Desarrollo de la criptografía Guerras mundiales—hasta ahora

Universidad de la Républica
Montevideo, Uruguay

Joachim von zur Gathen
Bonn, Alemania

The Zimmermann telegram of 1917, overview

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

Prehistory

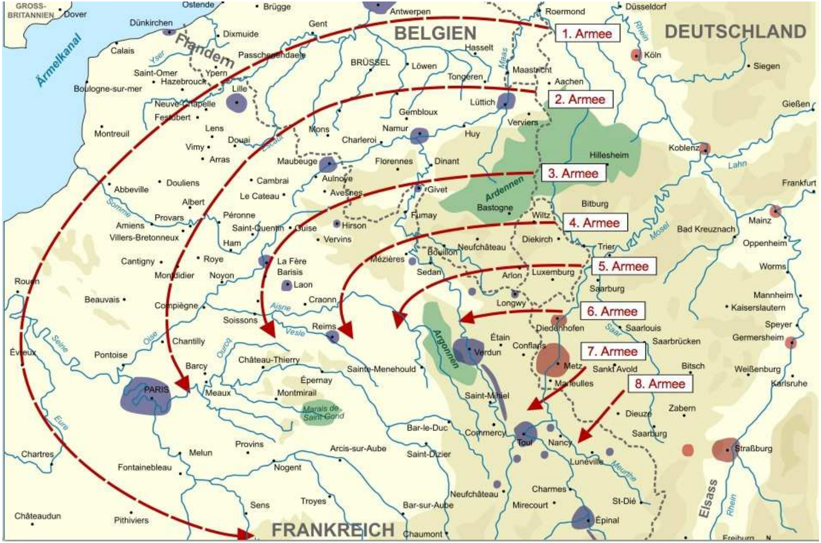
Mexican-American War 1846–1848: USA gain large tracts of Mexican territory, *Alta California* and *Santa Fe de Nuevo México* (including California, Texas, Arizona, New Mexico).

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

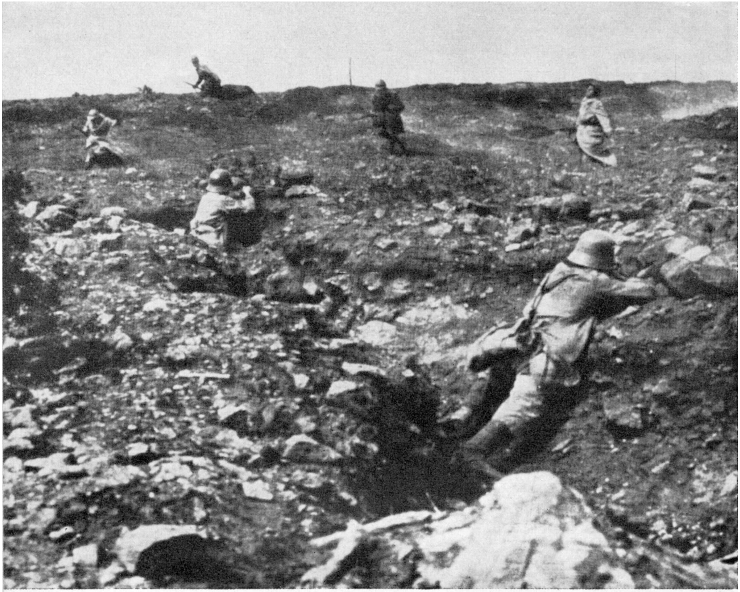
The First World War (in the West)

- 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.

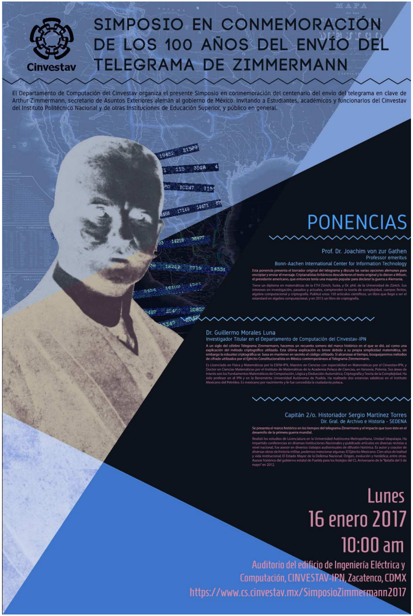
The Zimmermann telegram, Januar 1917

- 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 envio del telegrama en clave de Arthur Zimmermann, secretario de Asuntos Exteriores alemán al gobierno de México. Invitando a Estudiantes, académicos y funcionarios del Cinvestav del Instituto Politécnico Nacional y de otras Instituciones de Educación Superior, y público en general.

PONENCIAS

Prof. Dr. Joachim von zur Gathen
Professor emeritus
Bonn-Aachen International Center for Information Technology

Esta ponencia presenta el borrador original del telegrama y discute las varias opciones alemanes para encriptar y enviar el mensaje. Criptanalistas británicos descubrieron el texto original y lo dieron a Wilson, el presidente americano, que entonces tenía una mayoría popular para declarar la guerra a Alemania.

Tiene un diploma en matemáticas de la ETH Zürich, Suiza, y Dr. phil. de la Universidad de Zürich. Sus intereses en investigación, pasados y actuales, comprenden la teoría de complejidad, cuerpos finitos, algebra computacional y criptografía. Publicó unos 150 articulos científicos, un libro que llegó a ser el estandard en algebra computacional, y en 2015 un libro de criptografía.

Dr. Guillermo Morales Luna
Investigador Titular en el Departamento de Computación del Cinvestav-IPN

A un siglo del célebre Telegrama Zimmermann, hacemos un recuento somero del marco histórico en el que se dió, así como una explicación del método criptográfico utilizado. Esta última explicación es breve debido a su propia simplicidad matemática, sin embargo la robustez criptográfica se basa en mantener en secreto el código utilizado. Si alcanzase el tiempo, bosquejaremos métodos de cifrado utilizados por el Ejército Constitucionalista en México contemporáneos al Telegrama Zimmermann.

Es Licenciado en Física y Matemáticas por la ESFM-IPN, Maestro en Ciencias con especialidad en Matemáticas por el Cinvestav-IPN, y Doctor en Ciencias Matemáticas por el Instituto de Matemáticas de la Academia Polaca de Ciencias, en Varsovia, Polonia. Sus áreas de interés son los Fundamentos Matemáticos de Computación, Lógica y Deducción Automática, Criptografía y Teoría de la Complejidad. Ha sido profesor en el IPN y en la Benemérita Universidad Autónoma de Puebla. Ha realizado dos estancias sabáticas en el Instituto Mexicano del Petróleo. Es mexicano por nacimiento y le fue concedida la ciudadanía polaca.

Capitán 2/o. Historiador Sergio Martínez Torres
Dir. Gral. de Archivo e Historia - SEDENA

Se presenta el marco histórico en los tiempos del telegrama Zimermann y el impacto que tuvo éste en el desarrollo de la primera guerra mundial.

Realizó los estudios de Licenciatura en la Universidad Autónoma Metropolitana, Unidad Iztapalapa. Ha impartido conferencias en diversas Instituciones Nacionales y publicado artículos en diversas revistas a nivel nacional, fue asesor en diversos trabajos audiovisuales de difusión histórica. Es autor y coautor de diversas obras de historia militar, podemos mencionar algunas: El Ejército Mexicano. Cien años de lealtad y vida institucional; El Estado Mayor de la Defensa Nacional. Origen, evolución y heráldica; entre otras. Asesor histórico del gobierno estatal de Puebla para los festejos del CL Aniversario de la "Batalla del 5 de mayo" en 2012.

Lunes
16 enero 2017
10:00 am

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

Sending the telegram

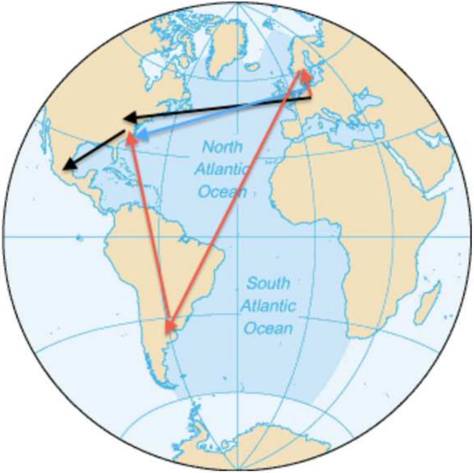
Codebooks for encryption:

- 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.

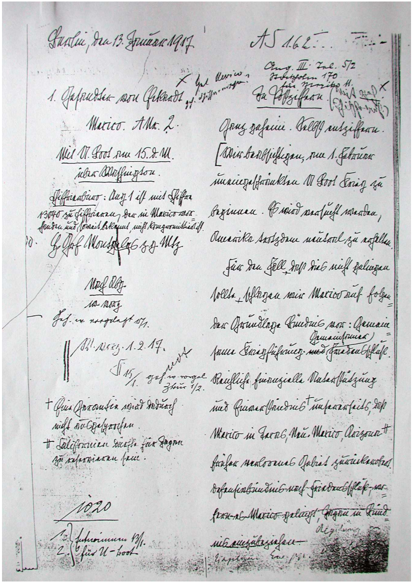
The British *HMS Telconia* had cut all transatlantic cables out of Germany on 5 August 1914. The Germans had the following four options for **transmission**:

- 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



Berlin, den 13. Januar 1917

AS 162

Ang. III. Tel. 572
Stockholm 170
für Mexico 11.

1. Gesandter von Eckardt × [illegible]

Mexico. A.No. 2.

Mit U-Boot am 15. d. M.
über Washington.

Chiffrierbüro: Anl. 1 ist mit Chiffre 13040 zu chiffrieren, der in Mexico vorhanden und, soweit bekannt, nicht kompromittiert ist.

G. Graf Montgelas z. g. Mtz

Nach Abg.
an Abg.

Geh. u. vorgelegt 15/1.

Abl. Wegz. 1.2.17.

15/1. geh. u. vorgel. [illegible] 1/2.

+ Eine Garantie wird dadurch nicht übernommen.

++ Californien dürfte für Japan zu reservieren sein.

1020

1. 2. } befördert 13/1. für U-boot

In Postziffern (nicht Geheimziffer) ×

Ganz geheim. Selbst entziffern.

[Wir beabsichtigen, am 1. Februar uneingeschränkten U-Boot Krieg zu beginnen. Es wird versucht werden, Amerika trotzdem neutral zu erhalten. Für den Fall, dass dies nicht gelingen sollte, schlagen wir Mexico auf folgender Grundlage Bündnis vor: Gemeinsame Kriegführung. ~~und~~ Gemeinsamer Friedensschluss. Reichliche finanzielle Unterstützung und Einverständnis+ unsererseits, dass Mexico in Texas, Neu-Mexico, Arizona++ früher verlorenes Gebiet zurückerobert. ~~Defensivbündnis nach Friedensschluss, wenn es Mexico gelingt, Japan in Bund mit einzubeziehen.~~

Regierung [illegible]

The Zimmermann telegram in English

Most secret. Decipher yourself.

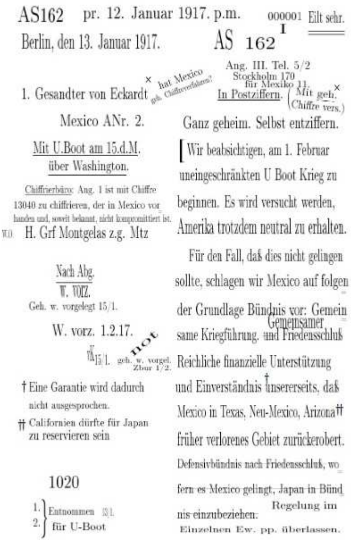
We intend to begin on the first of February unrestricted submarine warfare. We shall endeavour in spite of this to keep the United States of America neutral.

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 Eilt sehr.

Berlin, den 13. Januar 1917. AS 162 I

1. Gesandter von Eckardt × hat Mexico geh. Chiffreverfahren?

Mexico ANr. 2.

Mit U.Boot am 15.d.M.
über Washington.

Chiffrierbüro: Ang. 1 ist mit Chiffre 13040 zu chiffrieren, der in Mexico vorhanden und, soweit bekannt, nicht kompromittiert ist.

W.O. H. Grf Montgelas z.g. Mtz

Nach Abg.
W. vorz.

Geh. w. vorgelegt 15/1.

W. vorz. 1.2.17.

not

V/VA 15/1. geh. w. vorgel. Zbur 1/2.

† Eine Garantie wird dadurch nicht ausgesprochen.

†† Californien dürfte für Japan zu reservieren sein

1020

1.
2. } Entnommen 13/1. für U-Boot

Ang. III. Tel. 5/2
Stockholm 170
für Mexiko 11.
In Postziffern. (Mit geh. × Chiffre vers.)

Ganz geheim. Selbst entziffern.

[Wir beabsichtigen, am 1. Februar uneingeschränkten U Boot Krieg zu beginnen. Es wird versucht werden, Amerika trotzdem neutral zu erhalten.

Für den Fall, daß dies nicht gelingen sollte, schlagen wir Mexico auf folgender Grundlage Bündnis vor: Gemeinsame Kriegführung. ~~und Friedensschluß~~ Gemeinsamer Friedensschluß Reichliche finanzielle Unterstützung und Einverständnis †unsererseits, daß Mexico in Texas, Neu-Mexico, Arizona†† früher verlorenes Gebiet zurückerobert. ~~Defensivbündnis nach Friedensschluß, wofern es Mexico gelingt, Japan in Bündnis einzubeziehen.~~ Regelung im Einzelnen Ew. pp. überlassen.

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.

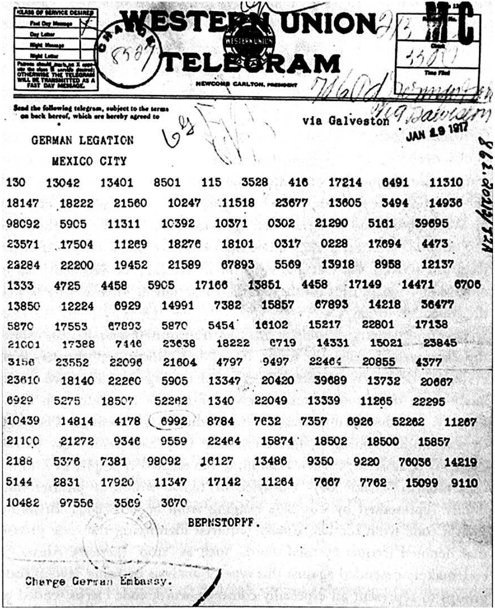
Transmission and interception

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	
Fast Day Message	✓
Day Letter	
Night Message	
Night Letter	

Patrons should mark an X opposite the class of service desired; OTHERWISE THE TELEGRAM WILL BE TRANSMITTED AS A FAST DAY MESSAGE.

CHARGE 8307

WESTERN UNION TELEGRAM

NEWCOMB CARLTON, PRESIDENT

Receiver's No. MC

Check 3300

Time Filed

Send the following telegram, subject to the terms on back hereof, which are hereby agreed to

via Galveston

JAN 19 1917

GERMAN LEGATION

MEXICO CITY

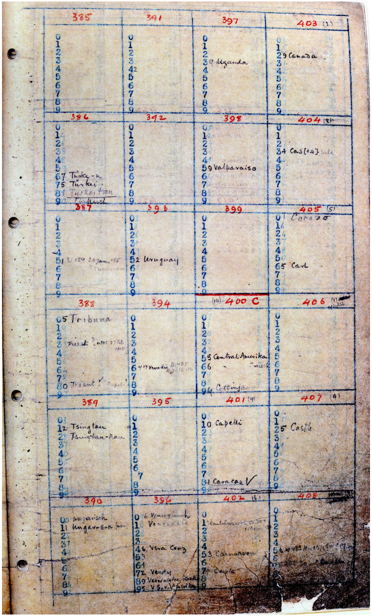
130 13042 13401 8501 115 3528 416 17214 6491 11310
18147 18222 21560 10247 11518 23677 13605 3494 14936
98092 5905 11311 10392 10371 0302 21290 5161 39695
23571 17504 11269 18276 18101 0317 0228 17694 4473
22284 22200 19452 21589 67893 5569 13918 8958 12137
1333 4725 4458 5905 17166 13851 4458 17149 14471 6706
13850 12224 6929 14991 7382 15857 67893 14218 36477
5870 17553 67893 5870 5454 16102 15217 22801 17138
21001 17388 7446 23638 18222 6719 14331 15021 23845
3156 23552 22096 21604 4797 9497 22464 20855 4377
23610 18140 22260 5905 13347 20420 39689 13732 20667
6929 5275 18507 52262 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 76036 14219
5144 2831 17920 11347 17142 11264 7667 7762 15099 9110
10482 97556 3569 3670

BEPNSTOPFF.

Charge German Embassy.

862.20212/82A

Room 40: one page of code 13040 deciphered



385

386
67 Türke-n
75 Türkei
81 Türkestan
90 Türkisch

387
51 W 024 20 Jan. -15 Tucuman

388
05 Tribuna
3 Triest ? W 32C 27 Feb 1915
80 Trient ✓ Tripoli

389
12 Tsingtau
2 Tsingtau-Kau

390
00 ungarisch
11 Ungar-s-n (man)

391
42

392

393
52 Uruguay

394
6 Verdun B.435 27-12-14

395
7

396
06 Venezolanisch
1 Venezuela
46 Vera Cruz
72 Verdun
89 Vereinigten Staaten
95 V.S.v. Amerika

397
39 Uganda

398
59 Valparaiso

399

(10) 400 C
55 Central Amerika
66 - -isch
94 Cettinje

401 (4)
10 Capelli
81 Caracas ✓

402 (3)
1 [illegible]
53 Carnarvon
7 Casela

403 (2)
29 Canada

404 (8)
34 Cas[+4]

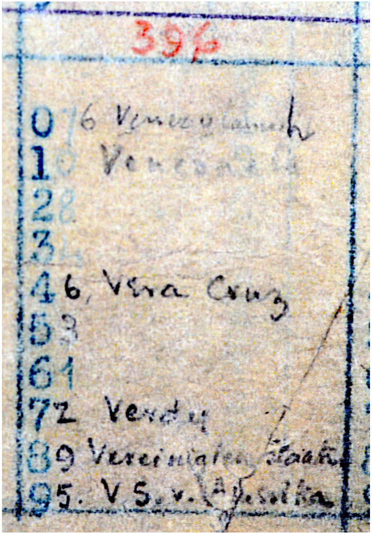
405 (5)
01 Carazo
65 Carl

406 (1)

407 (9)
25 Castle

408
56 W 433 [illegible]

Room 40: one section of code 13040 deciphered



396

076 Venezolanisch
10 Venezuela
28
34
46, Vera Cruz
53
61
72 Verdun
89 Vereinigten Staaten
95. V. S. v. Amerika

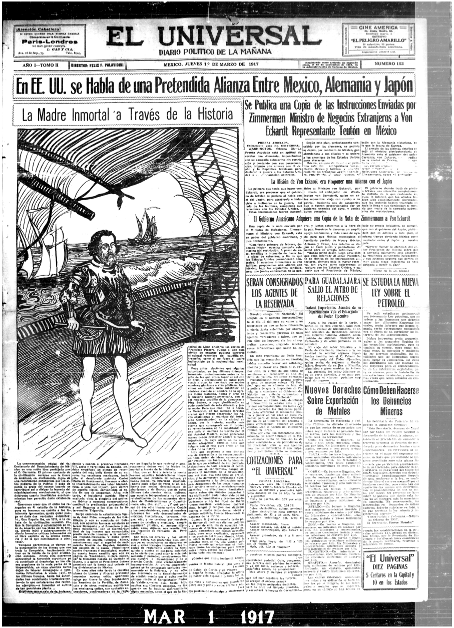
British decipherment

- *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 deciphers 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 *El 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



EL UNIVERSAL
DIARIO POLITICO DE LA MAÑANA

AÑO I—TOMO II | DIRECTOR: FELIX F. PALAVICINI | MEXICO, JUEVES 1º DE MARZO DE 1917 | Registrado como artículo de segunda clase, el 12 de noviembre de 1916, en la Administración de Correos de México. | NUMERO 152

En EE. UU. se Habla de una Pretendida Alianza Entre Mexico, Alemania y Japón

Se Publica una Copia de las Instrucciones Enviadas por Zimmerman Ministro de Negocios Extranjeros a Von Eckardt Representante Teutón en México

PRENSA ASOCIADA.
Exclusivamente para EL UNIVERSAL.

WASHINGTON, febrero 28.—La Prensa Asociada está en aptitud de revelar que Alemania, imponiéndose con su campaña submarina sin restricción y contando con sus consecuencias, propuso una alianza con el Japón y la República Mexicana para declarar la guerra a los Estados Unidos si [illegible] permanecían neutrales.

Según este plan, perfectamente concebido por los alemanes, se pediría al Japón, por conducto de México, que abandonara a sus aliados y se uniera a los enemigos de los Estados Unidos para atacarles.

México, en caso de llevar a la práctica este plan, reconquistaría Texas, Nuevo México y Arizona, y [illegible] recibiría un tremendo apoyo financiero, repartiéndo, al mismo tiempo, el botín con la Alemania victoriosa, en lo que le tocara de Europa.

El arreglo de los últimos detalles se dejó al ministro plenipotenciario de Alemania ante el gobierno del señor Carranza, von Eckardt, que radica en la ciudad de México, [illegible] con fecha [illegible] recibió amplias [illegible] cartas [illegible] Relaciones Exteriores [illegible] Zimmermann, sobre el particular.

La Misión de Von Eckardt era Proponer una Alianza con el Japón

Lo primero que tenía que hacer von Eckardt, era procurar que el gobierno de México se pusiera al habla con el del Japón, para atraérselo e inducirlo a inclinarse en la guerra, del lado de los teutones, rompiendo sus relaciones con los Estados Unidos.

Estas instrucciones fueron transmitidas al Ministro von Eckardt, por conducto del embajador en Washington von Bernstorff, quien en estos momentos viaja con rumbo a su patria, haciendo uso de pasaportes que le fueron proporcionados por un gobierno enemigo del suyo, y contra quien conspira.

El gobierno alemán trató de pintar a México una situación completamente distinta de la que realmente era, pues le informó que los aliados habían sido completamente derrotados, que los teutones habían triunfado en toda la línea y que dominaban el mundo por medio de la campaña submarina sin restricciones.

El Gobierno Americano Adquiere una Copia de la Nota de Zimmermann a Von Eckardt

Una copia de la nota enviada por el Ministro de Relaciones, Zimmermann al Ministro von Eckardt, está en poder del gobierno americano, y dice textualmente.

"Con fecha primero de febrero, debemos iniciar nuestra campaña submarina sin restricción. A pesar de esto, tenemos la intención de hacer toda clase de esfuerzos, a fin de que los Estados Unidos permanezcan neutrales. Si nuestras intenciones se ven fallidas, proponemos una alianza con México, bajo las siguientes condiciones: que juntos entraremos en la guerra, y juntos estaremos a la hora de la paz. Nosotros le daremos un amplio apoyo económico, y toda clase de ayuda para que México reconquiste el territorio perdido de Nuevo México, Arizona y Texas. Los detalles se dejan al buen juicio y patriotismo de usted para el arreglo definitivo."

"Queda usted desde luego advertido que debe informar al señor Presidente de México de las instrucciones anteriores, siempre bajo la mayor reserva, tan pronto como sobrevenga la ruptura con los Estados Unidos, y sugerir que el Presidente de México, bajo su propia iniciativa, se comunique con el gobierno del Japón, pidiéndole que se adhiera a este plan, al mismo tiempo sirviendo México como mediador entre el Japón y nuestro país.

"Sírvase llamar la atención del señor Presidente de México sobre que la campaña submarina está obteniendo resultados sumamente halagadores y que estamos seguros que dentro de muy pocos meses Inglaterra se verá obligada a hacer la paz."

(Sigue en la 5a. plana.)

La Madre Inmortal ´a Través de la Historia

La conmemoración oficial del 4o. Centenario del Descubrimiento de México es una noble idea prohijada por el C. Carranza. El primer contacto de la civilización europea con la tierra de Anáhuac, es, ciertamente, digno de una recordación consagrada por los altos poderes de la Patria! y sube de punto lo grato del suceso cuando se contribuye así a disipar la leyenda del mischihispanismo revolucionario, al que dolorosos cuanto inevitables acontecimientos han parecido darle existencia real.

Queremos creer que ni entre los rezagados en el estudio de la historia, pues no tenemos en cuenta a los totalmente ignorantes, queda quien ponga en duda dos verdades evidentes: 1o., Que España iba, en 1517, a la cabeza de la civilización mundial. 2o., Que la Conquista y colonización se hizo de acuerdo con las ideas de la época, siendo inútil y soberanamente ridículo formular críticas informadas en el libre espíritu de la última centuria y de la que comenzamos a atravesar.

Tampoco perderemos el tiempo en la ponderación de los bienes que nos trajo la Conquista, haciéndonos entrar en la órbita de la gran civilización europea. Ahora sólo queremos aprovechar la favorable coyuntura para contribuir al desarraigo en las clases populares de la mala yerba de la hispanofobia, en cuya siembra nunca dejan de laborar demagogos o ignorantes folicularios. A veces, ¡ay!, en los últimos tiempos, hasta las autoridades han contribuído irreflexivamente—de lo que señalaremos dos recientes ejemplos,—a fomentar el cultivo de tan perniciosa planta...

Explícase que a raíz de la Independencia y cuando el proterve Fernando VII, azote y vergüenza de España, andaba empeñado en planes de reconquista del más bello florón de su corona, los escritores mexicanos, inclusopito el desaforado patriota Carlos María de Bustamante, llevasen a efecto incansablemente una labor hispanófoba, a toda luz injusta, pero dentro de aquella lógica, conveniente al noble fin que se proponían. Años más tarde, el incipiente partido liberal exaltado, vista la simpatía del gobierno ibérico a nuestros conservadores, continuó la predicación antiespañola; y así llegamos a los días de la Intervención Tripartita.

Surge entonces la caballeresca figura de Juan Prim, marqués de los Castillejos, y con su conducta en Soledad, con aquellas famosas epístolas al tercer Bonaparte y al financiero y político Salamanca, con el reembarque final de las huestes que comandara, prestó servicio inmenso a la concordia hispano-mexicana. Y como grato recuerdo de aquella luctuosa época, mencionemos aquí al español de nacimiento Nicolás de Régules, incansable paladín de la causa republicana contra franceses é imperiales; modesto cuanto bravo caudillo que con su página de Tacámbaro, hiciera palidecer la tremenda hazaña de Guzmán el Bueno, y a quien el Presidente Juárez premiara con la banda azul celeste de los divisionarios de México.

En vano años más tarde la cáustica pluma de Llanos y Alcaraz pretendió encender nuevos odios, queriendo echar por tierra la obra bienhechora de Anselmo de la Portilla, de Zaracoie y de otros modestos escritores: los mexicanos cultos, con contadas excepciones, confirmadoras de la regla, ven en España lo que racional y amorosamente deben ver: la Madre Inmortal a través de la Historia.

Hoy, que en frío y serena la mente leemos aquellas lucubraciones hispanófobas, nos produce tal lectura, ya honda pena, ya hilaridad desatada. ¿Cómo pudo dejar de verse ni un momento que somos descendientes de aborígenes y de iberos; que de estos últimos data nuestra única cultura; que nuestra independencia no fue una reivindicación de los supuestos derechos de Moctezhomas y Cuauhtemocs, etc., etc., etc? .... ¿Y qué pensar de ese odio insano contra Cortés y los conquistadores, como si nosotros fuéramos tan sólo descendientes de mexicas, tlaxcaltecas, tarascos, mayas, etc., y no corriera por nuestras venas de criollos o mestizos, sangre española? ¡Risible, sí, aunque explicable, como dijimos, nos resulta hoy esa negación de verdades de Pero Grullo!...

Con todo, los errores y los odios echan raíces tan profundas que, aunque ya no escuchamos en discursos ni en otros trabajos literarios, las tiradas de reglamento contra la Conquista o contra el gobierno colonial, es lo cierto que, para citar lo más culminante y pasmoso, consideremos héroe nuestro a Cuauhtemoc y no a Hernán Cortés, cosa verdaderamente incomprensible. Al último emperador azteca se ha consagrado suntuoso monumento en la Reforma, y no sólo don Hernando no lo tiene—homenaje de sentido común que el culto pueblo chileno rindió al Conquistador Pedro de Valdivia,—sino que, hasta hoy, ocultos sus fúnebres despojos, no los guarda en la basílica metropolitana digno mausoleo, como el que en la Catedral de Lima encierra los restos de Francisco Pizarro. ¡Como si con este olvido de encargo pudiera borrarse el colosal renombre del caudillo extremeño; como si no fuera el padre indiscutible de la nacionalidad mexicana!

Poco antes decíamos que algunas autoridades, en los últimos tiempos, formando probablemente entre la legión de los que creen tapar el sol con un dedo, y desvistiendo un santo para vestir a otro, la han dado por mudar nombres gloriosos a vías públicas. Así, vimos en nuestra urbe substituir en céntrica avenida el nombre de la egregia Reina Católica, honra y prez de la historia hispano-americana, con el del modesto caudillo de la democracia Pino Suárez, a cuya glorificación se pudo contribuir de más discreto y justo modo. Pero qué más: ¡en la heróica Veracruz, en las mismas tórridas arenas que vieran desarbolar las naves castellanas al mandato del intrépido Conquistador; en la ciudad en donde, por la historia, resulta más eterna que consagrada en el bronce su remembranza, se ha substituído en una calle el nombre de Cortés por el del Apóstol Madero, cuyos generosos manes deben protestar contra tamaña injusticia: él, cuya gloria no ha menester atropellos edilicios para que fulgure con el más puro brillo en los cielos de la Patria!

Hoy que asistimos a una dichosa era de reparación y de reconstrucción en todo orden de ideas, comencemos por respetar los fueros de la historia, en lo que ya contiene de res judicata. Aplaudimos de todo corazón el centenario que se conmemora, porque así prueba el Gobierno de la Revolución, una vez más, que está libre de prejuicios, y lo demuestra celebrando nuestro nacimiento a la civilización europea. Juzguemos de las cosas humanas con criterio sereno y verdaderamente científico; no discutamos fantásticamente sobre que nuestro despertar a esa civilización pudo haber sido de mejor y más humanitario y previsor modo. Queramos o no, los hijos de Iberia fueron nuestros verdaderos padres: alma, lengua y religión nos dejaron; buenos o malos estos dones, viven y vivirán mientras flamee libremente la bandera de la Patria.

Cuando la gloriosa España tenía poco tiempo de lucir sus divinos colores, y al par de ella, las de nuestras hermanas de América, un gran poeta español, dementado por pasión avasalladora, pero muy explicable, apostrofó a los pueblos del Nuevo Mundo. Injusta vibró la lira al ensayar el vuelo la estrofa; mas, al fin, una verdad palmaria remató gallardamente el inspirado trozo. Lo escogemos para cerrar estas líneas, porque ese remate lo sintetiza todo noblemente:

¡Gentes que alzáis incógnita bandera
contra la Madre Patria! ¡En vano el mundo
de Colón, de Cortés y de Pizarro
a España intenta arrebatar la gloria
de haber sido español! ¡Jamás las leyes,
los ritos y costumbres que guardaron
entre oro y plata y entre aroma y [illegible]
los pueblos de Atahualpa y Moctezuma
y vuestros mismos padres conquistaron
restablecer podréis! Odio, venganza,
nos juraréis cual pérfidos hermanos,
y ya del indio, esclavos o señores,
españoles seréis, no americanos!
Más ahora y siempre el argonauta osado
que del mar desafiare los furores,
al arrojar el áncora pesada
en las playas antípodas distantes,
verá la cruz del Gólgota plantada,
y escuchará la lengua de Cervantes!...

SERAN CONSIGNADOS LOS AGENTES DE LA RESERVADA

Nuestro colega "El Nacional," dió acogida en el número correspondiente al día 15 del mes en curso a un reportazgo en que se hace referencia a cierta junta celebrada por abarroteros y cantineros quejosos de unos agentes, verdaderos o falsos, que según ellos les imponen sin ton ni son multas excesivas, alegando muchas veces infracciones que nadie ha cometido.

En este reportazgo se decía también que los comerciantes en cuestión habían resuelto cerrar sus establecimientos y elevar una queja al C. Primer Jefe, en virtud de que todos se complacen en reconocer el alto espíritu de justicia del señor Carranza.

Probablemente este asunto motiva la nota de nuestro colega "El Pueblo," que en su número de hoy, da la noticia de que la Inspección de Policía va a consignar al Gobierno del Distrito un artículo calumnioso y difamatorio de "El Nacional."

Nosotros no vemos nada delictuoso ni difamatorio en señalar ante la autoridad correspondiente, las faltas que se dice cometen los empleados públicos para averiguar si realmente existen y poner en tal caso el justo remedio; pero de todos modos creemos que no es al Gobierno del Distrito a quien corresponde conocer de estos asuntos, sino al Agente del Ministerio Público en turno.

Debe ser esta una lamentable equivocación. El señor Coronel de la Mata—estamos ciertos de ello—no ha de haber consignado a los periodistas de "El Nacional," sino a sus agentes, para que se investigue si son culpables y castigarlos como se merecen.

COTIZACIONES PARA "EL UNIVERSAL"

PRENSA ASOCIADA.
Exclusivamente para EL UNIVERSAL.

NUEVA YORK, febrero 28.—La cotización de metales y productos agrícolas durante el día de hoy, ha sido la siguiente:

Plata en barras, dól. 0.77 por onza, Standard.

Pesos mexicanos, dól. 0.58 5/8.

Cobre electrolítico, quieto, nominal.

Cobre electrolítico para entrega en abril-junio, de 33 a 35 cent. libra.

Algodón "middling," dól. 17.00 el quintal.

Azúcar mascabado, firme.

Azúcar melaza, dól. 4.40 el quintal.

Azúcar centrifugado, dól. 5.29.75 el quintal.

Azúcar granulado, de 7 a 8 cent. la libra.

Trigo para mayo, de 1.12 a 1.25 dól. el "bushel."

Maíz, dól. 1.02 el "bushel."

PARA GUADALAJARA SALIO EL MTRO DE RELACIONES

Tratará Importantes Asuntos de su Departamento con el Encargado del Poder Ejecutivo

Ayer, a las cuatro de la tarde, a bordo de un tren especial, salió rumbo a la ciudad de Guadalajara, el señor Ministro de Relaciones Exteriores, General Cándido Aguilar, acompañado de algunos miembros del Protocolo y de otras personas de su amistad.

El viaje del señor Ministro a la Perla de Occidente, obedece a la necesidad de acordar algunos importantes asuntos con el C. Primer Jefe, Encargado del Poder Ejecutivo, quien acaba de regresar a Guadalajara después de su jira a Etzatlán, Ahualulco y otros pueblos de Jalisco.

La ausencia del señor Ministro será de corta duración, y es muy probable que el viernes próximo esté aquí de regreso.

Nuevos Derechos Sobre Exportación de Metales

La Secretaría de Hacienda y Crédito Público, ha dictado el acuerdo de que las cuotas de exportación que deben regir durante el presente mes de marzo, para los minerales y metales, sean las siguientes:

ORO.—En barras o lingotes, [illegible] y seis pesos cincuenta centavos por kilo. En Minerales y concentrados, noventa y tres pesos treinta y tres centavos por kilo.

PLATA.—En barras o lingotes, dos pesos quinientos diecisiete milésimos de pesos por kilo. En Minerales y concentrados, tres pesos quinientos veintitrés milésimos de peso, por kilo.

COBRE.—En barras o lingotes, siete centavos, doscientos cinco milésimos de centavo por kilo. En Minerales y concentrados, ocho centavos seiscientos cuarenta y seis milésimos de centavo por kilo.

PLOMO.—En barras o lingotes, ochocientos cincuenta y ocho milésimos de centavo por kilo. En Minerales y concentrados, un centavo ciento cuarenta y cinco milésimos de centavo por kilo.

ESTAÑO.—En barras o lingotes, seis centavos, setecientos noventa y nueve milésimos de centavo por kilo. En Minerales y concentrados, ocho centavos, treinta y nueve milésimos de centavo por kilo.

ZINC.—En barras o lingotes, un centavo, un milésimo de centavo por kilo. En Minerales y concentrados, un centavo trescientos treinta y cuatro milésimos de centavo por kilo.

ANTIMONIO.—En barras o lingotes, quinientos veinticinco milésimos de centavo por kilo. En Minerales y concentrados, setecientos sesenta y seis milésimos de centavo por kilo.

TUNGSTENO.—En minerales y concentrados, doce centavos, doscientos diecisiete milésimos de centavo por kilo.

GRAFITO.—Amorfo, doscientos seis milésimos de centavo por kilo. Refinado, un centavo, quinientos ochenta y cuatro milésimos de centavo por kilo.

Las cuotas anteriores asentadas, son netas y su aplicación se hará sobre los pesos íntegros de los minerales y metales que se exporten, pues en su cálculo se han tenido en cuenta las consideraciones de la circular número 144, girada en diciembre último, por la Secretaría de Hacienda y las disposiciones económicas de la propia Secretaría, relativas a minerales de plomo.

SE ESTUDIA LA NUEVA LEY SOBRE EL PETROLEO

Se está estudiando activamente una interesante Ley petrolera, que se refiere a los impuestos que deberán pagar las diferentes Empresas locales, según informes que hemos logrado, serán enteramente equitativos con el objeto de no perjudicar los intereses de los concesionarios.

Dichos impuestos serán proporcionales a las ganancias líquidas de las compañías explotadoras, pues se tendrán en cuenta, entre otras muchas cosas, la extensión y condición de los terrenos explotados, las facilidades que las Compañías tengan para lograr su explotación, así como las dificultades con que muchas veces tropiezan para el almacenamiento de las substancias explotadas, para su acarreo, para la instalación de sus estaciones terminales, y otras varias cosas que serán tomadas en consideración.

Cómo Deben Hacerse los Denuncios Mineros

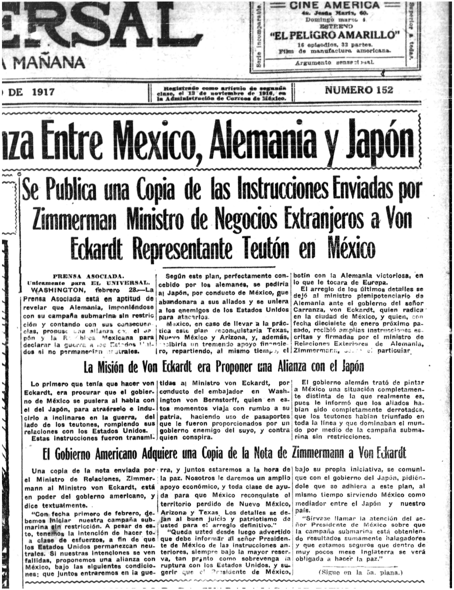
La Secretaría de Fomento ha expedido la siguiente circular:

"Esta Secretaría, deseosa de impulsar por todos los medios posibles el desarrollo de la industria minera, estableció el precedente de conceder a terceras personas el derecho de preferencia para denunciar fundos cuyos concesionarios no estuvieran al corriente en el pago del impuesto minero, siempre que previamente se hubiese acreditado ante esta misma Secretaría que se hicieron gestiones ante la de Hacienda, para obtener la declaratoria de caducidad del título del fundo respectivo, derecho que debería ejercitarse inmediatamente después de que, conforme a la ley, se considerase libre el terreno ocupado por el fundo en cuestión; pero como han desaparecido las causas que determinaron el procedimiento de que se trata, por medio del presente se hace saber al público que desde esta fecha no se otorgará más la mencionada concesión. En consecuencia, los interesados en denuncios de minas caducas, deberán sujetarse en todo a lo que previene la ley minera y reglamentos vigentes."

"Constitución y Reformas.—México, [illegible] de febrero de 1917.
El Secretario, Pastor Rouaix."

"El Universal"
DIEZ PAGINAS
5 Centavos en la Capital y
10 en los Estados

Portada El Universal del 1 marzo de 1917



ERSAL

MAÑANA

DE 1917

Registrado como artículo de segunda clase, el 13 de noviembre de 1916, en la Administración de Correos de México.

NUMERO 152

nza Entre Mexico, Alemania y Japón

Se Publica una Copia de las Instrucciones Enviadas por Zimmerman Ministro de Negocios Extranjeros a Von Eckardt Representante Teutón en México

PRENSA ASOCIADA.
Unicamente para EL UNIVERSAL.

WASHINGTON, febrero 28.—La Prensa Asociada está en aptitud de revelar que Alemania, imponiéndose con su campaña submarina sin restricción y contando con sus consecuencias, propuso una alianza con el Japón y la República Mexicana para declarar la guerra a los Estados Unidos si no permanecían neutrales.

Según este plan, perfectamente concebido por los alemanes, se pediría al Japón, por conducto de México, que abandonara a sus aliados y se uniera a los enemigos de los Estados Unidos para atacarlos.

México, en caso de llevar a la práctica este plan, reconquistaría Texas, Nuevo México y Arizona, y, además, recibiría un tremendo apoyo financiero, repartiendo, al mismo tiempo, el botín con la Alemania victoriosa, en lo que le tocara de Europa.

El arreglo de los últimos detalles se dejó al ministro plenipotenciario de Alemania ante el gobierno del señor Carranza, von Eckardt, quien radica en la ciudad de México, y quien, con fecha diecisiete de enero próximo pasado, recibió amplias instrucciones escritas y firmadas por el ministro de Relaciones Exteriores de Alemania, Zimmermann, sobre el particular.

La Misión de Von Eckardt era Proponer una Alianza con el Japón

Lo primero que tenía que hacer von Eckardt, era procurar que el gobierno de México se pusiera al habla con el del Japón, para atraérselo e inducirlo a inclinarse en la guerra, del lado de los teutones, rompiendo sus relaciones con los Estados Unidos.

Estas instrucciones fueron transmitidas al Ministro von Eckardt, por conducto del embajador en Washington von Bernstorff, quien en estos momentos viaja con rumbo a su patria, haciendo uso de pasaportes que le fueron proporcionados por un gobierno enemigo del suyo, y contra quien conspira.

El gobierno alemán trató de pintar a México una situación completamente distinta de la que realmente es, pues le informó que los aliados habían sido completamente derrotados, que los teutones habían triunfado en toda la línea y que dominaban el mundo por medio de la campaña submarina sin restricciones.

El Gobierno Americano Adquiere una Copia de la Nota de Zimmermann a Von Eckardt

Una copia de la nota enviada por el Ministro de Relaciones, Zimmermann al Ministro von Eckardt, está en poder del gobierno americano, y dice textualmente.

"Con fecha primero de febrero, debemos iniciar nuestra campaña submarina sin restricción. A pesar de esto, tenemos la intención de hacer toda clase de esfuerzos, a fin de que los Estados Unidos permanezcan neutrales. Si nuestras intenciones se ven fallidas, proponemos una alianza con México, bajo las siguientes condiciones: que juntos entraremos en la guerra, y juntos estaremos a la hora de la paz. Nosotros le daremos un amplio apoyo económico, y toda clase de ayuda para que México reconquiste el territorio perdido de Nuevo México, Arizona y Texas. Los detalles se dejan al buen juicio y patriotismo de usted para el arreglo definitivo."

"Queda usted desde luego advertido que debe informar al señor Presidente de México de las instrucciones anteriores, siempre bajo la mayor reserva, tan pronto como sobrevenga la ruptura con los Estados Unidos, y sugerir que el Presidente de México, bajo su propia iniciativa, se comunique con el gobierno del Japón, pidiéndole que se adhiera a este plan, al mismo tiempo sirviendo México como mediador entre el Japón y nuestro país.

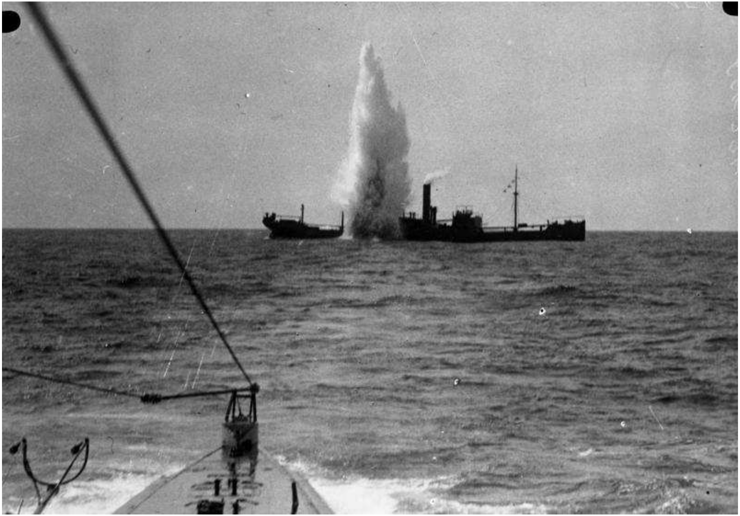
"Sírvase llamar la atención del señor Presidente de México sobre que la campaña submarina está obteniendo resultados sumamente halagadores y que estamos seguros que dentro de muy pocos mese Inglaterra se verá obligada a hacer la paz."

(Sigue en la 5a. plana.)

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.

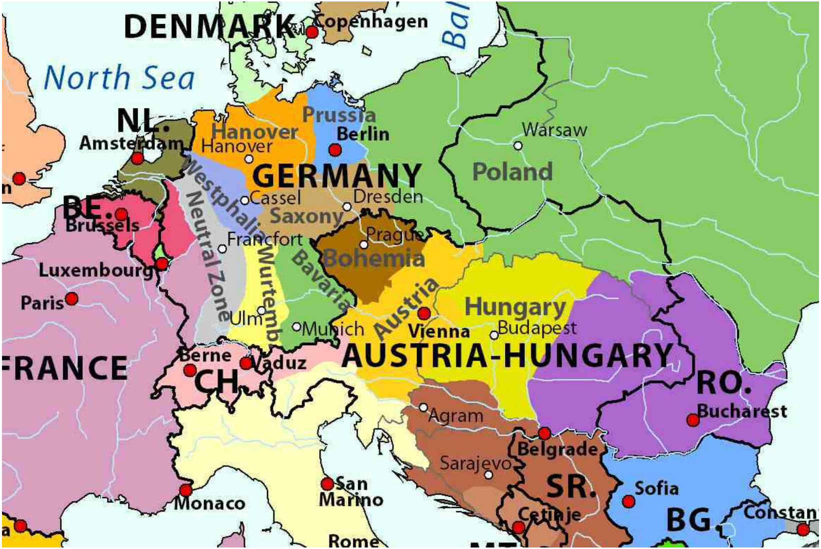
SM U 35 torpedoes HMS Maplewood in April 1917



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.

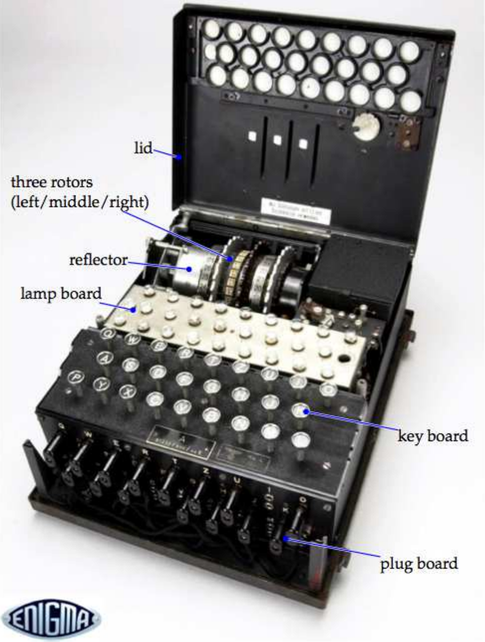
An 8-year old Afghan refugee in Bonn writes in December 2016:

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

Enigma

The ENIGMA was the cryptographic workhorse of the German military in World War II. It was originally broken by Polish mathematicians, who then handed their methods to French and British cryptographers. The latter eventually built up a large organization, whose most famous member was Alan Turing and whose cryptanalytic successes helped to shorten the war considerably. The team also designed COLOSSUS, the world's first electronic (valve) computer, for use in the cryptanalysis of a different German cipher machine.

Enigma


lid
three rotors
(left/middle/right)
reflector
lamp board
key board
plug board
ENIGMA

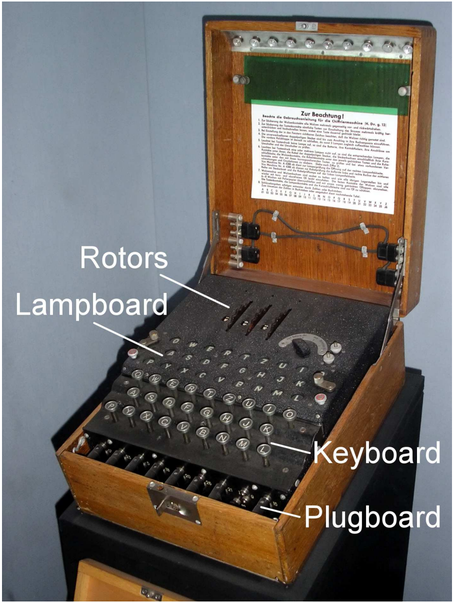
Enigma

In the 1920s, a new type of cryptographic hardware emerged electromechanical devices.
As is often the case in the history of ideas, the time was ripe and the possibilities of such a cryptosystem were realized by four men in four countries around the same time. Apparently the US American Edward Hugh Hebern (1869–1952) was the first to have the idea, in 1917, but made a US Patent application only in 1924. The German Arthur Scherbius applied for a patent on 23 February 1918, the Dutchman Hugo Alexander Koch(1870–1928) on 7 October 1919, and the Swede Arvid Gerhard Damm three days later.

Enigma

Their common idea was to use an apparatus as described below. Hebern took just one rotor and Scherbius three rotors, and the latter became the ENIGMA. It was initially sold commercially. The German military adopted it as a major cryptographic tool starting in 1926. The ENIGMA went through several stages of development, some of which increased security and others decreased it, unwittingly. The estimated number of ENIGMA machines built is estimated at around $200\,000$. Like Henry Ford's *Tin Lizzy*, it could be had in any color, provided the color was black.

Enigma



Enigma

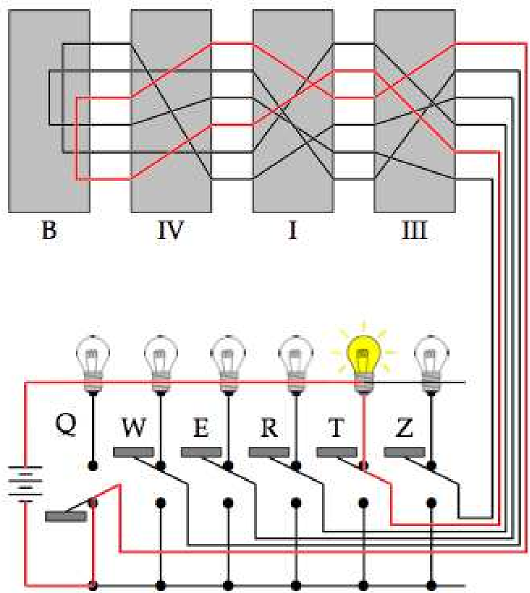
Enigma

The main parts of an ENGIMA are:

- *plug board* (German: *Steckerbrett*),
- *key board*,
- *lamp board*,
- *rotors* (German: *Walzen*).

When you close the lid, the 26 keys show through the holes in the lid, the grooved aluminum *ringsenigma!ring* attached to the rotors through the slits, and the letter at the top of a rotor through the three little windows. To the left of the left rotor, the *reflector* (German: Umkehrwalze) is fixed. Each of the 26 bulbs (the one at left in the middle row is a spare bulb) sits under a circular transparent cover with a letter printed on it.

Enigma



Enigma

Fictitious machine: QWERTZ, no plug board. When you press the Q key, contact is made with the battery at left. Current flows (in red) to the top contact of the entry (right) rotor, named III. On all rotors, contacts are labelled QWERTZ from top to bottom. Thus the internal wiring of III implements the permutation $N = (\text{ERQ})\ (\text{TWZ})$. Current exits at E which is in direct contact with the E on the middle rotor named I, whose permutation is $M = (\text{EQT})(\text{RZW})$. It exits I at Q and enters the left rotor IV, permuting as $L = (\text{ERZQ})(\text{T})(\text{W})$. It exits at E, enters the reflector B, permuting as $R = (\text{EZ})(\text{QT})(\text{RW})$, and then passes back through Z, R, and W to exit III at T. Now current passes through the T lamp which lights up and closes the circuit with the battery. Then T is the encryption of Q at this state of the machine. When the key R is pressed next, the left rotor III has rotated by one position (cyclically downwards in the figure, so that T–R and Z–Q are connected) and–assuming that I has not moved–the lamp Q lights up.

Enigma

The entry rotor turns by one letter (one 26th of a full turn) at each key stroke. Each rotor has a notch in one of 26 positions. When it is in the middle or at the left and the rotor to its right moves to the notched position, then the rotor turns by one letter. The *ring position* (German: *Ringstellung*) determines in which of 26 possible positions the ringenigma!ring is fixed to the rotor. This is only used in determining the machine's initial state before encryption.

Enigma

The plug board consists of 26 connectors, some of which are connected in pairs. In the early days of the war, up to five pairs were connected, later exactly ten pairs. If E is not plugged (“unsteckered”), then current flows from the E key on the key board to the E connector on the entry rotor. But if E is plugged, say to Q, then current goes to the Q plug on the entry rotor. Then it transits the rotor assembly to exit at T, as above. If T is plugged to Z, this causes the Z lamp to light up, and the electrical circuit closes.

Two operators are required: Fritz reads out the cleartext aloud (Alice was not enlisted). Emil types it into the ENIGMA, which he has set up with the current keys, and reads the ciphertext letter by letter back to Fritz, who taps it in Morse code into his radio transmission unit. The recipients have to set up their ENIGMA in the same way, type in the ciphertext, and the plaintext lights up, letter by letter, to be copied down.

Enigma

The setting used for encryption also serves for decryption, for the following reason. The encryption process can be viewed as a composition

$$\pi = P \circ N^{-1} \circ M^{-1} \circ L^{-1} \circ R \circ L \circ M \circ N \circ P \tag{0.1}$$

al:

of the plug board permutation P, the three rotor permutations N, M, and L, and the reflectorumkehrwalze permutation in the permutation group $\mathrm{Sym}_{\mathbb{A}}$ over the 26-letter alphabet $\mathbb{A} = \{$A, B, C$, \ldots,$ Y, Z$\}$. Now if E is sent to Q on the plug board, that is, $P($E$) =$ Q, then also $P($Q$) =$ E. That means that applying P twice does not change anything: $P \circ P$ is the identity and P is an involution. The same also holds for R. When we take the composition $\pi \circ \pi$, adjacent terms cancel one after the other, and we also find $\pi \circ \pi$ to be the identity. Thus for any state, the ENIGMA permutation $\pi \in \mathrm{Sym}_{\mathbb{A}}$ is an involution.

Enigma

The original rules for setting up the ENIGMA contained a serious security flaw, which allowed Polish cryptanalystscryptanalysis to discover the rotor wiringrotor wirings.

During much of its wartime use, a daily secret keysecret key was distributed on paper to all participants in a network of ENIGMAS. It consists of the rotor choice and order, the ring settingsecret key, and the plugboard connectionsplugboard connections. The operator chooses two (supposedly random) 3-letter keys, the starting position HMD and the secret session key YOS. He uses the grooves on the ringenigma!rings to move the rotors into position HMD, visible through the small windows. Then he encrypts YOS to obtain the public session key, say XMZ. He starts a transmission by sending HMD and XMZ, sets his machine to YOS and starts encrypting and sends the resulting ciphertext. The recipient initializes his ENIGMA with the same daily secret key and starting position HMD, decrypts XMS to obtain YOS, sets his machine to YOS and decrypts the received ciphertext.

Enigma

Figure : Two ENIGMA rotors.

Enigma

Enigma

Enigma

According to Kerckhoff's principle and the early commercial availability, the ENIGMA system must be assumed to be known to the enemy. Security only relies on the secret key. This consists of three parts:

- choice and sequence of rotors,
- setting of rotors,
- plugboard connections.

Initially, a further secret ingredient was the internal wiring of the rotors. It would be unwise to rely on this for security, because then a single stolen or captured machine would jeopardize the whole system.The reflector was fixed. The other rotors came in a wooden box. Initially, there were three to choose from, which allows six possible permutations. A later version had five to choose from, giving $5 \cdot 4 \cdot 3 = 60$ possibilities. The three rotors of the German Navy ENIGMA could be chosen from a set of eight. This rotor setting was first changed monthly, later daily, and from mid-1942 on every eight hours. In 1943, a machine with four rotors was introduced.

Enigma

Each rotor could be set in one out of 26 positions at the beginning of a transmission. The entry rotor advanced by one position every time a key was pressed. Like an odometer, it advances after 26 turns the middle rotor by one position and this then moves the leftmost rotor by one after 26 turns.With 60 choices for a sequence of three out of five rotors, 26^3 positions for them, and $26!/(2^{10} \cdot 6! \cdot 10!)$ choices for ten plugboard connectionsplugboard connections, the size of the key space is

$$158\,962\,555\,217\,826\,360\,000 \approx 1.6 \cdot 10^{20} \approx 2^{67}.$$

At the time, 67-bit security against exhaustive key search was more than enough. The ENIGMA's downfall were insecure operating modes and, above all, faulty behaviour of operators.

Enigma

The second most common mistake of crypto system designers is to take a large key space as a guarantee of security. (The most common mistake is to take the designer's failure to break his own system as proof that everybody else will fail, too.)

Enigma

No single event can be pinpointed that brought about Allied victory in the Second World War, but the British cryptanalysts at Bletchley Park played a vital role in many battles whose outcome eventually saved the world from brutal Nazi domination. It has been conjectured that *Ultra* shortened the war by two years, saving millions of lives on both sides.

Alan Turing, a famous British mathematician and computer scientist, had proposed in 1937 a precise mathematical model of computers—the *Turing machine*—invented the idea that programs could be stored as data (namely, for his *universal Turing machine*), and proved that deceptively simple questions cannot be solved by any algorithm.

Enigma

The cryptanalytic success against the ENIGMA was started by a team of Polish cryptographers, including the mathematician Marian Rejewski. They had completely solved the then standard machine in 1939. Their cryptanalysis of the ENIGMA rotors was completed in 1932. One of their main inventions was the *bombe*, an electromagnetic device simulating many ENIGMA runs on a fixed plaintext. On 25 July 1939, nine days before Hitler's blitzkrieg attack on Poland and while most people were still happy with the seeming success of appeasement politics at München, they were wise enough to share their secrets and machinery with French and British cryptographers. Later, they were treated in a cavalier way: while in exile in England, they were not allowed to participate in the British cryptanalytic effort.

Enigma

Figure : The main building, the *manor*, at Bletchley Park, used by the administration, of course. The cryptanalysts worked in wooden huts. Umbrella and shorts illustrate the versatile weather of a Buckinghamshire summer day.

Enigma

A vital ingredient to the initial Polish ENIGMA break was a classical espionage coup by the French Secret Service. Hans Thilo Schmidt, working in the *Chi-Stelle* of the *Reichswehrministerium* (cipher bureau of the Reich’s Defense Ministry) offered his services in October 1932. Directed by Colonel Gustave Bertrand and under the codename Asché, he divulged many secrets. Among them were complete key schedules for certain periods. The French secret agent Lemoine, captured and interrogated by the Germans, betrayed Asché, who was arrested at home in Fürstenwalde and executed in July 1943.

Enigma

The British Foreign Office set up a team of cryptographers at Bletchley Park on 4 September 1939, one day after Hitler attacked Poland. A little later, Turing joined the team. One of their main tasks became the breaking of the ENIGMA-encrypted communication between the German Navy headquarters at Kiel and the submarines in the North Atlantic. These inflicted crippling losses on Allied convoys from North America to Europe. After a long struggle, Bletchley Park started deciphering ENIGMA messages regularly in 1942. The resulting stream of deciphered data ran under the name of *Ultra*. The unfortunate U-boat captain who had just radioed his position to headquarters did not know that the US *Catalina* bombers dropping depth charges all around him were secretly directed by the brain of a mathematical genius.

Enigma

At the highest level of secrecy, German military messages were enciphered on different systems, the *Siemens Geheimschreiber* and the *Lorenz SZ* (Schlüsselzusatz). The latter also used rotors, namely, twelve of them. But the principle differed from the ENIGMA's: the rotors generated a pseudorandom bit string, and each letter of the message was encoded by five bits, according to the standard *Baudot code*. These two bit streams were then added bitwise (XORed), just as one does in a one-time pad. By a brilliant stroke of cryptanalytic genius, the mathematician Bill Tutte discovered this principle. He was unwittingly aided by a German radioman who transmitted essentially the same message twice in secret key. And then Bletchley Park, in collaboration with British Post Office engineers, set out for one of their main achievements: the world's first computer. This COLOSSUS had about 1500 valves. Its input was fed on rapidly moving paper tape, at right in the figure, showing the replica now standing in the Bletchley Park museum.

Enigma

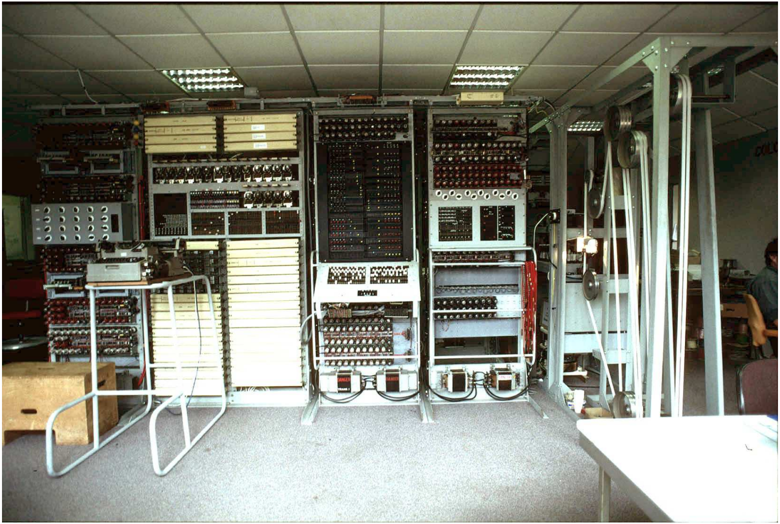
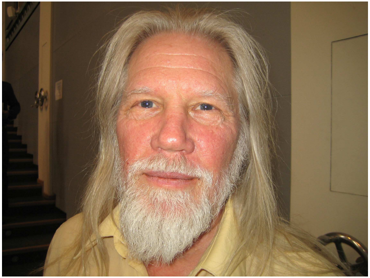


Figure : Colossus rebuilt at the Bletchley Park Museum.

Whitfield Diffie and Martin Hellman



* 1944

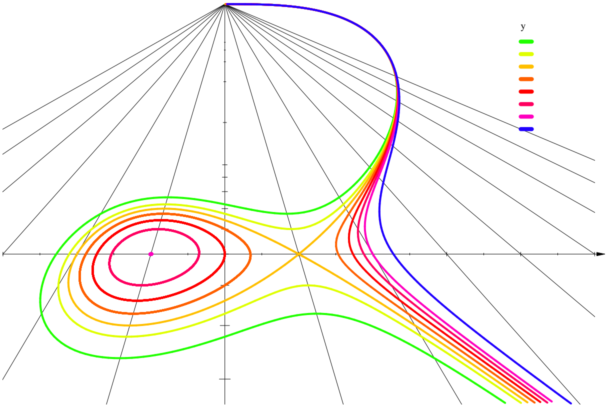
* 1945

Diffie-Hellman Revolution

New Directions in Cryptography, 1976

- Public-key cryptography
- Diffie-Hellman key exchange
- RSA (Rivest, Shamir, Adleman; factoring large numbers), discrete logarithms, elliptic curves
- cryptography turns into a science, using computational complexity. Precise formulation of theoretical security. Necessary: $P \neq NP$.
- Current question: alternative basis for cryptographic security?

Elliptische Kurven

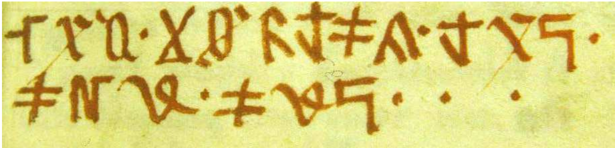


Quantum computers

Quantum computers can factor integers and compute discrete logarithms efficiently.
Question: will they ever be built with scalable size?

The D-Wave quantum computer.
“Post-quantum cryptography”

The end



das puchel hat ein ent

Herzog Rudolf IV. von Österreich (1339–1365)