التسلسل الزمني

	تحليل الشيفرة	الحرب
قبل الحرب		
1923	عرضت آلة الإنيغما في معرض اتحاد البريد العالمي في بيرن، سويسرا.	
كانون الثاني 1924	لورانس سافورد عين أول رئيس لمكتب أبحاث البحرية.	
1924	تأسست أول محطة اعتراض لبحرية الولايات المتحدة.	
1925	جوزيف روشفورت عين في مكتب الأبحاث.	
1928	بدأت دروس «العصبة على السطح» لتعليم إشارات مورس بالرموز اليابانية «الكانا».	
أيار 1929	إغلاق «الغرفة السوداء».	
كانون الأول 1932	اكتشاف ماريان ريجيفسكي لتوصيلات أسلاك الأقراص الدوارة في الإنيغما العسكرية الألمانية.	
30 كانون الثاني 1933		أصبح هتلر مستشاراً
1936	تفكيك آغنيس دريسكول للآلة الحمراء اليابانية.	
15 أيلول 1938	تقديم نظام مؤشر جديد لإنيغما الجيش الألماني.	
29–30 أيلول 1938		مؤتمر ميونيخ
15 كانون الأول	تقديم قرصين دوارين جديدين لإنيغما الجيش.	

	تحليل الشيفرة	الحرب
1938		
1939		
15 آذار		ألمانيا تغزو تشيكوسلوفاكيا
1 حزيران	تقديم شيفرة جديدة للبحرية اليابانية NJ–25.	
20 شباط	تبدأ الآلة البنفسجية تحل محل الآلة الحمراء في دارات الديبلوماسية اليابانية.	
24 تموز	الاجتماع في بيري بين مفككي الشيفرة من بولونيا وفرنسا وبريطانيا.	
1 أيلول		ألمانيا تغزو بولندا.
3 أيلول		فرنسا وبريطانيا تعلنان الحرب.
1940		
17 كانون الثاني	البولونيون يفككون أول إعدادات إنيغما زمن الحرب وذلك باستخدام الطرق اليدوية (صفحات زيغالسكي).	
12 شباط	استكشاف الأقراص الدوارة VI وVII من U–33.	
14 آذار	تشغيل أول «قنبلة» في بليتشلي بارك.	
9 نيسان		ألمانيا تغزو النرويج.
10 نيسان	يظهر مفتاح الإنيغما الصفراء ويتم تفكيكه.	
26 نيسان	أسر ترولار بولاريس.	
1 أيار	توقف التشفير المزدوج لمؤشرات الإنيغما.	
أيار – تموز	قراءة رسائل الإنيغما البحرية لأيام 22–27 نيسان باستخدام مواد بولاريس وأول «قنبلة».	
10 أيار		ألمانيا تهاجم في الغرب تشرشل يصبح رئيساً

	تحليل الشيفرة	الحرب
		للوزارة
21 أيار	قراءة رسائل إنيغما القوى الجوية بالمفتاح الرئيس (الأحمر) بصورة حالية.	
22 حزيران		استسلام فرنسا
الصيف		معركة برلين
آب	الاستيلاء على القرص الدوار VII.	
8 آب	تركيب القنبلة رقم2 (بلوحة قطرية «محورية»).	
أيلول	تفكيك الآلة البنفسجية من قبل جيش الولايات المتحدة أول تفكيك لشيفرة JN–25 في الوحدة OP–20–G	
1 كانون الأول	ظهور الشيفرة JN–25B	
	الوحدة GC&CS تفكك الشيفرة اليدوية الرئيسية للجيش الألماني ISOS.	كانون الأول
1941		
كانون الثاني	مهمة سينكوف إلى الوحدة GC&CS.	
12 شباط		رومل يصل إلى طرابلس الغرب
28 شباط	تفكيك شيفرة مفتاح الإنيغما الجوية لشمال افريقيا وهي «الأزرق الفاتح».	
4 آذار	أسر مطابقة ترولر من جزر لوفتون؛ وأخذ إعدادات الإنيغما البحرية لشهر شباط.	
13 آذار	يبدأ الكوخ 3 بإرسال رسائل مفككة إلى القاهرة.	
24 آذار	تعيين أول المجندات المتطوعات للعمل على أجهزة «القنابل».	
28 آذار		معركة رأس ماتابان
آذار	قراءة رسائل الإنيغما البحرية لشهر شباط	

	تحليل الشيفرة	الحرب
	باستخدام مادة لوفتون.	
3 نيسان	تشرشل يكتب إلى ستالين يحذره من نوايا هتلر	
7 أيار	أسر ترولر مونشن.	
9 أيار	أسر V–110.	
أيار	قراءة رسائل الإنيغما البحرية لواحد وعشرين يوماً بتأخير يتراوح بين 3 و7 أيام.	
15 أيار	استلام روشفورت قيادة محطة هيبو.	
27 أيار		إغراق البسمارك
حزيران	تقديم الشيفرة البحرية رقم 3 وقراءة رسائل الإنيغما البحرية باستمرار.	
22 حزيران		ألمانيا تهاجم روسيا
28 حزيران	أسر ترولر لوينبرغ.	
تموز – آب	تكشف رسائل مفككة من SS والشرطة عن فظائع ارتكبتها ألمانيا على الجبهة الشرقية.	
16–22 آب	دينيستون يزور واشنطن.	
6 أيلول	تشرشل يزور بليتشلي بارك.	
17 أيلول	تفكيك الشيفرة تشافينش، وهي مفتاح إنيغما الجيش في شمال إفريقيا.	
5 تشرين الأول	بدء استخدام شيفرة منفصلة تريتون، مفتاح الإنيغما «شارك» لغواصات المحيط الأطلسي.	
21 تشرين الأول	الكوخ 4 والكوخ 8 يتوسلون إلى تشرشل.	
19 تشرين الثاني	مراجعة سجل دونتيز عن مصادر التسرب المحتملة.	
كانون الأول	تفكيك شيفرة إنيغما المخابرات الألمانية (ISK).	
7 كانون الأول		بيرل هاربر
1942		

	تحليل الشيفرة	الحرب
كانون الثاني	الألمان يحصلون على مفتاح شيفرة الملحق العسكري للولايات المتحدة في القاهرة.	
1 شباط	الغواصات الألمانية في المحيط الأطلسي تبدأ استخدام مفتاح الإنيغما ذات الدواليب الأربعة (M4) والمسماة «شارك».	
15 شباط		سقوط سنغافورة
18 آذار	تبدأ قراءة الشيفرة اليابانية JN–25. البرازيل تجمع العملاء الألمان.	
6 أيار		استسلام جزيرة كوريجيدور في الفيلبين
15 أيار	كولباك يصل إلى الوحدة GC&CS كمراقب.	
26 أيار	رومل يبدأ هجومه على الغزاله.	
4 حزيران	معركة ميدوي	
30 حزيران		وقوف رومل في العلمين
11 تموز	الوحدة GC&CS تسمح بتفكيك الإنيغما في القاهرة.	
الصيف	يبدأ آرلنغتون هول بتحليل الرسائل حول رسائل الجيش الياباني	
8 آب		تعيين مونتغمري قائداً للجيش الثامن
31 آب		معركة تل الحلفا Alam el Halfa.
4 أيلول	بحرية الولايات المتحدة توافق على بناء «القنابل».	
تشرين الأول	التوصل إلى اتفاق تعاون بشأن الإنيغما بين الوحدة	

	تحليل الشيفرة	الحرب
	GC&CS والوحدة OP–20–G.	
23 تشرين الأول		بدء معركة العلمين
29 تشرين الأول	أسر الغواصة U–559.	
8 تشرين الثاني	TORCH، نزول الحلفاء في شمال افريقيا.	
13 كانون الأول	بدء تفكيك الشيفرة M4 «المشارك»، باستخدام كتاب شيفرة الطقس المختصر، والمأخوذ من الغواصه U–599.	
1943		
14 كانون الثاني		مؤتمر الدار البيضاء
30 كانون الثاني		دونيتز يصبح C في C البحرية الألمانية
31 كانون الثاني		استسلام الألمان في ستالينغراد
15 شباط	اكتشاف الإضافات الأخيرة على الشيفرة فلورادورا.	
نيسان	الكشف الأول على شيفرة الجيش الياباني للنقل المائي.	
18 نيسان	مقتل ياماموتو.	
أيار	تسليم هيث روبنسون.	
3 أيار	بدء اختبارات أول «قنبلتين» للولايات المتحدة في دايتون.	
17 أيار	توقيع الاتفاقية الأمريكية البريطانية BRUSA.	
24 أيار		دونيتز يسحب الغواصات من شمال الأطلسي.
22 حزيران	إرسال أو نتيجة من قنابل البحرية في الولايات	

	تحليل الشيفرة	الحرب
	المتحدة إلى الوحدة GC&CS.	
10 تموز		نـــزول الحلفـــاء في صقلية
31 آب	وصول أول «قنابل» البحرية في الولايات المتحدة إلى واشنطن.	
1944		
13 كانون الثاني		أول طـــــائرة V–1 تضرب لندن
19 كانون الثاني	أسر كتب الشيفرة اليابانية في غينيا الجديدة	
شباط	تسليم أول Colossus.	
25 شباط	البحرية في الولايات المتحدة تطلب 50 «قنبلة» إضافية.	
أيار	أول اســتخدام RAM علــى مــشكلات الجــيش الياباني.	
6 حزيران		يـــوم – دي (نـــزول الحلفـــــــاء في النورماندي)
20 تموز	فشل محاولة على حياة هتلر	
	إلغاء 25 «قنبلة» للبحرية الباقية من الكلبية.	1 أيلول
8 أيلول		أول طـــــائرة V–2 تضرب لندن
تشرين الثاني	التفكيك الأولي لشيفرة VENONA.	
16 كانون الأول		هجوم الأردين
1945		
كانون الثاني	تفكيك «الصفحة في المرة الواحدة» الألمانية GEE.	
12 نيسان		موت روزفلت
30 نيسان		انتحار هتلر

	تحليل الشيفرة	الحرب
7 أيار		استسلام ألمانيا
6 و9 آب		إلقاء القنابل الذرية
14 آب		استسلام اليابان

الإنيغما البحرية

نظام المؤشر فيها، وطريقة بانبوريزمس Banbursimus

إن الصعوبات التي واجهها الكوخ 8 في تفكيك إنيغما البحرية الألمانية في عام 1939 وعام 1940، تعود بالأصل إلى نظام مؤشرها الآمن جداً. فعلى العكس من أنظمة القوى الجوية والجيش، استخدمت الإنيغما البحرية إجراء منع بصورة ناجحة كشف أي معلومات عن إعداد الآلة، وذلك في المؤشرات ذاتها – إلا إذا امتلك المرء مجموعة خارجية من الرموز المستعملة للمؤشرات. بعد تفكيك أول فقرة بمفتاح القوى الجوية أو الجيش لكل يوم، تصبح جميع الرسائل بذلك المفتاح سهلة القراءة حالاً. لكن الأمر لم يكن كذلك بالنسبة لمفاتيح البحرية الرئيسية.

في النظام الذي تبنته البحرية الألمانية في الأول من أيار من عام 1937، يختار العامل مجموعتين في كل منهما ثلاثة أحرف من قائمة مطبوعة – «مجموعة مؤشر الإجراء» و«مجموعة مؤشر الشيفرة». وتكتب هاتان المجموعتان (وهما في هذا المثال VFN وHYU) فوق بعضهما، ويضاف إلى كل منهما حرف عشوائياً:

X H Y U
V F N K

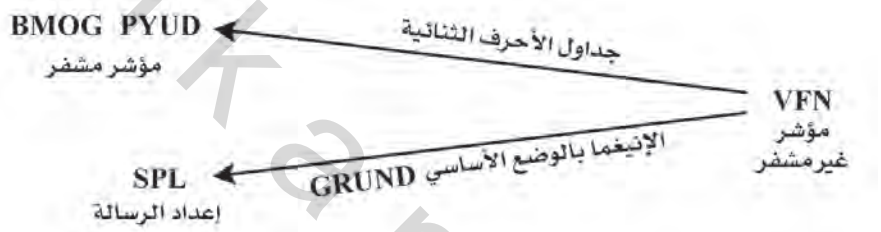
وتقسم الأحرف بعد ذلك إلى حرفين وتكتب أفقياً:

XV HF YN UK

ويستبدل كل زوج من الحرف بزوج من جدول تبديل ثنائي يعمل به في ذلك اليوم، لتصبح:

BM OG PY UD

وترسل هذه الأحرف في بداية الرسالة: BMOG وPYUD. ولتقرير الوضع الابتدائي للأقراص الدوارة المستخدمة في تشفير الرسالة الحقيقية، تطبع عندئذ «مجموعة مؤشر الإجراء»، VFN على الإنيغما وتكون أقراصها الدوارة على «وضع الإعداد الأساسي» المحدد لذلك اليوم. وتبرز مجموعة الأحرف الثلاثة من عملية التشفير، ولنقل SPL، فتكون هي وضع الأقراص التي سيوضع لتفشير هذا النص. كان الأمان الشديد لهذا النظام نتيجة لاستخدام نظامين مختلفين للتشفير: جداول الحرف الثنائية لتشفير المؤشر، وتحويل الإنيغما المؤشر غير المشفر إلى الإعداد الحقيقي للرسالة:



سمحت «القنبلة»، عند توفر مطابقة ناجحة، للكوخ 8 باكتشاف القابس، ونظام الدولاب، وإعداد الرسالة لرسالة مفردة. لكنها هذا وحده لم يفتح قفل المفتاح للنظام المؤشر الذي سيسمح لمفككي الشيفرة من تفكيك رسائل أخرى مباشرة من اليوم نفسه. فدون جداول الأحرف الثنائية والوضع الأساسي (GRUND)، تبقى المؤشرات المرسلة موكل رسالة غير قابلة للتفكيك.

يقدم كتالوج تيورينغ «EINS»، وسيلة لاكتشاف رسائل أخرى دون اللجوء إلى البداية من الصفر وذلك بتشغيل «القنبلة» من جديد؛ وبما أن القابس ونظام الدولاب يبقيان صالحين ليوم كامل، فكل ما يجب إيجاده هو إعدادات الرسالة. في البداية كان كتالوج «EINS» مصنوعاً يدوياً، وبوضع الأقراص الدوارة في نسخة الإنيغما لكلٍ من مراكز البدء والبالغة 17.576 بالتتابع، ومن ثم طباعة الكلمة «EINS»، وباستخدام القابس ونظام الدولاب لذلك اليوم والذي وضعه تدوير «القنبلة». فيما بعد قامت آلة، عرفت باسم «بيبي»، بجعل هذه المهمة آلية. كانت الآلة «بيبي» عبارة عن

«قنبلة» صغيرة، ذات أربع آلات إنيغما موضوعة على مراكز متوالية؛ تدار آلياً عبر مراكز البداية جميعها، وفي نسخة جاءت بعد ذلك أصبحت تثقب تشفير «EINS» في كل مركز على بطاقات IBM مباشرة. وبعد ذلك تفرز البطاقات على كتالوج مطبوع وترتب فيه مجموعات الأحرف الأربعة ترتيباً أبجدياً وتمثل 17576 تشفيراً محتملاً لـ «EINS». ولكن مقارنة النص المشفر للرسالة مع الكتالوج يجب تنفيذها بالعين.

إن كانت جداول الأحرف الثنائية معروفة وإن عرضت رسائل كافية على كتالوج «EINS» في يوم واحد، فمن الممكن اكتشاف «الأساس Grund» إما عن طريق «القنبلة» وإما بالمطابقة اليدوية. والإجراء هو: تقدم جداول الأحرف الثنائية مجموعة مؤشر غير مشفرة لكل رسالة؛ ويكشف كتالوج EINS إعداد الرسالة الحقيقي والمستعمل في تشفير الرسالة؛ وهكذا يكون لدى المرء قطعة تماثل النص البسيط (إجراء مؤشر غير مشفر، وهو في المثال أعلاه VFN) وما يقابله من النص المشفر (إعداد الرسالة الحقيقي – وهو في المثال أعلاه SPL) «للقنبلة» وهي في الوضع «الأساسي Grund». يقدم عدد من هذه المطابقات معطيات كافية للقائمة التي يمكن استخدامها لتأسيس أي وضع – أساس – تستطيع الإنيغما أن تنتج البدائل من النص البسيط والنص المشفر.

حتى قبل أن يتم تفكيك أول رسالة في اليوم، فإن معرفة الجداول ذات الأحرف الثنائية ذات فائدة ضخمة في تخفيض عدد أنظمة الدولاب التي ينبغي أن تدار على «القنبلة». إن الاكتشاف الكبير الذي أنجزه تيورينغ في عام 1939 هو أساس طريقته «Banburismus» التي اكتشفها، والتي تلعب دوراً مركزياً في تفكيك الإنيغما البحرية حتى أنتجت بحرية الولايات المتحدة عدداً كبيراً من القنابل في عام 1943، فلم تعد ضرورية لاختصار زمن القنبلة. عرف تيورينغ أنه إذا كان هناك مؤشران غير مشفرين من الشكل ABX وABY، ومع أنه من غير المعروف أي إعدادات للرسالة يمكن أن تحول الإنيغما عند وضعها على وضع «الأساس Grund» غير المعروف، فإن هناك شيئاً واحداً هو أكيد: إن الحرف A في كل حالة يتحول إلى الحرف نفسه a، وإن الحرف B يتحول إلى الحرف نفسه B؛

وهكذا تكون إعدادات الرسالة الحقيقية للرسالتين شيئاً مثل ZYA وZYQ. وهذا يعني أن مراكز بداية الأقراص الدوارة تقع ضمن 26 مركزاً لكل منهم.

يكمن السر هنا في إيجاد رسالتين لهما المؤشرات القريبة من بعضها وبعدها محاولة معرفة كم تبعد مراكز بدايتها وذلك باستخدام مبدأ «المطابقة»: يكون للنصين المشفرين لرسالتين يوضعان معاً نسبة عالية من الصدفة أعلى من رسالتين عشوائيتين يوضعان معاً – أي إن الاستثناءات أفضل من مجرد العشوائية، واحدة من أصل ست وعشرين فرصة أن يظهر حرف النص المشفر نفسه في آن معاً في المركز ذاته في كلتا الرسالتين عندما توضعان بشكل صحيح. كان الإجراء أن تثقب الرسالة التي تحتوي على مراكز بداية قريبة من بعضها على صفحات من الورق طويلة. والورق الخاص المستعمل لهذه العملية يأتي من بلدة اسمها بانبري، وكان الاسم اللاتيني لذلك «Banburismus». توجد الأبجدية على الصفحة من الحرف A إلى الحرف Z بشكل عمودي، وتوجد الرسالة نفسها بشكل أفقي؛ يثقب ثقب على مكان في الصفحة ليشير إلى حرف ما في مكان ما. وبوضع صفحتين بانبري وفق بعضهما، وتحريكهما بصورة نسبية الواحدة على الأخرى، تظهر الأحرف المتطابقة حالاً عندما يمر ضوء من الثقب، فإن تماثلت سلسلة مؤلفة من حرفين أو ثلاثة أحرف أو أكثر من ذلك من المراكز المتتالية، فهذا توكيد شجع لمطابقة صحيحة؛ ويشير إلى أن مجموعة الأحرف نفسها أو حتى الكلمة الكاملة نفسها قد تم تشفيرها بالمفتاح نفسه. ثم اتسع البحث وذلك بمسح جميع الرسائل، لمعرفة إن كانت تشترك بالمؤشرات القريبة اشتراكاً واضحاً أم لا، وذلك من أجل إشارات مؤكدة بصورة أكبر للمطابقة، مثل تكرار مجموعات من أربع أحرف أو خمسة أحرف أو صدف أكبر؛ وقد نفذت هذه العملية على بطاقات IBM وآلات الفرز.

إن عدد الأحرف التي تتغير فيها رسالة بالنسبة لرسالة أخرى لوضعها في الطابقة تعطينا قراءة حقيقية للفرق في مراكز بداية القرص الدوار فيها. وهكذا إن كانت الرسالة مع المؤشر غير المشفر ABX يجب أن تنزلق مسافة خمسة مراكز إلى اليسار من الرسالة ذات المؤشر ABY، لتوضعا فوق بعضهما بالمطابقة، من

الواضح أن إعدادات الرسالة الحقيقية (الناتجة عن تشفير ABX وABY في وضع الأساس Grund) لهما الحرف الثالث ينفصل مسافة خمسة أحرف في الترتيب الأبجدي – شيء من مثل ZYA وZYF، أو ZYB وZYG، أو ZYC وZYH، وهكذا. مهما تكن إعدادات الرسالة، فيجب أن تكون منفصلة بمقدار خمسة أحرف.

وهذا مكّن من بناء أبجدية شيفرة للإنيغما في المركز الثالث من الوضع الأساس Grund – أي تبادل النص البسيط والنص المشفر الذي تنفذه الإنيغما على الحرف الثالث من كل مؤشر غير مشفر. إن تم الحصول على بعض مطابقات مترابطة في رسائل طريقة بانبري، عندئذ تتأكد المراكز النسبية لبضعة أحرف في أبجدية الشيفرة، ويمكن إنزلاقها معاً على أبجدية النص البسيط حتى يحدث مركز دون «كسور Crashes» – أي، حيثما لا يوجد تناقض بين الأزواج المتبادلة بين أحرف النص البسيط والنص المشفر، مثل حرف يتم تشفيره بنفسه. مثلاً إذا قررت صفحات بانبري المراكز النسبية لأزواج الرسائل:

المسافة النسبية بين الأحرف (تقرره صفحات بانبري)	زوج رسائل (مؤشرات غير مشفرة)
5	QWR, QWX
2	BBC, BBE
13	RWC, RWL
5	PNX, PIC

وعندئذ فإن المراكز النسبية للأحرف X, L, C, E, R يمكن وضعها في أبجدية الشيفرة:

```
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
R . . . . X . . . . C . E . . . . . . . . . . L . .
```

إن الطبيعة المتبادلة لإنيغما تعني إذا تحول حرف X إلى الحرف F، فإن حرف F ينبغي أن يتحول إلى حرف X؛ لذا فإن المركز المذكور أعلاه غير ممكن – هنا

«كسر» (حرف F يذهب إلى X، لكن الحرف X يذهب إلى L). انزلاق الحرفين دون أي كسور ينتج عنه هذا الحل الممكن:

```
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
. . . C . E . . . . . . . . . . L . . R . . . . X .
```

وهذا يمكن أن يستكمل فيما بعد ويختبر لضمان ثباته وذلك بإضافة التبادل المتضمن في أزواج الأحرف:

```
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
. . D C F E . . . . . Q . . . . L T U R S . . Y X .
```

ثبتت الهوية الحقيقية للحرف الثالث لكل مركز بداية للرسالة. فالرسالة ذات المؤشر غير المشفر RWC، مثلاً، لها مركز بداية حقيقي للشكل aBD (لأنه بموجب أبجدية التشفير التي أعيد تركيبها أعلاه، فإن الحرف C يتحول إلى D بواسطة الإنيغما في المركز الثالث للأساس Srund)؛ وكذلك RWL ذات مركز بداية حقيقي للشكل ABQ (لأن حرف L يتحول إلى Q).

إن الجزء الذكي في طريقة تيورينغ هي القفزة التالية. وضعت ثلمة التحويل في مركز مختلف على الأقراص الدوارة. على القرص الدوار رقم 4 مثلاً يحصل التحول بين الحرفين J وK. وهذا يعني إن كان القرص الدوار رقم 4 في الفتحة في أقصى اليمين، ومن ثم عندما تطبع الرسالة التي تبدأ في وضع القرص الدوار في aBD، فإن القرص الدوار المتوسط يدور بعد دخول ستة أحرف من الرسالة. على سبيل المثال، إذا كانت مراكز بداية القرص الدوار الحقيقية للرسالتين المتراكبتين aBD وaBQ هي ABD وABQ، تكون عندها إعدادات القرص الدوار بالمراكز المتتالية للرسالتين كما يلي:

```
1 2 3 4 5 6 7 8 9 10111213141515 17

A A A A A A A A A A A A A A A A A
B B B B B B B C C C C C C C C C C . . .
D E F G H I J K L M N O P Q R S T

                                A A A A
                                B B B B . . .
                                Q R S T
```

لكن هذا مستحيل لأنه يعني أن تحويل الدولاب المتوسط قد حصل في الرسالة الأولى قبل أن يصل إلى نقطة التراكب مع الرسالة الثانية، أي ثلاثة عشر حرفاً في الأمام: عندما تكون الأولى في الوضع ACQ، تكون الثانية في الوضع ABQ. والصدفة في النص المشفر التي اكتشفتها صفحات بانبري لا يمكن أن تحدث بهذا الشكل، لأن النص المتراكب إذن لحدث تشفيره في وضع مختلف للقرص الدوار في رسالتين. لذا يمكن الغاء القرص الدوار رقم 4 من اعتباره القرص الدوار في أقصى اليمين.

إن التغير في موقع ثلمة التحويل بين الأقراص الدوارة المختلفة كان المقصود منه بالنسبة للأمان أن يكون مصدراً آخر لأمان كتابة الشيفرات، لكن ذلك أثبت في الواقع أنه ضعف رهيب ويمكن استغلاله. لو كانت الأقراص الدوارة الثمانية لها مركز التحويل ذاته، لكانت خطة تيورينغ عديمة الفائدة. في الواقع، استخدمت الألمانية ثلاثة أقراص دوارة بشكل حصري هي القرص رقم 6 و7 و8، وأعطيت جميعها نقاط التحويل ذاتها (وفي الحقيقة كان لكل قرص ثلمتا تحويل، بين حرف M وN، وبين Z وA). كانت ثلم القرص رقم 1 وحتى القرص رقم 5، تقع بين Q وR، وبين E وF، وبين V وW، وبين J وK، وبين Z وA، والتي كان اسمها الرسمي في الكوخ Royal Flags Wave Kings Above 8.

ومع كثير من الحظ، كان من الممكن تكرار عملية الإلغاء وذلك بتحليل تحويلات الدولاب الأيسر، وبذلك تثبت هوية الدولاب المتوسط. وهكذا يمكن تخفيض أنظمة الدواليب من 336 نظام محتمل إلى عدد صغير يصل إلى 6 وهو الذي نحتاجه لاختباره على آلة «القنبلة». وعادة يضيق هذا الإجراء الدولاب الأيمن إلى احتمال واحد أو ثلاثة احتملات، فيترك $7 \times 6 = 42$ أو $3 \times 7 \times 6 = 126$ احتمالاً يجري اختبارها، وهذا ما يزال تخفيضاً كبيراً من 336.

--- --- ---

تحليل شيفرة الآلة البنفسجية

استغرق فرانك روليت وزملاؤه في مصلحة مخابرات الإشارة في جيش الولايات المتحدة بضعة أشهر ليقرروا أن الآلة البنفسجية اليابانية، مثل سابقتها الآلة الحمراء، تستخدم قناتين منفصلتين من التشفير. توصل ستة أحرف مختارة بواسطة لوحة قوابس إلى خلاط واحد؛ وتذهب الأحرف العشرون إلى خلاط آخر. وتتغير عملية القوالب كل يوم. لكن «الأحرف الستة» يمكن تحديدها مباشرة تماماً وذلك بتعداد التكرار في النص المشفر. وحيث أن «الأحرف الستة» تخلط فيما بينها، فإن تكرار كل حرف من هذه الأحرف في النص المشفر يساوي التكرار الوسطي «للأحرف الستة» في النص البسيط الذي وراءه، وكذلك فإن تكرار كل من «الأحرف العشرين» فهو يساوي للتكرار المتوسط لهذه الأحرف في النص البسيط. ينتج عن كل ستة أحرف تختار عشوائياً من أحرف الأبجدية مجموعة يكون متوسط تكرارها إما أكبر أو أصغر من تكرار الأحرف العشرين الباقية؛ وهكذا يميل تكرار الأحرف في الشيفرة البنفسجية إلى الإنقسام إلى قسمين متميزين.

بعد استخدام مقدار كبير من مماثلة النص المشفر والنص البسط، تمكن محللو الشيفرة في مصلحة مخابرات الإشارة من اكتشاف الصيغة المخبأة والتي كانت فيها «الأحرف الستة» مخلوطة في كل مركز من مراكز المفتاح المتتابعة، وأثبت أن هذا جدول بدائل من 6×25. فعندما يتقرر هذا الخلط، يصبح موضوعاً مباشراً لتحديد أي من كل «ستة» يومياً تتعلق بأية أحرف في جداول البدائل.

مثلاً إن صيغ الخلط كانت:

النص البسيط

مركز المفتاح	a	b	C	D	E	f
1	F	A	E	B	C	D
2	D	A	C	F	E	B
3	D	E	F	C	B	A
4	C	E	B	F	A	D
.	.	.	.	.	.	.

وإذا حدد تعداد التكرار لنص مشفر O, H, D, B, A وR على أنها «الستة أحرف»، فإن الخطوة التالية تكون بتعداد تكرار منفصل هذه الأحرف عند كل «مركز المفتاح» في الرسالة. وأول، وست وعشرون، وخمس وعشرون وستة وسبعون حرفاً لكنها شفرت بنفس «المركز المفتاح»؛ وكذلك الثاني والسابع والعشرون والثاني والخمسون والسابع والسبعون؛ وهكذا.

الرسائل المتعددة من اليوم نفسه (وكلها تستخدم القوابس ذاتها) يمكن جمعها معاً إذا كان نظام المؤشر، الذي يكشف أي مركز رئيسي بدأت به كل رسالة، قد تفكك. إذا كان تعداد التكرار للمركز الرئيس (المفتاح) 1 إلى 4 يري ما يلي:

المركز الرئيس	التكرار في النص المشفر					
(المفتاح)	A	B	D	H	O	R
1	2	7	15	10	8	1
2	2	0	6	14	9	3
3	4	19	7	3	14	1
4	9	18	0	25	11	1

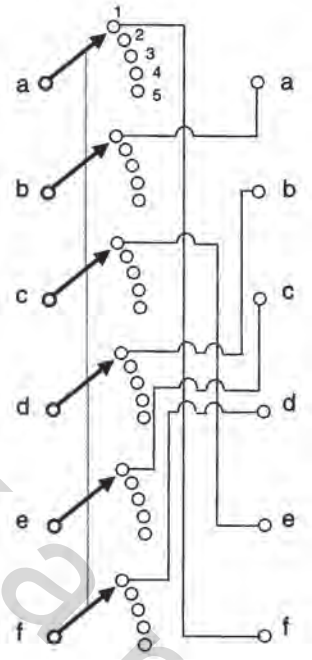
فمن الممكن البدء بصنع تحديدات باستخدام معرفة التكرار الحقيقي للأحرف a وb وd وh وo وr في نص ياباني بالرموز الرومانية. إن الحرف o أكثر الأحرف الستة تكراراً، وبعده يأتي الحرف o. وهكذا من المحتمل أن يكون الحل بالنسبة للمركز الرئيس 1 هو D = 0؛ وللمركز 2 هو H = 0؛ وللمركز الثالث هو

B = 0. وجدول البدائل فيه عمود واحد يناسب هذه الصيغة، وهي أن المركز الرابع (وفيه يتحول الحرف d على التوالي إلى BFCF؛ وهذا مماثل للحرف o الذي يتحول إلى DHBH). وكذلك يظهر الحرف a بتعداد التكرار ليكون HOOB في المراكز الأساسية (المفاتيح) التي تماثل صيغة العمود الأول في جدول البدائل (a تتحول إلى FDDC). وبمزيد من تحدير التكرار أكثر قليلاً، فيمكن أن تكون الهويات الكاملة للأحرف في جدول البدائل على الشكل التالي:

النص البسيط

المركز الرئيسي (المفتاح)	a	b	d	o	r	h
1	H	A	R	0	D	0
2	0	A	B	H	R	D
3	0	R	H	B	D	A
4	B	R	D	H	A	0
.	.	.	.	.	.	.

لم تكن صيغة الخلط للمراكز الرئيسية في جدول بدائل «الأحرف الستة» واحدة يمكن أن ينتجها قرص دوار كما في آلة الإنيغما. فقد كان كل مركز رئيسي لا علاقة له مطلقاً بالمركز السابق. إن المكون الصلب (الآلة) الذي استطاع عمل مثل هذا الخلط بقي سراً حتى فرصة اكتشاف ليو روزين للمفاتيح الهاتفية «الناخب الواحد» التي جاءت بالجواب. تألفت هذه من مجموعة من ستة مفتاح مجتمعة معاً. في كل من الخطوات الخمس والعشرين، تقوم بوصل ستة أحرف داخله بستة أحرف خارجة بترتيب مختلف.

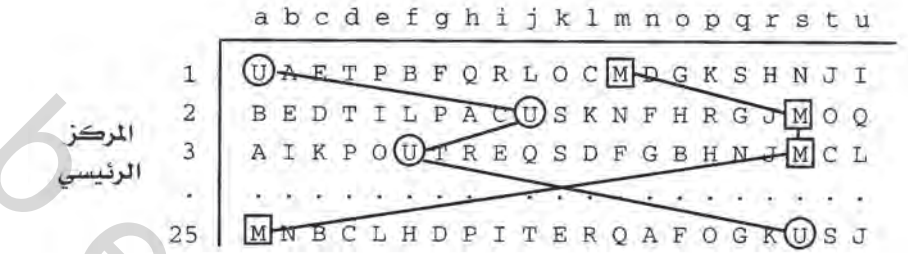


إن عملية توصيل أسلاك مفاتيح «الخطوة» لفتاة «الأحرف الستة» في الآلة البنفسجية، تصور الصلات البينية لمفتاح المركز 1 في جدول البدائل أعلاه. تتحرك المفاتيح الستة معاً بتزامن خلال 24 مركزاً، ثم تعيد الدورة.

ثبت أن اكتشاف صيغة التبديل للعشرينات أكثر صعوبة. فكان طول المفتاح أطول كثيراً من الخمس والعشرين، وكان اكتشاف جينفياف غورتجان الشهير وهو: على الرغم من أن جداول البدائل تتغير بعد كل دورة من خمسمة وعشرين حرفاً، فإن الجداول التي تتكون في كل دورة متعلقة ببعضها بصيغ معينة.

وأخيراً ظهرت صيغتان من صيغ العلاقات فيما بينها. في إحداها، كانت هويات الأحرف في الجدول تتغير بعد كل دورة من المراكز الرئيسية الخمسة والعشرين، ولكن الطريقة التي تقفز فيه الأحرف من سطر إلى السطر التالي في كل جدول كانت ثابتة.

دورة 1



دورة 2

إن الأحرف ضمن الدوائر والمربعات في كلتا الحالتين تتبع سلسلة الحركات ذاتها من سطر إلى السطر الذي يليه؛ وكذلك تفعل الأحرف في المراكز الأخرى. بعبارة أخرى، هذه الجداول يشبه بعضها بعضاً.

في الصيغة الأخرى، وجدت أعمدة كاملة من جداول التشفير أنها تتطابق في كل دورة تأتي بعدها:

دورة 1

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u
1	U	A	E	T	P	B	F	Q	R	L	O	C	M	D	G	K	S	H	N	J	I
2	B	E	D	T	I	L	P	A	C	U	S	K	N	F	H	R	G	J	M	O	Q
3	A	I	K	P	O	U	T	R	E	Q	S	D	F	G	B	H	N	J	M	C	L
.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
25	M	N	B	C	L	H	D	P	I	T	E	R	Q	A	F	O	G	K	U	S	J

المركز الرئيسي

دورة 2

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u
1	A	P	R	I	J	E	L	D	F	U	T	S	O	Q	M	K	B	N	G	C	H
2	E	I	C	Q	O	D	U	F	P	B	T	G	S	A	N	R	L	M	H	K	J
3	I	O	E	L	C	K	Q	G	T	A	P	N	S	R	F	H	U	M	B	D	J
.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
25	N	L	I	J	S	B	T	A	D	M	C	G	E	P	Q	O	H	U	F	R	K

هذه الصيغ هي ما يتوقفه المرء تماماً عندما يستخدم جدولين أو أكثر من جداول البدائل الأبجدية على نص بسيط بالطريقة الدائرية على التوالي. أي، إن أول حرف من النص يشفر بالسطر 1 من الجدول 1، وتشفر النتيجة بالسطر 1 من الجدول 2؛ والحرف الثاني يشفر بالسطر 1من الجدول 1، والسطر 2 من الجدول 2 وهكذا حتى الأسطر 1 و25؛ وبعد ذلك في جميع الأسطر الخمسة والعشرين من الجدول 2 مرة ثانية ولكن باستخدام السطر 2 من الجدول 1. عندما يكون الجدول 1 في دورة «بطيئة»، تنتج الصيغة المشابهة. وعندما يكون الجدول 2 هو الدورة البطيئة، ينتج التطابق العمودي.

أظهر التحليل الأكثر أن الآلة البنفسجية قد استخدمت شلالاً من ثلاثة جداول تبديلية «للعشرين حرفاً». تأثرت هذه البدائل في الآلة الحقيقية بثلاث مجموعات في كل منها أربعة مفاتيح من مفاتيح «الناخب الوحيد»؛ وقدمت المجموعة الرباعية 6 × 4 = 24 مفتاحاً مجمعين، وبذلك فسح المجال للأربعة والعشرين حرفاً مضافاً إليهم أربعة مفاتيح إضافية كانت تستخدم كدارات تحكم. يمكن وضع أي من المجموعات الثلاث في الدورة السريعة أو المتوسطة أو البطيئة. ومع أن هذا قد أضاف إلى عدد التغيرات التي ولدتها الآلة ككل، فقد كان نقطة الضعيف القريبة من تغيير نظام الدولاب في آلة الإنيغما، لأنها قدمت لمحلل الشيفرة تشخيصاً أبعد حول أسلاك كل مجموعة مفتاح «ناخب وحيد».

--- --- ---

شبكة اعتراض الرسائل

أدى اختلاف الأولويات والخطوط في الحرب إلى تغيرات مستمرة في شبكات اعتراض الرسائل في بريطانيا وأمريكا. ففي أواخر 1943 كانت الوحدة OP–20–G تشغل ما يقرب من 445 جهاز استقبال لاعتراض الرسائل ذات المستوى العالي في المحيط الهادي (وقد يرتفع العدد إلى 775 مع نهاية الحرب) في أربعة مواقع ثابتة.

جزيرة برين بردج، واشنطن	**120 جهاز استقبال**
أمبريال بيتش، كاليفورنيا	**75 جهاز استقبال**
واهياوا، هاواي	**200 جهاز استقبال**
استراليا	**50 جهاز استقبال**

وكانت رسائل الغواصات الألمانية يتم اعتراضها في تشازم، على رأس كود في ماساشوستس؛ إضافة إلى ذلك كانت محطات اكتشاف الاتجاه منتشرة على طول المسافة من غرينلاند حتى البرازيل. ووضُعت محطات أخرى لاكتشاف الاتجاه في جزر المحيط الهادي.

كانت شبكة جيش الولايات المتحدة تتألف من ست محطات ثابتة تركز جهدها على الإشارات العسكرية اليابانية ورسائل دول المحور الديبلوماسية:

فنت هيل، وارينتون، فيرجينيا
تو روك رانش، بيتالوما، كاليفورنيا
اسمرة، اريتريا
فورت شافت، أراضي هاواثي

فيربانكس، آلاسكا

نيودلهي، الهند

وكانت الوحدة GC&CS في منتصف عام 1943 تتلقى الرسائل من شبكة بعيدة في المملكة المتحدة:

سكاربورا	72 جهاز استقبال
فلورداون	45
تشيك ساندرز	16
كوبار	15
شيتلاندز	2

الجيش

بومانور	140
هانبدن	23
كيدلستون هول	36
وحدات متنقلة	6

القوى الجوية الملكية

تشيك ساندز	105
تشيديل	75
كنغزداون	15
ودنيغتون	24
تين	19
ويك	14

وزارة الخارجية

برورا	14
كوبار	13
دانمارك هيل	23
ساندريدج	54

ويت تشرش	40
نوك هولت	35

دائرة البريد

سانت البانز	8
محطات ساحلية	9

واستكملت هذه المحطات بمحطات فيما وراء البحار في كندا (اوتاوا، ونييبغ، وغراند، وبربيري، وبوينت غري، وفيكتوريا)، وفي مالطا وجبل طارق والاسكندرية والقاهرة وبغداد وفي مواقع أخرى في مصر، وجنوب أفريقيا، غرب افريقيا والهند.

--- --- ---

آلات التحليل السريعة RAM

استخدم محللو الشيفرة البريطانيين والأمريكيين معدات شركة IBM لتثقيب البطاقات استخداماً واسعاً خلال الحرب العالمية الثانية؛ وكان أحد الاستعمالات الرئيسية لآلات IBM هو خلق قوائم مرتبة ترتيباً رقمياً لمجموعات رسائل ظهرت في الرموز المشفرة كخطوة أولية نحو وضع هذه الرسائل فوق بعضها في «المطابقات».

لم يظهر أول حاسوب للأغراض العامة حتى بعد الحرب، وكانت طرق بطاقات IBM، على الرغم من قوتها المدهشة، ذات قيود متميزة؛ لم تستطع بصورة خاصة مقارنة أو جمع أرقام لمعالجة بعض المشكلات الخاصة بتحليل الشيفرة التي تظهر. ولم يكن بينها «حاسوب» بالمفهوم الحديث، ولم تكن حتى أسلافاً للحاسوب، على الرغم من أنها كانت رائدة لبعض تقنيات المكونات (مثل دارات التعداد الاليكترونية ودارات تخزين الذاكرة) التي تلعب دوراً في أوائل الحواسب الرقمية.

«القنابل»

القياسية:

تحتوي على ست وثلاثين آلة إنيغما ذات الدواليب الثلاثة (وكانت ثلاثين في النماذج الأولى).

142 تم بناؤها من قبل شركة آلة الجدولة البريطانية.

لوحة الاختبار ("الطفلة"):

أربع آلات إنيغما ذات ثلاثة دواليب توضع لمراكز قرص دوار متتالية.

استخدمت لجمع كتالوج «EINS» لاكتشاف إعدادات رسائل الإنيغما البحرية بعد تفكيك أول رسالة في اليوم: تقوم الآلة بتشفير الكلمة EINS في جميع المراكز الأولية للقرص الدوار وعددها 17576 من أجل نظام دولاب وقابس وإعداد حلقة مفترضة وتثقيب النتائج على بطاقات IBM.

الجامبو:

قنبلة قياسية مع إضافة «المدفع الرشاش» الذي يفحص كل توقف للقوابس المتوافقة ويطبع النتائج؛ وسمح بدوران القوائم الأضعف دوراناً فعالاً.

بني منها أربع عشرة آلة.

الكوبرا (طراز «وين ويليامز»):

دولاب رابع عالي السرعة إضافة إلى وحدة أنابيب مفرغة حساسة توصل إلى «قنبلة» قياسية؛ فجوة توقف قصد منها معالجة مشكلة الإنيغما البحرية ذات الدواليب الأربعة.

صممها مهندسو دائرة البريد العامة؛ أثبتت أنها غير موثوقة.

بني منها اثنتا عشرة آلة.

الماموث السريعة (طراز «كين»):

قنبلة ذات أربعة دواليب كاملة لمشكلة الإنيغما البحرية: استخدمت مقويات عالية السرعة لتستشعر التوقفات.

بني منها سبع وخمسون آلة.

بحرية الولايات المتحدة N–350 وN–1350

ست عشرة آلة إنيغما ذات الدواليب الأربعة: «قنبلة» عالية السرعة مع حساس توقف اليكتروني.

بنت منها شركة NCR ما يقرب من 125 آلة.

003 ("الماموث X"):

144 آلة إنيغما ذات الدواليب الثلاثة؛ استخدمت مقويات مفاتيح الهاتف بدل الأقراص الدوارة.

بنت شركة AT&T مخابر بيل لجيش الولايات المتحدة واحدة. واستخدمت في الأبحاث بصورة رئيسية.

الحواسب الإلكتروميكانيكية (أوتوسترتشر)، والحواسب الإلكترونية بالكامل (سوبر سترتشر)

وقد استخدمت لمهاجمة الإنيغما ذات العاكس ذي القابس.

بناها الجيش الأمريكي: كان الحاسب الإلكتروميكانيكي بطيئاً؛ واستكمل الحاسب الإلكتروني كاملاً في خريف 1945، واحتوى على ثلاثة آلاف وخمسمائة أنبوب مفرغ.

دونيا:

وحدة قنبلة صغيرة لكشف الإعدادات المجهولة للعاكس ذي القابس صنع منها القليل لبحرية الولايات المتحدة.

البلدوزر:

اثنتان وثلاثون إنيغما ذات الدواليب الأربعة «القنبلة الإحصائية» لاستخدامها حيث لا تتوفر مطابقات، مللت تكرار النص البسيط، وتوقفت عند التوصل إلى مجموع يمكن إعداده.

بني منها واحدة لبحرية الولايات المتحدة.

غرينيدز:

إضافات مختلفة على القنابل لإيجاد الإعدادات عندما يعرف نظام الدولاب والقابس وإعدادات الحلقة.

المقارنات: الأفلام والأشرطة الورقية

آلة I. C. :

استخدمت لوضع النصوص المشفرة فوق بعضها: لوحات زجاجية مضاءة قياس 3.5 × 1.5 انش، سجلت نص رسالة من ستمائة رموز رسالة؛ واستخدمت خلية ضوئية واحدة لقياس مقدار الضوء الذي يظهر من اللوحات الموضوعة فوق بعضها، عندما يتغير وضعها النسبي.
بناها ايستمان كوداك.

آلة المقارنة 70 ملم:

تُثقب الرسائل على شريط ورقي عرضه (70 ملم)، ويلف على شكل طوق بطول 24 قدم يحتوي على ألف وسبعمائة رمز من نص الرسالة، ويتم إدخاله في رأسين قارئين في كل البدايات النسبية الممكنة؛ تقوم عدادات اليكترونية وطابعة تحصي المصادفات على فترات مختلفة تحددها لوحة قوابس.
بنتها شركة NCR وشركة غري الصناعية.

هيبو:

استخدمت لتفكيك (duds) ورسائل «الضباط» في رسائل الإنيغما البحرية؛ يسجل فيلم تصوير 35 ملم التشفير من رسالة إلى خمس رسائل بالتوتر العالي (مثل N, R, E) في جميع المراكز لقابس معين ونظام دولاب واعدادات حلقة من ثم مقارنتها مع فيلم نص الرسالة.

الرأس النحاسي:

آلة مقارنة بشريط مثقب بعرض 70 ملم، يقارن بصرياً توالي مائة مجموعة من الرموز في المرة الواحدة وذلك باختبار «التعتيم» في أشرطة الرسائل الموضوعة فوق بعضها والمعدّة بترميز تكميلي؛ تستخدم لوضع الرموز المشفرة فوق بعضها.

تيسي:

استخدمت للبحث عن التوالي الهندسي في نص الشيفرة؛ يجري بفحص فيلم (35 ملم) فحصاً آلياً لرسالتين لانتاج شريط مثقب يسجل أحداث تكرار الأحرف في عشرين مركز لكل من هذه المراكز؛ الأشرطة المثقبة الناتجة، التي سجلت الفسحة بين الأحرف المتكررة في كل رسالة، توضع بعد ذلك فوق بعضها وتفحص بالنظر بحثاً عن صيغ معينة.

5202:

آلة مقارنة بفيلم 35 ملم تستخدم لانزلاق النص الألماني المشفر على الطابعة عن بعد (توني) على متواليات رئيسية معروفة؛ قادرة على المقارنات المعقدة والاختبارات الإحصائية.

بنتها شركة ايستمان كوداك لصالح جيش الولايات المتحدة؛ وسلمت واحدة إلى الوحدة GC&CS في نيسان من عام 1945.

معدات الأشرطة الورقية الأخرى

ماثيو:

آلة تعتمد على المقوية لتنفذ عمليات الجمع والطرح بدن حمل من أجل تعرية إضافية. شريط ورقي لكتابة الرسائل وذلك من أجل الإدخالات والإخراجات.

مايك:

عداد تكرار الأحرف الثنائية؛ الإدخالات من شريطين لكتابة الرسائل؛ ومجال مقوية يوجه الإشارات إلى واحد من 676 عداد كهربائي يحسب جميع الاحتمالات الممكنة (26 × 26) من الأحرف الثنائية.

العمالقة

روبنسون:

بنت هذه الآلة الوحدة GC&CS للهجوم على («توني»)؛ تطبع الأشرطة عن بعد لنص رسالة، وتلقم الترددات الرئيسية في الوقت نفسه من خلال قارئين في أطواق

مستمره تسير في البدايات الممكنة كلها؛ وتقوم عدادات اليكترونية بتعداد المصادفات.

العملاق:

نسخة متقدمة من روبنسون وفيها يرمز التسلسل الأساسي داخلياً بواسطة دارات اليكترونية؛ وتحتوي على ألفين وخمسمائة أنبوب مفرغ لتقوم بدور ذاكرة وترمّز العمليات الحسابية جبرياً (بولينيا).

--- --- ---

الملاحظات

اختصارات مستعملة في الملاحظات:

AI: مقابلة المؤلف.

BI: المخابرات البريطانية في الحرب العالمية الثانية (هنسلي وأصحابه).

CAC: مركز أرشيف تشرشل، جامعة كامبردج.

GC+CS: الشيفرة الحكومية، وتواريخ مدرسة التشفير الرسمية للحرب العالمية الثانية، المتحف الوطني للكتابة السرية

HCC: مجموعة الكتابة السرية التاريخية، الأرشيف الوطني بكلية بارك.

NACP: المتحف الوطني بكلية بارك.

OH: تاريخ شفهي.

PRO: ديوان السجل العام، كيو، المملكة المتحدة.

الإشارات الكاملة للمراجع المطبوعة وغير المطبوعة الموجودة بصورة مختصرة في الملاحظات قد توجد في المراجع.

- البحرية الألمانية 1937/5/1، تاريخ الكوخ الثامن، رقم 4685، مجموعة الرسائل السرية التاريخية، 13.
- مجموعات من قائمة مطبوعة: الإينغما إجراء عام، رقم 1679، مجموعة الرسائل السرية التاريخية 10، 11، 15؛ انظر أيضاً إيرسكين، الإينغما البحرية: صلة مفقودة، 494–496.
- عرفت باسم "بيبي" مقالة تيورنغ حول الإينغما، رقم 964، مجموعة الرسائل السرية التاريخية 141، (مفككو الشيفرة) إعداد هنسلي وستريب، 114؛ قسم الفرقة بقيادة جونز، HW3/164، ديوان السجل العام.
- من الممكن استرجاع الرمانة: مذكرة ج هـ. هوارد إلى القائد انغستروم، 21 آب 1942، الموضوع: موقع الإعداد الأساسي بعد حل القنبلة حلاً كاملاً، الرمانات، رقم 2338، مجموعة الرسائل السرية التاريخية.
- بناء أبجدية الشيفرة: وصف كامل، مع أنه غير واضح، للنظرية التي يقوم عليها المبدأ الأساسي Banburismus موجود في تاريخ الكوخ الثامن، 4685، مجموعة الرسائل السرية التاريخية 16–20.

- الرايات الملكية، ترفع الملوك عالياً: (مفككو الشيفرة) إعداد هنسلي وستريب، 158.
- تواتر الرسائل بنص الشيفرة البنفسجية: ديفرز وكرو، الرسائل السرية بالآلة، 325 تذكر بصورة غير صحيحة أن تواتر أرقام (6) أعلى في نص الشيفرة وذلك لأن كل رقم (6) يحل محله ست بدائل، بينما أرقام (20) فلكل منها عشرون بديلاً محتملاً، لكن هذا التأثير يلغي تماماً بوجود عشرين رقماً من (20) مقابل كل ستة أرقام من (6) بعبارة أخرى، مع أن العشرينات يستبدل كل منها بعشرين بديلاً مختلفاً، فيوجد منهم الكثير للبدء بها، بالحقيقة، إن ما يقرر التواتر الذي تظهر فيه الحروف في كل مجموعة في النص المشفر، هو التواتر الوسطي في النص البسيط للأحرف التي تتألف منها كل مجموعة.
- في النص الياباني بأحرف رومانية: ديفرز وكرو الرسائل السرية بالآلة 236–237.
- فرص اكتشاف روزين، روليبت (قصة سحر) 148–149.
- دائرة سريعة، أو متوسطة، أو بطيئة، الآلات اليابانية، 9 آذار 1945، الإينغما (مؤتمرات ونظرية ومعلومات ذات علاقة) رقم 1737، مجموعة الرسائل السرية التاريخية.
- كانت المجموعة OP–20–G تشغل ما يقرب من 445 جهاز استقبال: بينسون، مخابرات الاتصالات في الولايات المتحدة، 67.
- شبكة بعيدة المدى في المملكة المتحدة، رحلة العقيد ماك كومارك إلى لندن، أيار–حزيران 1943، رقم 3600، مجموعة الرسائل السرية التاريخية 40.
- RAM، وصف موجز لمعدات RAM، رقم 1494، مجموعة الرسائل السرية التاريخية، مطلوب للبحث آلة تحليل سريعة، رقم 2803، مجموعة الرسائل السياسية التاريخية، تطوير RAM (آلة تحليل سريعة) رقم 2808، مجموعة الرسائل السرية التاريخية، هيبو رقم 1548، مجموعة الرسائل السياسية التاريخية، طلب معدات RAM، رقم 2701، مجموعة الرسائل السرية التاريخية، ملف RAM، رقم 3315، مجموعة الرسائل السياسية التاريخية، الـ 5202، رقم 2748، مجموعة الرسائل السرية التاريخية.

- القنابل: قسم الفرقة بقيادة جونز HW3/164، ديوان السجل العام؛ تقرير تحليل الرسائل السرية على الآلة الصفراء رقم 3175، مجموعة الرسائل السرية التاريخية؛ تاريخ القنبلة، رقم 1736، مجموعة الرسائل السرية التاريخية، معلومات عن القنابل مأخوذة من الملفات الخاصة بالسيد فليتشر، HW3/93، ديوان السجل العام؛ كروفورد Auto scrit cher + Superscritcher، وصف حدسي موجز لمعدات تحليل الرسائل السرية لمشكلات الإينغما، رقم 4645 مجموعة الرسائل السرية التاريخية، وايتهيد (الكوبرا والقنابل الأخرى).
- كولوسي: (مفككو الشيفرة)، إعداد هنسلي وستريب ص 139–162، راندیل (العملاق Colossus)؛ فلورز (تصميم العملاق).

--- --- ---