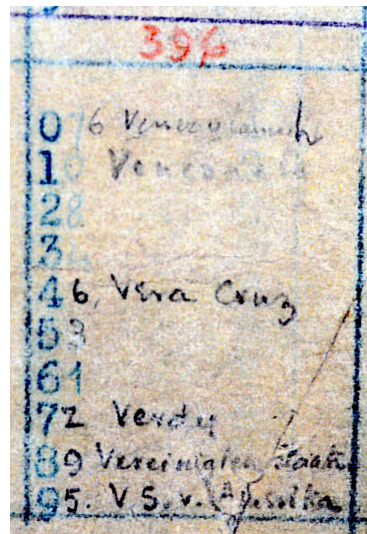
Zimmermann telegram in 13040

CLASS OF SERVICE DESIRED		<b>WESTERN UNION</b>		M.C.					
Per Day Telegram	<input checked="" type="checkbox"/>	<b>TELEGRAM</b>		3577					
Per Letter	<input type="checkbox"/>								
Per Message	<input type="checkbox"/>	NEW YORK CARLTON, PRESIDENT		JAN 8 9 1917					
Per Cable	<input type="checkbox"/>	Send the following telegram, subject to the terms on back hereof, which are hereby agreed to:							
Please show this bill to a Cashier, Agent or Operator, and the amount will be returned to you as a bill for collection.		via Galveston		JAN 8 9 1917					
GERMAN LEGATION MEXICO CITY									
130	13042	13401	8501	115	3528	416	17214	6491	11310
18147	18222	21560	10247	11518	23677	13605	3494	14936	
98092	5905	11311	10392	10371	0302	21290	5161	39695	
23571	17504	11269	18276	18101	0317	0228	17694	4473	
22224	22200	19452	21569	67893	5569	13918	8958	12137	
1333	4725	4458	5905	17166	13851	4458	17149	14471	0706
13850	12224	0929	14991	7382	15857	67893	14218	36477	
5870	17553	67893	5870	5454	16102	15217	22801	17138	
21001	17388	7446	23638	18222	0719	14331	15021	23845	
3158	23552	22096	21804	4797	9497	22464	20855	4377	
23410	18140	22260	5905	13347	20420	39689	13732	20667	
6929	5275	18507	52242	1340	22049	13339	11265	22295	
10439	14814	4178	6992	8784	7632	7357	6926	52262	11267
21100	21272	9346	9559	22464	15874	18502	18500	15857	
2188	5376	7381	98092	16127	13486	9350	9220	78056	14219
5144	2831	17520	11347	17142	11264	7667	7762	15099	9110
10482	97556	3509	3070						
BEPHSTOPFF.									
Charge German Embassy.									

Room 40: one page of code 13040 deciphered

385	391	397	403 (1)
U	U	U	U
1	1	1	1
2	2	2	2
3	3	3	3
4	4	4	4
5	5	5	5
6	6	6	6
7	7	7	7
8	8	8	8
9	9	9	9
10	10	10	10
11	11	11	11
12	12	12	12
13	13	13	13
14	14	14	14
15	15	15	15
16	16	16	16
17	17	17	17
18	18	18	18
19	19	19	19
20	20	20	20
21	21	21	21
22	22	22	22
23	23	23	23
24	24	24	24
25	25	25	25
26	26	26	26
27	27	27	27
28	28	28	28
29	29	29	29
30	30	30	30
31	31	31	31
32	32	32	32
33	33	33	33
34	34	34	34
35	35	35	35
36	36	36	36
37	37	37	37
38	38	38	38
39	39	39	39
40	40	40	40
41	41	41	41
42	42	42	42
43	43	43	43
44	44	44	44
45	45	45	45
46	46	46	46
47	47	47	47
48	48	48	48
49	49	49	49
50	50	50	50
51	51	51	51
52	52	52	52
53	53	53	53
54	54	54	54
55	55	55	55
56	56	56	56
57	57	57	57
58	58	58	58
59	59	59	59
60	60	60	60
61	61	61	61
62	62	62	62
63	63	63	63
64	64	64	64
65	65	65	65
66	66	66	66
67	67	67	67
68	68	68	68
69	69	69	69
70	70	70	70
71	71	71	71
72	72	72	72
73	73	73	73
74	74	74	74
75	75	75	75
76	76	76	76
77	77	77	77
78	78	78	78
79	79	79	79
80	80	80	80
81	81	81	81
82	82	82	82
83	83	83	83
84	84	84	84
85	85	85	85
86	86	86	86
87	87	87	87
88	88	88	88
89	89	89	89
90	90	90	90
91	91	91	91
92	92	92	92
93	93	93	93
94	94	94	94
95	95	95	95
96	96	96	96
97	97	97	97
98	98	98	98
99	99	99	99
100	100	100	100

Room 40: one section of code 13040 deciphered



A handwritten list on a grid background. At the top, the number '396' is written in red. Below it, a list of numbers and names is written in blue ink. The entries are: 076 Venezuela, 10 Venezuela, 28, 3, 46 Vera Cruz, 53, 61, 72 Verdug, 89 Vereinigten Staaten, and 95. V.S.v. Assoziation.

396
076 Venezuela
10 Venezuela
28
3
46 Vera Cruz
53
61
72 Verdug
89 Vereinigten Staaten
95. V.S.v. Assoziation

## British decipherment

- ▶ *Room 40*, the cryptanalytic unit of the British, founded in August 1914. Director: Captain Reginald Hall, later Admiral and Sir Reginald.
- ▶ The cryptanalyst Nigel de Grey can read parts of the intercepted telegram (“drop copy”) in 0075. Not readable: *Texas, New Mexico, Arizona*.
- ▶ Edward Thurstan, British legation in Mexico City, bribed an operator at the post office. De Grey writes: *Although we had the 13040 version and knew Eckardt had no 7500 book, without disclosing our drop copy source, we could not produce it. Nor could we prove that the telegram had actually been delivered in Mexico to the German Legation and had not been faked in London . . . How we succeeded in stealing the copy I never knew but money goes a long way in Mexico and steal it we did.*

## British decipherment

- ▶ Room 40 receives the 13040 copy, “el resto fue sencillo”: de Grey decipheres it, Hall gives the solution to the US ambassador Walter Page in London, who passes it to US President Woodrow Wilson.
- ▶ David Kahn: “the greatest intelligence coup of all times”.
- ▶ Published in newspapers on 1 March, including *EI Universal*. Public outcry in the US, Congress declares war on the Central Powers on 6 April 1917.
- ▶ 11 November 1918: victory of the Entente, followed by the Treaty of Versailles.
- ▶ Challenge to historians: contradictory, erroneous, and intentionally false statements by participants and in the literature.

Portada El Universal del 1 marzo de 1917





Portada El Universal del 1 marzo de 1917

**EL UNIVERSAL**  
MAÑANA

DE 1917

CINE AMERICA  
El mejor teatro de  
premieras  
**"EL FELICITO AMARILLO"**  
El sábado, la película  
más emocionante comienza.  
Argumento original.

---

NUMERO 152

## Guerra Entre Mexico, Alemania y Japon

### Se Publica una Copia de las Instrucciones Enviadas por Zimmerman Ministro de Negocios Extranjeros a Von Eckardt Representante Teuton en Mexico

**PRENSA AMERICANA.** Según este plan, perfectamente com-  
bato con la Alemania victoriosa, en  
Washington, febrero 23.—El el que la fuerza de Eckardt.  
Frente Asociada está en actitud El arreglo de las instrucciones se  
de revelar que Alemania, impondría el al ministro plenipotenciario de  
para electricos. Alemania ante el gobierno del señor  
con su campaña submarina sin restric- Carranza, von Eckardt, quien reside  
ción y contando con sus contorne- en la ciudad de México, y quien, cir-  
losa prima. co a México, el 24 de febrero, fecha discutida de entre próximas ga-  
de la guerra, el 24 de febrero, día de las instrucciones de Eckardt, que  
de la guerra, el 24 de febrero, día de las instrucciones de Eckardt, que  
de la guerra, el 24 de febrero, día de las instrucciones de Eckardt, que

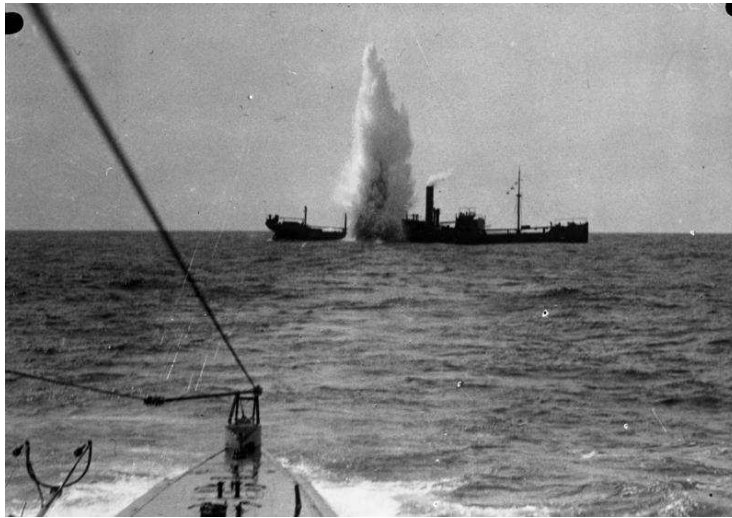
La primera que tenía que hacer von Eckardt, por El gobierno alemán toda de guerra  
Eckardt, era procurar que el gobier- a México una situación completa-  
no de México se pusiera al habla con mente, la guerra no la que realmente en-  
el del Japón para atraerlo a lado- los momentos viaja con rumbo a su  
de la guerra, el 24 de febrero, día de las instrucciones de Eckardt, que  
de la guerra, el 24 de febrero, día de las instrucciones de Eckardt, que  
de la guerra, el 24 de febrero, día de las instrucciones de Eckardt, que

**El Gobierno Americano Adquiere una Copia de la Nota de Zimmerman a Von Eckardt**  
Una copia de la nota enviada por rra, y juntos estaremos a la hora de bajo su propia iniciativa, se comen-  
al Ministro de Relaciones. Zimmer- la paz. Nuestra le damos un amplia que con el gobierno del Japón, judi-  
man al Ministro von Eckardt, está cado que se adhiera a este plan, al  
en poder del gobierno americano, y mismo tiempo enviamos México como  
dice testadamente. mediador entre el Japón y nuestro  
país.  
"Con fecha primera de febrero, que Arizona y Texas. Los detalles se de-  
lancez militar, nuestra campaña sub- que en New York, y gobierno de  
marina del territorio. A propósito de México, el 24 de febrero, día de las instrucciones de Eckardt, que  
de la guerra, el 24 de febrero, día de las instrucciones de Eckardt, que  
de la guerra, el 24 de febrero, día de las instrucciones de Eckardt, que

## Consequences

- ▶ Von Eckardt presents the German offer to the Mexican government on 20 February 1917. Mexican President Venustiano Carranza rejects it on 14 April: “era una locura pensar que Alemania realmente iba a poder cumplir con esa oferta de ayuda militar” (Felipe Ávila).
- ▶ German U-boats sink many ships, but the ground troops are exhausted and cave in after the massive US intervention.

SM U 35 torpedoes HMS Maplewood in April 1917



## Consequences

- ▶ Zimmermann admits authorship of the telegram in the German parliament on 3 March 1917.
- ▶ Strong criticism by various Members: Zimmermann *has played a brilliant argument into Wilson's hand to rally the American people in unison around him. Zimmermann: I share the opinion that the Mexicans are unable to wage war successfully against the United States . . . My intention was to convince Carranza to start marching as soon as possible . . . It was important to me to avoid exposing our faithful field-gray uniforms to new enemies . . . In this war, moral has been filed away . . . Mexico has no weapons in the modern sense, but the irregular gangs are sufficiently supplied with weapons to stir up discomfort and unrest in the border states of America.*
- ▶ Why did Zimmermann admit the telegram's origin? My speculative answer: because he did not see anything wrong with it.

## French plans 1915



## Aftermath of the First World War

- ▶ Austria-Hungary is cut up into various countries. Poland is created as an independent state and given parts of Germany and Russia; France regains Alsace and Lorraine and controls some parts of Germany in the west for several years.
- ▶ A democratic republic is created in Germany (*Weimar Republic*), but weakened by the compensation payments according to the Versailles treaty and massive internal strife by extremists. Ultimately, this gives rise to a Nazi government and the next disaster.

An 8-year old Afghan refugee in Bonn writes in December  
2016:

I wish that sometime there will be no war in the world anymore.