السيطرة على الأثير

بين مئات الكتبة وعاملي الطباعة والرياضيين والكهربائيين والميكانيكيين ومهندسي IBM المعينين حديثاً والذين وصلوا إلى آرلنغتون هول في صيف 1943، كان هناك شخصان من طرفي العالم المتضادين، وهما متضادان من جميع النواحي فعلاً. وليام وايزباند، ويبلغ من العمر 35 سنة، ولد من أبوين روسيين، ونشأ في مصر. وهاجر إلى الولايات المتحدة في العشرينيات، وأصبح مواطناً أمريكياً في سنة 1938. كان وايزباند يتكلم اللغة الروسية بطلاقة؛ وكان اجتماعياً ومحبوباً في آرلنغتون هول حيث تلقى دورة مدتها أربعة أسابيع لتعلم اللغة الطليانية في حزيران 1943 قبل قيامه بجولة بمهمة في أوربا.

أما سيسيل فيليبس فكان حلو الكلام ويبدو أنه شاب (18 سنة) غير طموح من جبال كارولينا الشمالية، وترك الكلية ولم يقبل في الجيش بسبب تسطح قدميه. طلبت منه أمه أن يعود إلى الكلية أو أن يجد لنفسه عملاً، وهكذا تصادف حضوره إلى مكتب التشغيل في بلدته آشفيل في اليوم الذي جاء فيه الملازم بالجيش من واشنطن ومعه عدد من الوظائف وكان عليه أن يختار من يشغلها. سأله الملازم، «ما رأيك في الذهاب إلى واشنطن وتصبح محللاً للشيفرة؟». وأجاب فيليبس، «يبدو ذلك مثيراً للاهتمام». فكان من الواضح أن الملازم دُهش لأن شخصاً عرف عما كان يتحدث فعلاً، فقال: «تعني أنك تعرف ما يعني ذلك؟».

كان فيليبس يعرف لأنه ذات مرة كان لديه لعبة «خاتم آني اليتيمة الصغيرة الذي يحلل الرموز»، مع أن ذلك أبعد ما أمكنه أن يتذكر من معلوماته. لكنه عُيّن

سريعاً ككاتب من الدرجة GS – 2 براتب سنوي مقداره 1440 دولار، وطُلب منه أن يحضر إلى آرلنغتون هول بعد أسبوع في 22 حزيران 1943. كانت أولى واجباته أن يختم التاريخ على الرسائل المعترضة الواردة. وبعدما أثبت كفاءته في ذلك العمل تخرج إلى عمل آخر هو فرز الأوراق. كان رئيسه الأول في آرلنغتون هول، الملازم بيل فليشمان، قد تلقى دورة في تحليل الشيفرة في سيتي كوليدج في نيويورك و«أراد أن يُعلّم بالطريقة السيئة» كما يذكر فيليبس، وأصبح يوفر ساعتين من كل يوم ليعلم فيليبس وستة موظفين جدد آخرين أسرار تحليل الشيفرة. وتبين سريعاً أن مواهب فيليبس تتخطى عملية الختم والخرز. في 1 أيار 1944 أخذوه إلى نهاية خلفية لأحد الأجنحة من البناء A حيث فصلت منطقة من الجناح بفاصل خشبي عن بقية الجناح المفتوحة. فالناس الذين يسلكون الممر من البناء لا يلاحظون وجود هذه المنطقة، وإن لاحظوها، لم يتمكنوا من الدخول إليها. وعرف العاملون في آرلنغتون هول ألا يسأل بعضهم البعض الآخر عما يعملون، ولكن إن سأل شخص ما، ما الذي يجري خلف الجدران الخشبية، فمن المؤكد ألا يتلقى أي إجابة. في الليل تغطى الطاولات بالقماش. وتختفي عدة العمل، كالقواميس والخرائط وما شابه، بحيث لاترى. قيل لفيليبس إن هذه هي «المشكلة الروسية»، وإنه سيعمل هنا لآن.

لم تكن المشكلة الروسية موجودة رسمياً. وفي المخطط التنظيمي تبدو «كمشكلات خاصة» أو «B–11–6–9» وتصمم كواحدة من الأقسام الثانوية العديدة من فرع تحليل الشيفرة. وكانت سراً حتى على البريطانيين. قبل سنتين اكتشف ضابط الاتصال البريطاني، جيفري ستيفنز، مثل GC&CS أن البحرية تجمع البرقيات الدبلوماسية الروسية وتفكر في أنها «إن عاجلاً أو آجلاً ستحاول تفكيكها لأنهم لا يثقون بالروس أكثر من قدرتهم على إلقاء مدحلة تجارية». عندما بدأت مخابرات الإشارة بالعمل على تحليل الرسائل الديبلوماسية الروسية في شباط من 1943 بتوجيهات غامضة قليلاً من أوكراني يدعى ليونارد زيبكو، وسرعان ما علم بها ستيفنز الذي كان نشيطاً في تجواله في آرلنغتون هول. بعد أسابيع قليلة أعلن على الملأ إغلاق هذا القسم. وبعد شهرين أعيد إلى العمل بهدوء،

وهـذه المـرة كـان تحـت قيـادة فرديناند كـوديرت، وهـو لغـوي موهـوب ويـتكلم الروسية بطلاقة. وبدا أن الحيلة بكاملها مصممة لتضليل البريطانيين، بعد بضعة أشهر كتب كوديرت مسودة طلب إلى المكتب في آرلنغتون هول الذي كان يقوم بتبادل المعلومات مع الوحدة GC&CS: «هل لدى البريطانيين أي معلومات حول الشيفرة الروسية الديبلوماسية أو التجارية؟» ولكن يبدو أن شخصاً تدخل ولم يُقدَّم الطلب إلى لندن. وبقيت الرسائل الديبلوماسية في أي حادث النقطة الحساسة جداً بين الأمريكيين والبريطانيين. في الواقع، كانت الوحدة GC&CS قد بدأت عملها في الرسائل الروسية غير العسكرية وذلك في الوقت ذاته، في حزيران 1943. وركز مشروعهم، الذي سمي إيسكوت (ISCOT) بصورة أولية على الإشارات التي مرت بشبكات الإذاعات السرية التي اكتشف البريطانيون أنها تعمل بين موسكو والحزبيين الشيوعيين في ألمانيا التي تحتلها أوربا. عند نهاية الحرب فقط سمح البريطانيون والأمريكيون بأن يعرف الطرفان ماذا يفعلان، وعند هذا الحد بدأ التعاون الكامل ضد حليفهما السابق الذي يتحول سريعاً لأن يكون عدوهما الجديد.

تجنبت الاتفاقية البريطانية الأمريكية (BRUSA) في شهر أيار 1943 موضوع الرسائل الديبلوماسية تجنباً حكيماً وحذراً؛ فمع أنها تنص على تعاون كامل وتبادل كامل لنتائج تحليل الشيفرة والرسائل المعترضة، فإنها اشتملت فقط على الرموز المستخدمة لدى الجيش والقوى الجوية لقوات دول المحور وكذلك لدى المخابرات الألمانية «Abwehr» بصورة خاصة، ظهرت علاقة عمل جيدة غير رسمية بين GC&CS وقسم دينيستون الديبلوماسي في شارع بيركلي. لكن البريطانيين وضعوا خطاً لتزويد واشنطن بنسخ من الرسائل الديبلوماسية المتعلقة بدول حيادية التي ترسل برقياً وهي التي تسيطر عليه بريطانيا، لكنهم ينظرون نظرة حذرة إلى الطلبات الأمريكية حول مواد الشيفرة من دول مثل العراق التي ما زالت في مجال التأثير البريطاني. نقل ضابط ارتباط أمريكي من آرلنغتون هول في تشرين الثاني 1944 بأن دينيستون «لديه انطباع يتكرر بأننا نستخدم الحرب لاستغلال المعرفة

البريطانية في تحليل الشيفرات» في مجالات لا علاقة لها بكسب الحرب. وتوقفت الولايات المتحدة عن إرسال معلومات إلى شارع بيكرلي حول شيفرة دول أمريكا اللاتينية في أيلول من عام 1944.

إن اتساع معاملة «القرض والاستئجار» لتشمل السوفييت زادت من الوجود السوفيتي في الولايات المتحدة. فكان هناك بعثات تجارية ولجان مشتريات ومفتشون في المعامل التي تنفذ طلبات السوفييت. وكان هؤلاء الممثلون الروس يتصلون مع موسكو بصورة منتظمة بطريق البرقيات التجارية. وعندما بدأ القسم الروسي في آرلنغتون هول بحل جميع هذه البرقيات، اتضح سريعاً أن هناك خمسة أنظمة شيفرة مختلفة في الاستعمال. أولها، المستخدم في نصف جميع البرقيات التي تتعامل بالمواضيع التجارية لأنها تأتي من أمكنة حيث توجد لجان الشراء السوفيتية. أما الأنظمة الأربعة الأخرى فيبدو أنها ديبلوماسية فقط تأتي من السفارة والقنصليات. واتضح أيضاً، كما كان معروفاً منذ العشرينيات، أن السوفييت يستخدمون رموزاً من أربع أو خمس خانات يتم تشفيرها بطريقة «الصفحة لمرة واحة». إن استخدمت استخداماً صحيحاً – وإن كانت الطريقة «الصفحة لمرة واحدة» بطريقة عشوائية حقاً – فلا يمكن تفكيكها.

لكن ما دام لا يوجد شيء آخر ليجربه، قرر أحد أعضاء الفريق وهو ريتشارد هالوك، الذي كان أستاذ علم الآثار في جامعة شيكاغو، أن يبدأ بحثاً بوهيميا في الرسائل التجارية. ابتدأ في خريف سنة 1943، فجعل قسم الآلة يثقب أول خمس مجموعات من الرسائل من أصل عشرة آلاف رسالة تجارية وذلك على بطاقات IBM وكتابتها بترتيب رقمي. وعند تنفيذ ذلك، تبين وجود سبع ضربات مزدوجة، ويمكن أن يكون ذلك محض صدفة. ولكن عندما بدأ هالوك وفريقه العمل خلال الأزواج السبعة للرسائل المتطابقة واستخدم لذلك أسلوباً قياسياً لصنع جداول فروقات، وجدوا أنهم استطاعوا اكتشاف بعض الإضافات من «الصفحة لمرة واحدة» ومجموعات الرموز وراءها. واتضح سريعاً أنهم كانوا يصبون شيئاً. فلم تكن «الصفحات لمرة واحدة» صفحات لمرة واحدة؛ وكان بعضها لأكثر من

«الصفحة لمرتين». وظهرأن كل رسالة قد شفرت بدءاً من قمة الجانب الأيسر لصفحة «المرة الواحدة»، وكان هناك ستون مجموعة إضافات لكل صفحة، وبين الفينة والأخرى، يعاد استخدام الصفحة كاملة.

تقدم العمل بطيئاً خلال الشتاء والربيع. وفي تموز 1944، بينما كان الجهد الأولي مستمراً في الشيفرة التجارية، عُيّن فيليبس مسؤولاً عن بقية المشكلة الروسية. وكان هذا يعبر عن شيئين: الأول تصويت بالثقة على الشاب المحلل للشيفرة ذي الثمانية عشر ربيعاً، والثاني بيان بالأمل المتدني بالنجاح الذي يبدو في تفكيك الشيفرة الديبلوماسية. كان هناك القليل جداً من هذه الرسائل للابتداء بها، وكانت مقسمة إلى أربعة أنظمة مختلفة أظهرت الشواذ والاستثناءات أكثر.

كان فيليبس يمحص الرسائل ويدققها لكنه لم يتقدم كثيراً في أي اتجاه عندما قرر في شهر تشرين الثاني أن يلقي نظرة على رزمة رسائل من نيويورك إلى موسكو. وبصورة غير واضحة بدأ يظهر وسط بحر من الأرقام الرباعية التي لا معنى لها شكل ما. يجب أن يُنتج الرمز المشفر توزعاً عشوائياً للخانات. لم تكن مجموعة الرموز الأولى التي ينظر إليها فيليبس عشوائية، ولكن هناك شيء شاذ شذوذاً بسيطاً حولها. بدأ يعد تكرار كل خانة؛ ينبغي أن تظهر كل منها 10٪ من المرات. ظهرت الخانة 6 عشرين بالمائة من المرات. عند هذه النقطة أخذ حزمة الرسائل إلى جنفياف غروتيجان Genevieve Grotjan – وهي من شهرة البنفسجة Purple وقد عُينت في المشكلة الروسية – وقالت على الفور: «يبدو أن هذا مفتاح واضح: وكانت تعرف مجموعات الأرقام الرباعية التي تبدأ كل رسالة بوصفها مجموعات مضافة من الزاوية اليسرى العلوية من «صفحات المرة الواحدة» تستخدم مرة أخرى في الشيفرة الديبلوماسية أيضاً. والأكثر من ذلك، كان فيليبس وغروتيجان قد فككا نظام المؤشر الذي يقول أي صفحة استخدمت: فالمؤشر الذي يبث في بداية كل رسالة هو مجموعة الإضافات الحقيقية في الزاوية اليسرى العليا من الصفحة المفتاح التي تستخدم في تشفير النص الذي يلي.

وتم الضغط على آلات IBM لتكون في الخدمة مرة ثانية؛ وكذلك الآلة الرأس النحاسي Copper Head، وآلة المقارنة السريعة للبحرية، وذلك للوصول إلى ضربات مزدوجة في بضعة آلاف من الرسائل التي أرسلت على أنظمة ديبلوماسية سوفياتية أخرى. إن اللاعشوائية في مجموعة الإضافات الأولى التي حددها فيليبس كانت مجرد ضربة حظ، وربما نتيجة للآلة الطابعة التي استخدمت لتوليد «صفحات لمرة الواحدة» آلياً، والتي عملت بانحياز بسيط. في الواقع، إن نسبة صغيرة فقط من صفحات الإضافات كان فيها الميل (الانحياز) هذا، ولو أن فيليبس اختار رزمة مختلفة من الرسائل لما استطاع تحديدها. وكذلك لو أن مركز التشفير في (الكي جي بي KGB) قام بواجبه بشكل صحيح لما استطاع آرلنغتون هول بحث 750000 برقية وأن يجد 30000 صفحة من «صفحات لمرة الواحدة» تستعمل أكثر من مرة. ويتضح فيما بعد أن (الكي جي بي KGB) قد طبع لفترة بضعة أشهر تحت ضغط النقصان في زمن الحرب نسخاً مزدوجة ووضعها معاً وغالباً ما أعطاها أرقام صفحات مختلفة على أنها «صفحات لمرة الواحدة» منفصلة.

ويتضح أيضاً أنه بينما استخدم واحد من الأنظمة الأربعة الديبلوماسية لأغراض قنصلية قانونية تماماً، خصصت الأنظمة الثلاثة الأخرى إلى (الكي جي بي KGB)، والمخابرات العسكرية السوفيتية والمخابرات البحرية السوفيتية. كشفت 2900 رسالة بثت ما بين 1940 و1948 التي قرأها آرلنغتون هول، وبعضها تأخرت قراءتها حتى السبعينيات، وجود عملية تجسس سوفيتية واسعة في الولايات المتحدة.

كان من أكبر سخريات الحرب الباردة أن المكارثيين بمعلوماتهم السيئة وجنون الشك وهجومهم الشرير، والأذى الذي أصابوا به أشخاصاً بريئين تماماً، كانت حقيقة تسرب الشيوعية إلى الولايات المتحدة في مناطق قليلة على الأقل، أسوأ مما كانوا يشكون به. أظهرت البرقيات أن السوفيات اخترقوا مشروع مانهاتن في نقاط متعددة، على الأقل أربعة عملاء في لوس ألاموس Los Alamos ينقلون تقارير إلى شبكة يتم التحكم بها من نيويورك. وكانت البرقيات تشير إلى مصادر مطلعة عليها في الأركان العامة في وزارة الحربية، وفي (OSS دائرة

الخدمات الاستراتيجية*)، وفي السفارة البريطانية في واشنطن. وتذكر هذه التقارير يوماً بيوم عمل أعضاء الحزب الشيوعي في الولايات المتحدة الذين ينقلون التقارير مباشرة إلى موسكو عن المعامل العسكرية والتقنيات العسكرية. ويذكرون عملية وحشية قام بها (الكي جي بي KGB) لمطاردة فارين من الأسطول التجاري السوفيتي، ويعيشون على الساحل الغربي للولايات المتحدة واختطافهم وإعادتهم إلى الاتحاد السوفياتي. تظهر التفاصيل الحرفية (للكي جي بي KGB) أن الرسائل، بما فيها كلمات السر وإشارات التعريف، والرقابة المقابلة، والتوظيف والتزوير كفاءة حرفية عالية ووكالة مخابرات خبيرة تقوم بعملها.

في عام 1945 عاد وايزباند إلى آرلنغتون هول، وعيّن في القسم الروسي «كمستشار لغوي». وقف في يوم من الأيام وراء كتف ميريديث غاردنر، وهو لغوي آخر في القسم، بينما كان غاردنر يستخلص نص برقية من (الكي جي بي KGB) تحتوي على قائمة من علماء الذرة الأمريكيين الذين يعملون في مشروع مانهاتن. بعد خمس سنوات فصل وايزباند من عمله بعدما أخبر المهندس الفضائي جيمس أوين يورك – الذي كان يعمل في معامل نورثروب ودوغلاس على الساحل الغربي في أواخر الثلاثينيات والأربعينيات – مكتب التحقيقات الفيدرالي أن وايزباند كان نقطة الوصل لنقل المعلومات السرية حول الطائرات ومحركات الطائرات إلى السوفييت.

رفض وايزباند أن يعترف أو ينكر أنه كان جاسوساً للسوفييت مع أن إحدى الرسائل المعترضة تشير إليه بصورة واضحة. لكن كان هناك شخص آخر، جاسوس شيوعي دون شك، يعرف كل شيء عن المشروع الروسي في آرلنغتون هول (والذي سيعرف اسمه الرمزي «فينونا Venona»). وصل كيم فيلبي إلى واشنطن في خريف عام 1949 كضابط اتصال من المخابرات البريطانية، وأصبح يزور آرلنغتون هول سريعاً كما أصبح زائراً منتظماً، يحيث تسلم إدارة القسم الروسي بكاملها.

* Office Stratigic Services = OSS.

لم يمض زمن طويل بعد ذلك حين بدأ عملاء موسكو من الأمريكيين، لا سيما أولئك الذي تعاملوا بالتجسس الذري كلاوس فوكس، يتلقون تعليمات بأن يستعدوا للهرب من الولايات المتحدة عبر المكسيك. وحوالي هذا الوقت توقف السوفييت عن استخدام صفحاتهم المزدوجة من «الصفحة لمرة واحدة»، مع أن هذا لا يبدو أن له علاقة بأي شيء عرفوه عن طريق الجواسيس: فقد قاموا بكل بساطة بمراجعة الصفحات المتكررة، والخطأ الذي حدث خلال الحرب والذي أدى إلى طباعتها في المكان الأول ينبغي ألا يتكرر.

كان لدى بليتشلي بارك جاسوس روسي أيضاً – أو يحتمل أن يكونوا جواسيس. عمل جون كيرن كروس في الكوخ 3 ما يقارب السنة من عامي 1942 و1943. «واحتفظ بجذوره في لندن»، وشرح لزملائه بأنه يسافر إلى المدينة الكبيرة في عطلة نهاية الأسبوع. وما لم يعرفه زملاؤه هو أنه كان يضع في حقيبته في كل أسبوع نخبة مختارة من الرسال المفككة حول الجبهة الروسية وينقلها إلى مساعده السوفيتي في لندن. ما لم يكن يعرفه كيرن كروس هو أن معظم الرسائل المفككة، إن لم يكن كلها، كانت ترسل إلى موسكو عبر أقنية رسمية على كل حال. ويبدو أن الخوف الدائم من الاعتقال سبب الكثير من الإرهاق، فطلب كيرن كروس نقله إلى MI6 في صيف 1943.

وتظهر الإشارة إلى جاسوس سوفيتي آخر محتمل في بليتشلي في رسائل فيرونا المفككة كان اسمه بارون، ويبدو أنه عمل في بليتشلي قبل كيرن كروسي؛ أُرسلت واحدة من رسائل فيرونا المفككة إلى موسكو في أوائل عام 1941، وكانت تحتوي على النص الحرفي لرسالة مفككة من ULTRA، كان الكوخ 3 قد قرأها. من الملاحظ أن وايزباند وكيرن كروس وبارون هم الجواسيس الذين اخترقوا عمليات تفكيك الشيفرة في بريطانيا وأمريكا خلال الحرب بكاملها – وكانوا يعملون لحساب حليف اسمي. أما جواسيس المحور فلم يقتربوا من معرفة ماذا كان أعظم سر، بعد القنبلة الذرية، في الحرب العالمية الثانية.

--- --- ---

لقد برهن محللو الشيفرة لدى الحلفاء عند هذه النقطة أن أدق الأخطاء يكفي لأن يجعل أكمل صروح الكتابة السرية مكشوفة بشكل واسع. حتى «الصفحات لمرة واحدة» غير محصنة، فحتى «الصفحات لمرة واحدة» التي تستخدم لمرة واحدة حقاً (بخلاف الصفحات الروسية). تحدت الشيفرة الدبلوماسية الألمانية الحل على مدى بضعة عقود من الزمن، ولكن مع اختراق شيفرة فلورادورا في عام 1943، تحول الانتباه إلى شيفرة أكثر أمناً وهي GEE، وهي من نظام «الصفحة لمرة واحدة». ولكن كانت هناك دائماً فرصة استخدام الألمان هذه الصفحات أكثر من مرة واحدة، وكان هناك بضعة آلاف من المطابقات المتوافرة الآن من رسائل كانت قد وُجهت إلى سفارات وقنصليات مختلفة في آن معاً وهي تستخدم الشيفرتين فلورادورا وGEE. وكان هناك أيضاً 3651 صفحة من مفتاح «الصفحة لمرة واحدة» حقيقي، وتم الحصول عليه من رسالة اعترضها مكتب FBI في 1940 من المراسل فاربن I. G. Farben. ويحتمل أن ذلك كان مستحيلاً، ووضع في العمل 12 شخصاً للعمل في المشكلة في آرلنغتون هول. وقرروا صنع عمل ضخم آخر لـ IBM. ويتطلب هذا وضع قائمة فيها كل مجموعة معروفة أو مجموعة إضافات مكتشفة في ترتيب رقمي مع موقعها مع رقم الصفحة، وصفها، وعمودها في «الصفحات لمرة واحدة». لم يكن هناك تكرار الاستخدام يعثر عليه، لكن كان هناك واحدة من تلك التموجات الخفيفة في العشوائية التي تهز هوائيات محللي الشيفرة. وكان طبيعياً أن توجد مجموعات إضافات مفردة وتظهر أكثر من مرة واحدة بين مئات ألوف الإضافات ذات الأرقام الخمسة بطريق الصدفة. والمفاجأة أن المجموعات التي جاءت قبل المجموعات المكررة وبعدها تتجه لأن يكون فيها عدد غير عادي من الأرقام المشتركة. وما جاء بعد ذلك كان عملاً خارقاً من أعمال آرلنغتون هول في تحليل الشيفرات، وهو تمشيط الأرقام رقماً بعد رقم في الإضافات بحثاً عن صيغة مهمة. ووجدوها في كانون الثاني 1945. وجاءت فكرة أخرى من فحص دقيق لأخطاء طباعية صغيرة في الأرقام على صفحات «الصفحة لمرة واحدة» الحقيقية. وأصبح واضحاً أن كلاً من المجموعات الثماني والأربعين ذات الأرقام الخمسة في الصفحة تطبع على دولاب طباعة مختلف؛ بعبارة أخرى، جميع الخانات (الأرقام) وهي 240

قد طبعت بمجموعة من الدواليب التي تدور بحسب صيغة تختلف من صفحة إلى صفحة. وكانت الأرقام على كل دولاب موجودة بنظام غير متسلسل. ولكن ما أن تكتشف الحيلة، يتهيأ لمحللي الشيفرة طريقة لتخمين التسلسل المفتاح لصفحات «الصفحة لمرة واحدة». وجرى تشغيل آلة IBM لاختبار نص مشفر مقابل تدوير مختلف للإضافات. في حزيران 1945، كان 110 أشخاص يعملون على الشيفرة GEE، وخلال النصف الأول من عام 1945 أعطت الرسائل بضع قطع حساسة من المخابرات التي لم تكن معروفة بوسائل أخرى حتى ذلك الحين، وشمل ذلك حقيقة أن اليابانيين قد بدؤوا باستخدام دبابة متوسطة جديدة وسلاحاً ذاتي الضغط.

والإسفين الرفيع – الذي دقه فيما بعد جبروت الرياضيات المركزة الذي كان يجمعه بليتشلي بارك حتى ذلك الحين – استخدم أيضاً لفصل شيفرات الجيش الألماني من الطباعة عن بعد. تستعمل الطابعات عن بعيد القياسية نظام ترميز ثنائي ذي خمس قطع، فيه كل رمز يتمثل بسلسلة من خمس نبضات (فتح / إغلاق On/off). مثلاً، يتمثل الحرف A بـ 11000، والحرف Bبـ10011، وعودة حامل الورق 00010. وكانت فكرة إضافة دواليب ترميز إلى الطابعة عن بعد القياسية كي يتم التشفير آلياً لهذه التيارات من النبضات يتابعها المصالح العسكرية الألمانية في أوائل الحرب، وفي عام 1941 بدأت محطات المراقبة البريطانية تعترض إشارات «غير إشارات مورس» وكانت هذه الإشارات تتولد من إشارات التشفير التجريبية هذه. وأعطى بليتشلي بارك لهذه الإشارات الاسم الرمزي «فيش Fish»، ولم يستغرق وقتاً طويلاً ليخمن ماذا كانت هذه الإشارات. وسوف يتضح فيما بعد أنها كانت بضع آلات مختلفة في الاستعمال. فقد بنت شركة لورينز الآلات المعروفة «المرفقات المشفرة، SZ40 و42» التي حصلت اسم من بليتشلي بارك هو «توني Tunny»؛ وبنت شركة سيمنز الآلة «الكاتب السري T52»، وعُرفت في بليتشلي بإسم السمكة «سترجون».

الرياضيات الثنائية يمكن تحقيقها بسهولة في الآلات المعدنية، وكان هذا هو جزء من جمال الاختراع الألماني. فللآلات مجموعتان، في كل مجموعة خمسة

دواليب تشفير، دولاب واحد لكل جزء من تشفير الآلة الطابعة عن بعد. في كل وضع يسبب الدولاب دارة كهربائية إما لإرسال نبضة أو لا – 1 أو صفر. ولكل جزء، تضيف مجموعات من المقويات (الريليات) نبضات من مجموعتي دواليب التشفير إلى النبضة الناجمة عن لوحة مفاتيح الطابعة عن بعد للرمز الذي جرى الضغط عليه (أو في أغلب الأحيان، يتم تثقيب شريط مسبقاً للطابعة عن بعد). العملية بكاملها آلية تماماً، والتدفق الناجم هو عبارة عن الأعداد (1) و(الأصفار)، وعلى شكل (بيب) و(فراغ) يمكن بثها بسرعة عالية جداً عبر أسلاك أرضية أو عبر الراديو.

كانت المشكلة المباشرة للوحدة GC&CS اكتشاف توالي الإضافات الخمس المستخدمة لتغطية رموز النص البسيط، وهنا برزت المواهب الكلية لجون تيلتمان مرة أخرى إلى المقدمة في 30 آب 1941، أرسل عامل ألماني رسالة طولها أربعة آلاف رمز. ولم يتسلمها المرسلة إليه بصورة صحيحة فطلب إعادة إرسالها. فأرسلها العامل مرة ثانية مستخدماً وضع البدء ذاته للدولاب تماماً، لكنه اختصر الكلمة الأولى وهي «رقم الرسالة». وكانت هذه قطعة من المطابقة التي لا تصدق. وبعد طرح جدولي النص المشفر، الواحد من الآخر، وحذف الإضافات من المعادلة بالكامل، نتج تيار من مجموعات من خمسة قطع، وهي الفرق بين نصي الرسالة البسيطين. وشرع تيلتمان يعمل عليها، يعتمد على الحزر أحياناً، ويكتشف أنها كانت ببساطة النص نفسه مع انتقال بعض الرموز بين بعضها. وبعد طرح النص البسيط المكتشف من النص المشفر الأصلي، نتج منه تسلسل رئيسي طوله أربعة آلاف رمز.

وكانت المشكلة الأخرى تخمين صيغ الدواليب التي تولد مثل هذا التسلسل. ووقعت المهمة على وليام ت توت، وهو شاب رياضي من كامبريدج. أخذ القطعة الأولى من كل إضافة ذات خمس قطع، وجرب كتابة التسلسل الرئيسي في جداول بأرقام مختلفة من الأعمدة حتى بدأت صيغة التكرار بالظهور في كل صف. فكرر العملية لكل قطعة من القطع الأخرى. بعد أربعة أشهر اكتشف عدداً من المراكز على كل دولاب وتسلسل الأرقام (واحد) والأرقام (صفر) في كل دولاب. واكتشف

الرسائل بوضعها فوق بعضها والمطابقة اليدوية واستطاع، من الناحية النظرية، أن يكتشف الإعدادات الأولية للدولاب لكل رسالة جرى بثها، وقد فضل الرائد رالف تيسترهذه الطريقة، وكانت مجموعته في «تيستري» في الجناح B قد عينت لهذه المهمة أولاً. أما ماكس نيومان، وهو رياضي وقد علّم تيورينغ في كامبريدج، فضغط من أجل طريقة أكثر آلية. أظهر تحليل توت Tutte أن مجموعة واحدة من الدواليب، وهي المسماة في بليتشلي بارك (س دواليب) تنتقل مع طباعة كل رمز؛ والمجموعة الأخرى (ع دواليب) تبقى لتضع امتدادات طويلة، وتتقدم في فترات غير منتظمة. وهذا يعني أن معظم الوقت، حوالي 70٪ من الوقت في الواقع، كل رمز يشفر بالرقم 1 على الدولاب ع، يتبعه مباشرة رمز آخر يشفر بالرقم 1؛ أو (صفر) يتبعه (صفر) آخر. وهذا يعني إن كان ناتج الدواليب ع لرموز سلسلة تُكتب ثم تضاف إلى نفسها فإنه تنتقل برمز واحد، عدد غير متناسب «للأصفار» قد يحدث، لأن الإضافة الثنائية دون الحمل

1 + 1 = 0 وصفر + صفر = صفر. وللنص البسيط هذ الانحياز أيضاً (على الرغم من أنه ليس كما يلفظ) بسبب حدوث الأحرف المزدوجة في الكلمات الألمانية، وكذلك طريقة الخط التي حددت أرقام (الواحد) وأرقام (الصفر) للأحرف المختلفة في الأبجدية في رموز الآلة الطابعة عن بعد. وهكذا مرة أخرى، إضافة نص بسيط إلى نفسه مع انحراف رمز واحد قد تنتج ايضاً رجحاناً بسيطاً «للأصفار». كانت النتيجة أن هذه المعالجة «نقل وإضافة» ذاتها على خيط من النص المشفر الحقيقي قد تعطي تسلسلاً من أرقام (الواحد) و(الصفر) التي تتجه غالباً لتسير على صيغة تولدها الدواليب س وحدها – لأن كلا النصين البسيطين والدواليب ع تحول نفسها إلى الصفر في المعادلة في معظم الوقت.

ما كان مطلوباً عند ذلك إعداد شريطين طويلين للآلة الطابعة عن بعد. يحتوي الواحد على النص المشفر مضافاً إلى نفسه مع نقلة واحدة؛ ويحوي الآخر على ناتج الدولاب س مضافاً إلى نفسه مع نقلة واحد، لكل مركز بداية محتمل في الدواليب س. فيقارن الشريطان بعد ذلك، الرمز إثر الرمز، ويجري تعداد عدد الصدف.

وينبغي أن ينتج مركز الإبتداء الصحيح في الدولاب س أكثر المصادفات بين الشريطين.

سميت أول آلة بنيت لتقوم بهذا العمل «هيث روبنسون» (وكان الاسم الانكليزي المعادل «روب غولدبيرغ»، وقد وصلت إلى «نيومانري» في أيار 1943. قال جاك غود، وهو رجل إحصاء وشكل جزءاً رهيباً من فريق نيومان للرياضيين: إن أعظم الاكتشافات السرية في الحرب هو شريط الطابعة عن بعد الذي يمكن أن يعمل بسرعة ثلاثين ميلاً بالساعة دون انقطاع. لكنه كان يتمدد – خاصة شريط الدولاب س الذي كان يستعمل مراراً. وكان هذا بالطبع قاتلاً، لأن الآنية الدقيقة بين الشريطين شيء أساسي بالنسبة للتعداد الصحيح. خدم تيورينغ كمستشار غير رسمي لمشروع (فيش) بقليل أو كثير، لكنه اقترح أن يستدعي نيومان تومي فلورز، وهو مختص بالاليكترون، من محطة أبحاث دائرة البريد. وقد صمم فلورز قبل الحرب وصنع مفاتيح لهاتف تستخدم الأنابيب المفرغة بدل أي أجزاء متحركة، واقترح حالاً أن الحل هو تصميم دارات تولد صيغ الدولاب س اليكترونياً. فاكتمل «الصرح رقم Colossus Mark I 1» وتم تركيبه في نيومانري في شباط من عام 1944؛ واشتمل على 1500 أنبوباً مفرغاً (واحتوت النسخ الأحدث على 2500 أنبوباً) وأثبت أنه موثوق أكثر كثيراً من روبنسون الذي قال عنه (غود Good) إن فيه سمة جيدة وهي أنه من الممكن عادة تشخيص الخطأ من صوت الضجيج الذي يحدثه – وأحياناً من الرائحة التي يصدرها، كما كان هناك مشكلة خاصة تتكرر وتسبب زيادة حرارة الآلة إلى درجة قد تشتعل معها.

كان الصرح أول جهاز حاسوب ذي ذاكرة كبيرة ويمكن برمجته بمفاتيح وحبال توصيل؛ وكان قادراً حتى على نوع من المنطق الشرطي، وتعديل الحساب بموجب المعطيات المتراكمة في دورة التشغيل. بعد الحرب كانت عشرة صروح تقوم بالعمل. مثل المعدات الأمريكية RAM، اشتمل الصرح على عناصر جديدة كثيرة من الحاسوب الرقمي الحديث دون أن يكون هو ذاته في الخط المباشر الذي يؤدي إلى الحاسوب؛ آلات أخرى من زمن الحرب، وخاصة الإينياك ENIAC الأمريكية،

التي احتوت على بطاقات تثقيب للإدخال والإخراج وعلى دارات لتقوم بالعمليات الحسابية والجذر التربيعي وعلى بعض القدرة لتخزين البرامج اليكترونياً، والتي لها فضل كبير لتدعي بأنها كانت وراء ولادة عصر الحاسوب.

لكن ما من شك في أن «الصرح Colossui» قد بذر بذور الحظ السعيد للمخابرات. فقد كانت دارات الطابعات عن بعد تصل برلين مباشرة مع رئاسة قيادات العمليات ومع المجموعات العسكرية وكشفت عن نوايا الألمان واستراتيجيتهم على أعلى المستويات. ومع أن الآلة (فيش Fish) لم تنافس إنيغما من حيث كمية الرسائل المفككة (ففي عام 1943 حوالي 300 رسالة فقط من فيش في الشهر الواحد مقابل ثمانية آلاف رسالة من الإنيغما)، لكنها قدمت سلسلة من التقارير التي لا تقدر بثمن عن تقديرات الألمان لتهديدات الحلفاء بالغزو في ربيع عام 1944 – واستعدادات الألمان لمجابهته. وخطة الحلفاء المخادعة التي ثبت أنها حاسمة في النصر (يوم دي) إنما اعتمدت بصورة كبيرة على عمل بليتشلي بارك في اختراق الآلة الألمانية للطباعة عن بعد.

--- --- ---

أوضحت ULTRA فعالية الخداع الكبير في يوم دي (D–Day)؛ وهي أيضاً صنعته بالمعنى الحقيقي جداً. في عام 1939 لم تكن مصلحة مخابرات الإشارة البريطانية تعرف اسم نظيرتها الألمانية (آبويهر الدفاع). بعد سنتين، ويعود الفضل الكبير لآلة ULTRA، كان البريطانيون إما يعتقلون كل جاسوس حاولت المخابرات الألمانية (الأبويهر) إدخاله إلى البلاد وإما يجعلون منه عميلاً مزدوجاً.

في كانون الأول من عام 1940، نجحت عملية أوليفر ستراتشي في بليتشلي بارك في فك الشيفرة التي تستخدمها (أبويهر) للاتصال بالمحطات الخارجية. واعتمدت العملية ISOS على من تخاطبه، فقامت مقام (توضيح إشارات أوليفر ستراتشي) أو (توضيح سلسلة أوليفر ستراتشي) أو حتى مصلحة المخابرات أوليفر ستراتشي)، ولكن مهما كان الاسم فإن العملية عالجت الشيفرة اليدوية لمصلحة المخابرات الألمانية أبويهر Abwehr، وسرعان ما نتج عن عملية ISOS حصتان

كبيرتان، الأولى، قدمت إلى قسم ديلي لوكس «ISK»، الذي يعالج النسخ التي لا قوابس فيها من الإنيغما، مع المطابقات التي تحتاجها لتفكك إنيغما المخابرات الألمانية Abwehr. وكان كثير من مراسلات المخابرات الألمانية تتضاعف ما بين الشيفرة اليدوية وأقنية الإنيغما، وكانت الإنيغما محجوزة للمحطات في الأراضي المحتلة حيث كان خطر فقدان آلاتها لتصل إلى أيدي العدو أقل كثيراً. (كانت نسخة المخابرات الألمانية من الآلة، فضلاً عن كونها دون قوابس، معقدة وتعقيدها في استخدام أقراص دوارة ذات نتوءات تبلغ بمجموعها 17) في كانون الأول من عام 1941 بدأ قسم نوكس بتفكيك رسائل إنيغما المخابرات الألمانية بصورة منتظمة.

وكان الحصة الأخرى، التي دفعتها عملية ISOS، والتي جمعها نوكس ISK عندما أصبحت متوفرة، هي تقديم تحذير مسبق من محاولات المخابرات الألمانية لتسريب عملاء إلى بريطانيا. في ربيع وصيف عام 1941 حاولت المخابرات الألمانية تهريب عملاء على ظهرسفن اللاجئين من النرويج ست مرات؛ كشفت عملية ISOS خمساً من هذه المحاولات في الوقت المناسب وتم اعتقال القادمين الجدد حين دخلوا بريطانيا. وكانت الحالة السادسة حالة الرسالة، التي كشفت وجود ثلاثة عملاء ألمان على ظهر إحدى السفن، التي لم يتم تفكيكها خلال بضعة أشهر، وعند هذه النقطة اكتشفت أن المدير التنفيذي للعمليات الخاصة البريطانية SOE قد وظف الرجال ليقوموا بمهمات تخريبية في النرويج. وتم اعتقال اثنين من الرجال سريعاً، ولكن كان هناك بضعة أشهر عصيبة، عندما أرسل الثالث إلى النرويج واعتقله الألمان – لكنه لم يخن المدير التنفيذي للعمليات الخاصة SOE أبداً.

كانت مصالح المخابرات البريطانية سرعان ما تدير العملاء المعتقلين، وأحياناً تجمعهم مع إذاعاتهم في زنزانة السجن حيث يعملون بإنشاء اتصالات مع زملائهم الألمان ويتبعون نصوصاً ذكية يعدها لهم من يتولونهم من البريطانيين. فلم تمكن قراءة شيفرات المخابرات الألمانية من تنفيذ عمليات خداع مدروسة فقط، بل الأهم من ذلك إنها مكنت من فحص إن عرفت المخابرات الألمانية بذلك. وقد فعلوا، حتى عندما قررت «لجنة الفحص المزدوج» البريطانية، التي تدير العملاء المسيطر عليهم،

أنه من الجدير إفشاء أمر عميل من أجل عملية خداع مهمة بصورة خاصة، بدا أنه من المستحيل إفشاء أمره. كان ضباط المخابرات الألمانية دائماً متشوقين لأن يتمسكوا بتفسير معقول آخر لزلات عميل بدلاً من الاعتراف بأنهم قد خدعوا.

تذكر ج سي ماسترمان، في بداية عام 1941، وهو رئيس «لجنة الفحص المزدوج»، أنه بدأ يخطر للسلطات البريطانية – «بصورة مبهمة جداً» – أن كل عميل ألماني في بريطانيا كان تحت سيطرتهم. بالتأكيد لم يكن هناك آخرون. في تموز 1942 أصبح هذا التخمين المبهم حقيقة مؤكدة بمعيار كبيرة نتيجة للتثبيت الذي قدمه محللو الشيفرة من المستوى العالي في فريق ISK.

كان نجم لجنة الفحص المزدوج العميل الإسباني المعادي للفاشية خوان بويول غارسيا، Juan Pujol Garcia، واسمه الرمزي «غاربو GARBO». عند بداية الحرب حاول غارسيا أن يحصل على وظيفة كعميل بريطاني وفشل، لذا تخيل الفكرة الجريئة بأن يقدم خدماته أولاً إلى الألمان فيكون لديه شيء كثير ليعرض خدماته على البريطانيين. فسار إلى السفارة الألمانية في مدريد؛ ومع مجرى الأيام قبلته المخابرات الألمانية؛ وفي تموز 1941 غادر إلى انكلتره كما هو مفروض، مجهزاً بالحبر السري والمال وبقائمة من الأسئلة. لكنه بدل أن يذهب إلى انكلترة، ذهب إلى لشبونة حيث أمضى تسعة أشهر وليس معه ما يدله سوى خريطة ودليل سياحي لبريطانيا، ومطبوعة برتغالية عن الأسطول البريطاني، وأي صحف فنية استطاع أن يجدها في المكتبة العامة، وشرع بتأليف سلسلة من التقارير الاستخبارية المبتكرة بصورة عالية إلى رؤسائه الألمان. على الرغم من بعض الزلات العجيبة – في أحد التقارير المفروض أنه من غلاسكو، شرح نجاحه بفوزه بالمعلومات من السكان المحليين بملاحظة أن «هناك أشخاصاً مستعدون لأن يفعلوا أي شيء مقابل ليتر من المشروب» – كانت المخابرات الألمانية مقتنعة بصدقه وإخلاصه. و«وظف» غارسيا ثلاثة عملاء ثانويين خياليين إضافة إلى ساع، وهو موظف في شركة طيران يقوم بنقل المراسلات إلى لشبونة ومن ثم ترسل إلى زميله، كما شرح.

في كانون الثاني 1942 تقدم غارسيا مرة ثانية إلى البريطانيين، واتصل بمخابرات الإشارة في لشبونة. كان البريطانيون مرتابين بصورة واضحة؛ كانت قصته خيالية. لكن أفضل ضمان يملكه هو الشيفرة ULTRA، وبعد أشهر قليلة وفي 2 نيسان أظهرت الرسائل المفككة من فريق ISOS، بشكل لا يقبل الخطأ، أن المخابرات الألمانية ليس لديها أي شك في تقارير غارسيا، فككت الوحدة GC&CS إشارة من مدريد إلى برلين تنقل تقرير غارسيا عن عدم وجود قافلة من ليفربول إلى مالطة. وتبع هذه الرسالة سريعاً رسالة إنغما بحرية تفضح خبر استعدادت ألمانيا لاعتراض القافلة. وانتقل غارسيا جواً إلى بريطانيا بعد ذلك في الشهر ذاته.

ازدادت شهرة غارسيا أكثر بسبب أذكى خطط الخداع في الحرب كلها. قدمت تورش TORCH الفرصة في ذلك الخريف. ففي 29 تشرين الأول كتب غاربو GARBO رسالة يذكر فيها مغادرة قافلة كبيرة تبحر من كلايد في 26 من الشهر. نقلت الرسالة إلى لشبونة حيث انتظرت مصلحة مخابرات الإشارة حتى تثبتت قيادة البحرية أن القافلة قد حددتها استطلاعات دول المحور. ثم أرسلت بالبريد في 4 تشرين الثاني. ورسالة أخرى تحمل خاتم البريد وتاريخ 2 تشرين الثاني، لكنها لم ترسل بالواقع حتى 7 تشرين الثاني – وهو اليوم الذي سبق نزول الحلفاء وبالتأكيد ستصل الرسالة بعد فوات الأوان – تنقل هذه الرسالة أن ناقلات جنود وسفناً حربية مموهة بأعلام البحر الأبيض المتوسط قد غادرت كلايد. وكان زملاؤه الألمان يثمنون ذلك حسب الأصول: «إن تقاريرك الأخيرة رائعة جميعاً، ولكننا نأسف لأنها وصلت متأخرة». أصبحت سمعة غاربو GARBO الآن ثابتة لا تتزعزع، وفي يوم دي «D – Day» أعدت الخدعة، ولكن هذه المرة رافقتها حبة سم. في عام 1944 أصحبت شبكة غاربو من العملاء الخياليين تضم ثلاثين شخصاً وذلك بتخطيط ودراسة من لجنة التحقيق المزدوج؛ وفيهم ضابط ثرثار من القوى الجوية، وموظف متطرف من الجناح اليساري من وزارة الإعلام، ورجل أعمال فنزويلي من غلاسكو، وبحار يوناني شيوعي في شرق اسكتلندة، وعامل مطعم من جبل طارق يعمل في مطعم

المصلحة، ورقيب أمريكي معاد للإنكليز، وثمانية من القوميين الويلزيين. في الساعات الأولى من صباح السادس من حزيران، بعث غاربو رسالة عاجلة عن طريق الراديو إلى ضابطه في المخابرات الألمانية: كان الغزو وشيك الوقوع. وهنا أيضاً كان توقيت الرسالة مثالياً؛ فعند وصولها إلى أيدي الألمان، كان الغموض قد بدأ. وبعد ثلاثة أيام جاءت ضربة المعلم التي كانت العملية كلها تعد لها. وبعد «اجتماع» غاربو مرة أخرى بشبكته نقل بتقرير عاجل بأن الهجوم على النورماندي كان عملاً تضليلياً؛ وأن الضربة الحقيقية سوف تنزل بمدينة بادوكاليه. وهذا بالطبع ما كان الألمان يميلون إلى تصديقه منذ أشهر، وكان ذلك ما أراد الحلفاء جميعاً تأكيده من خلال عملية الخداع كلها، لاسيما بخلق مجموعة عسكرية من نسج الخيال في بريطانية «فوساغ (أول مجموعة عسكرية للولايات المتحدة تحت إمرة الجنرال جورج س. باتون. لاحظ غاربو في رسالته بتاريخ 9 حزيران بأن يشارك بالنزول إلى النورماندي عسكري واحد من تشكيل الفوساغ ، وهذا دليل على أنهم أُوقفوا احتياطاً للضربة الرئيسية. وكان ذكاء الخطة المتفوق أن الخداع استمر بضعة أيام، بل بضعة أسابيع في الواقع، بعدما بدأ الهجوم فعلاً – وأفلحت الخطة في جعل فشل الوحدة غير الموجودة يحقق مصدراً من القلق المهم للعدو. في أواخر حزيران تلقى غاربو رسالة لم تقدم أي نهاية للرضى في لجنة التحقيق المزدوج: كان الألمان يكافئونه بالصليب الحديدي على عمله البطولي.

أكدت الرسائل المفككة من شيفرة «فيش FISH» في ربيع 1944 أن الألمان كانوا مقتنعين بأن هدف الحلفاء كان بادوكاليه؛ وهذا ما فعلته سلسلة من الرسائل الثمينة والمفككة من الشيفرة البنفسجية Purple من أوشيما، فذكرت واحدة في تشرين الثاني 1943 وفيها ذكر لتفاصيل لا تُصدق حول جولته التفتيشية «للخط الدفاعي الألماني الغربي». في أواخر كانون الأول استدعى مارشال على عجل أيزنهاور إلى واشنطن (ليجد شخصاً آخر ليدير الحرب لمدة عشرين دقيقة) وذلك لأنه شعر أن أيزنهاور كان بحاجة شديدة إلى استراحة، ولأنه أراد أن يراجع المعلومات الجيدة هذه معه. واستمرت تقارير أوشيما لبضعة أسابيع بعد يوم دي

D–Day لتقدم تأكيداً لأيزنهاور بأن الخداع لا يزال يعمل. في 9 حزيران أبرق أوشيما إلى طوكيو بأن الألمان على استعداد لمقاومة النزول في أقاليم كاليه وسانت مالو؛ وبعد شهر كامل من يوم دي، نقل السفير الياباني أن الألمان لا يزالون يستعدون لهجوم ثان في منطقة القنال تقوم به قوة فرقة (غير موجودة).

في السنة الأخيرة من الحرب حقق العملاء المزدوجون ضربة أخيرة. عندما بدأ السلاح

V–1 وV–2 يضرب لندن، طالبت المخابرات الألمانية عملاءها في انكلترة أن يذكروا زمان ومكان التأثير. وبموجب إرشادات الخبراء العلميين البريطانيين، حرف العملاء المعطيات بذكاء مما يجعل الألمان يعتقدون أنهم يطلقون النار على أهدافهم في وسط لندن. وبسبب تأثير هذه التقارير الكاذبة، كان متوسط تأثير النقطة سلاح V–2 انتقلت نحو الشرق بمعدل 2 ميل في الأسبوع، وحتى منتصف شباط 1945، سقطت معظم الصواريخ خارج حدود المدينة الآهلة بكثافة سكانية.

--- --- ---

تساقطت أنظمة شيفرة العدو، الواحد تلو الآخر، ومع تساقطهم رجحت كفة الحلفاء في السيطرة على أمواج الأثير. واستمرت شيفرات البحرية اليابانية بإجراء تغيرات وتحسينات منتظمة، لكن الوحدة OP–20–G أنجزت خطواتها وكانت صعوبة المحافظة على مستواها قليلة. وأعطت القراءة المنتظمة لشيفرات القوافل اليابانية جعلت الغواصات الأمريكية تسيطر سيطرة شبه كاملة على خطوط التموين اليابانية، وعند صباح كل يوم وفي الساعة التاسعة، وكأن الساعة تدق في الإدارة، يجتمع ضباط مخابرات أسطول المحيط الهادي بكبار ضباط قوات غواصات الأسطول ليتقاسموا الأهداف. في كانون الثاني 1944 كانت الغواصات الأمريكية تغرق ثلث مليون طن كل شهر.

كانت الشيفرة اليابانية JN–25 تحمل ما يقارب 70٪ من رسائل البحرية اليابانية جميعاً، وكان تُقرأ بصورة مستمرة طيلة ما تبقى من الحرب. في 14 نيسان 1943، نزلت برقية مفككة من الشيفرة JN–25 على مكتب إديون ليتون، رئيس

مخابرات نيميتز، وسرعان ما كهربته وأزعجته. بدأت الرسالة بما يلي: في نيسان CINC 18 الأسطول المشترك سيزور PXZ,R –، وRXP بحسب البرنامج التالي: 1. يغادر RR الساعة السادسة في طائرة هجوم متوسطة يرافقها ست مقاتلات. وتصل RXZ الساعة الثامنة. إنها وثيقة وفاة الأميرال إيزوروكو ياماموتو. وعقد ليتون ونيميتز اجتماعاً مضطرباً. وسأل نيمتيز ليتون – الذي كان في اليابان كطالب يدرس اللغة اليابانية، عرف الأميرال حقاً – إن كانت البحرية اليابانية تستطيع أن تجد بديلاً له. فأكد ليتون أن ياماموتو لا يُعوض حقاً. وبهذه الإجابة سُويّ الأمر بالنسبة لنيميتز وصدرت الأوامر. وحددت RXZ بجزيرة صغيرة من جزر سليمان جنوب بوغينفيل واسمها بُليل. أقلعت ست عشرة طائرة من طراز P–38 من مطار هندرسون من جزيرة غوادال كنال، وطارت بأقصى سرعتها، واعترضت حاشية ياماموتو المحمولة جواً دون خطأ. عندما فتح النقيب توماس لانغاير النار، انفجرت واحدة من القاذفات اليابانية، واندلعت ألسنة اللهب من محركها، وانقسم الجناح إلى قطع، وهوت الطائرة إلى غابة تحتها. كما أصيبت ثلاث طائرات من طراز «زيرو» وقاذفة ثانية. وانتظرت الحكومة اليابانية حتى 21 أيار لتعلن نبأ وفاة ياماموتو سواء بالنسبة للأسطول وللشعب الياباني.

--- --- ---

لا يزال هناك شيفرة أخيرة غير مفككة، وحيث أنها مركزية بالنسبة للجهد الحربي، فقد أصبحت إحراجاً حاداً بالنسبة لآرلنغتون هول. كانت الوحدة OP–20–G تعمل على شفرات البحرية اليابانية على مدى سنين قبل الحرب.

ولكن مصلحة مخابرات الإشارة في الجيش، وكانت تنقصها القدرة المطلوبة للاعتراض وتحرفها الكلفة العالية لشيفرة الديبلوماسية اليابانية، لم تبذل أي جهد تقريباً لدراسة الشيفرات المماثلة للجيش الياباني. في نيسان 1942، بلغ مجموع عناصر مصلحة مخابرات الإشارة الذين يعملون في قسم الشيفرة العسكرية اليابانية أحد عشر شخصاً، ولكن أربعة أشخاص فقد عينوا في الشيفرة العسكرية اليابانية بصورة خاصة. وجدوا الفوضى والاضطراب من أنظمة مختلفة،

وكل ما استطاع جميع محللي الشيفرة فعله هو أن يفرزوا الرسائل ويصنفوها عند وصولها. وكانت جميع الأنظمة من المستوى العالي ذات أربعة أرقام، شيفرات من جزئين تُشفر بإضافات، وكل رسالة ترسل بأي منهما تحمل أربعة أرقام «مميزة» تحدد النظام المستخدم – قبل بيرل هاربر كان هناك نظام رئيسي واحد يستخدم الطبقات العليا؛ وكانت تحمل الرقم المميز 5678 والذي حدده محللو الشيفرة الأمريكيون بالأحرف ATRW. ولكن عندما تدفق الجيش الياباني على المحيط الهادي في عام 1942 وزاد عبء الرسائل سريعاً، صدرت كتب إضافية جديدة لمناطق منفصلة. في أيار 1942 انقسم النظام الأساسي إلى 7890، الذي دعته مصلحة مخابرات الإشارة JEM، و2345 أو JEN. وكان هناك نظام منفصل أيضاً هو 2468 أوJEK، ا لذي كان يستعمل على ما يبدو لدى منظمة نقل الماء، الذي أصبح نافذاً في بحرية الجيش ويستخدم لتنقلات القوات في المحيط الهادي. واستمرت التقسيمات بحسب الأقاليم والمصالح، وكان مجرد وضعها في نسق مستقيم مهمة ضخمة في آرلنغتون هول. وكان الأمل في إنجاز اختراق في تحليل الشيفرة أملاً ضئيلاً إلى درجة جعلت قسم تحليل الرسائل يتلقى الأفكار الأولى حول الرسائل الواردة جميعاً، وبما أنه لا يوجد سوى خطين للطابعة عن بعد تصل مصلحة مخابرات الإشارة SIS بفرع تو روك في كاليفورنيا، الذي يعترض معظم الرسائل، فإن جميع الرسائل تقريباً تأتي بواسطة البريد. وبعضها يأتي بالبريد من استراليا أيضاً، حيث وصل أفراد أمريكيون في منتصف نيسان ليقيموا وحدة اعتراض وتحليل للرسائل بناء على طلب ماك آرثر. وكان عمرها من شهر إلى ثمانية أشهر عندما ظهرت أخيراً في واشنطن؛ ومن ثم تتكب عليها وحدة تحليل الرسائل لمدة ثلاثة أشهر أخرى؛ ثم يتوجب أن يراها أخيراً محللو الشيفرة. هناك حرب دائرة، ولكن في صيف 1942 كان هناك لا يزال حوالي عشرين شخصاً يعملون على الشيفرة العسكرية الرئيسة للعدو الرئيسي، بالنسبة لمعظم الأمريكيين على الأقل.

عندما حقق محللو الشيفرة ضربتهم أخيراً، بدا أن الأمل الوحيد هو تشغيل القوة الهائلة لآلة IBM. فالمؤشرات المستخدمة لتحديد نقطة البداية في كتاب

الإضافات لكل رسالة كانت تُشعر في رموز خاصة بها لا يمكن اختراقها. ويستهلك تثبيب أربعة آلاف رسالة في جميع أشكالها المحتملة من ثلاثة إلى أربعة ملايين بطاقة IBM، واستمر العمل من نيسان 1942 إلى نهاية السنة قبل أن يرفع محللو الشيفرة أيديهم محبطين ويائسين. لقد كان هنا مواد كثيرة يتعين فحصها، وكان هناك فرصة لصدفة عشوائية تولد «الخبطة» المزدوجة. عدد صغير من رسائل مزدوجة تبين أن فيهم «خبطات» ثلاثية، ولكن حتى هؤلاء لم يوصلوا إلى أي مكان. أظهرت حسابات احصائية أن «خبطة» مزدوجة واحدة في نظام يستخدم كتاب إضافات فيه خمسون ألف مجموعة ذات فرصة واحدة من 45 فرصة لأن تكون سببية؛ حتى «الخطبة» الثلاثية فهي اقتراح يصل إلى 50/50 فقط.

لم يكن فرانك لويس، الذي عين الآن في قسم الجيش الياباني، سعيداً بطريقة القوة الهائلة منذ البداية – «قوة هائلة وجهل لعين» هو ما يشبه هذه الطريقة، كما كان يشعر – واعتقد أنه قد يكون أكثر فائدة أن نبدأ بالرسائل القديمة بالعودة إلى الخلف ونحاول العمل إلى الأمام لتثبيت الاستمرارية. فنظام ما قبل الحرب ARTW استخدم نظام مؤشر مستقيم إلى الأمام ليحدد نقطة البداية في كتاب الإضافات: عند بدء الرسالة ونهايتها كان هناك مجموعتان من أربع رموز من الصيغة BPPS RCRC، حيث B هو رقم كتاب الإضافة

(1 إلى 3)، وPP هما رقم الصفحة (من 0 إلى 9)، وS هو تدقيق المجموع الذي يحصل عليه من جمع الأرقام الثلاثة الأولى جمعاً حسابياً دون حمل، وRCRC هي النسق والعمود على الصفحة، وتتكرر مرتين للتدقيق. وكانت المؤشرات نفسها مشفرة بجدول من مائة إضافة. والسؤال الآن أين كان المؤشر، في الأنظمة الحالية، مختبأ وكيف يُشفر؟

جاءت فكرة في آذار 1943، عندما سلمت أربعة أشكال من الرسائل 5678، تم أسرها، إلى آرلنغتون هول. أوحت الملاحظات على الأشكال أن بعضاً من مجموعات نص الرسالة نفسها تستخدم بطريقة ما كمفتاح ليحدد تشفير المؤشرات. لكن الاختراق الأكثر أهمية جاء بعد أسابيع قليلة. لفتت برقية واردة من الوحدة

GC&CS الانتباه إلى ظاهرة غريبة وملفتة: لم تكن الخانة الأولى من مجموعة الشيفرة الثالثة من كل رسالة عشوائية تماماً. حققت وحدة جيش الولايات المتحدة في استراليا، وهي المعروفة باسم مكتب بريتربين المركزي Central Brueau Brisbane (CBB) وتحت إمرة آب سينكوف الذي أُرسل في حزيران 1942، اكتشافاً آخر في الأول من نيسان. فبالنسبة لأي خانة في المركز الابتدائي للمجموعة الثانية من الرسالة، هناك ثلاث خانات ممكنة فقط لتخطر في المركز الأول من المجموعة الثالثة. فإذا بدأت المجموعة الثانية، لنقل، بـ 1، فتبدأ المجموعة الثالثة إما بـ 3، أو 5، أو 6. وإن بدأت بـ 2، تبدأ المجموعة الثالثة بـ 2 أو 8 أو 9. وهذا يدل على أشياء كثيرة، لأنه كما أظهرت دراسة لويس التاريخية للنظام 5678، فإن الحرف B في BPPS يمكن أن تكون له القيم من 1 إلى 3. وواضح أن مجموعة النص الثانية من الرسالة كانت تستخدم كمفتاح من نوع تشفير المؤشر BPPS، ثم أُدخلت في الرسالة كمجموعة ثالثة. وبصورة مماثلة، أصبح واضحاً أن مجموعة الرسالة الرابعة استخدمت كمفتاح لتشفير المؤشر RCRC، فأُدخل بعد ذلك في المجموعة الخامسة من الرسالة. خلال أسبوع قام المكتب CBB وآرلنغتون هول بتفككيك النظام واستخدم ذلك مربع تحويل 10 × 10؛ وخانات النص البسيط (0 – 9) يسير عبر القمة، والخانات المفتاح عمودي في الجانب واحتوى الجدول على خانات تشفير النص. على سبيل المثال:

النص البسيط

المفتاح	0	1	2	3	4	5	6	7	8	9
0	7	9	6	0	3	1	4	2	8	5
1	3	1	0	7	9	6	2	8	4	5
2	7	5	0	8	2	9	6	1	3	4
3	8	4	9	5	2	6	1	3	0	7
4	7	8	2	9	4	1	3	0	5	6
5	6	9	5	1	2	8	4	0	3	7
6	5	8	4	9	1	3	0	7	2	6
7	3	9	6	8	4	1	0	5	7	2
8	7	4	1	0	6	2	9	8	5	3
9	3	6	4	7	5	0	1	9	2	8

إن كان المؤشر BPPS غير المشفر 2697، والمجموعة الثانية لنص الرسالة التي تقوم بدور المفتاح كانت 0724، فإن الصيغة المشفرة من BPPS التي تستخدم مربع التحويل تكون 6040.

أرسل المكتب CBB برقية إلى واشنطن في 6 نيسان يعلن فيها أنه فككها، وأعطى نتائجه. وأرسل آرلنغتون هول في اليوم التالي برقية جوابية يقول فيها: «نعم، لقد فعلنا ذلك، أيضاً»، وهذا ترك الفريق في بريزين مرتاباً نوعاً ما.

ليكن الأمر كما هو، فإن هذا تقدماً في النهاية. من 1 آذار إلى 30 نيسان زاد عدد العاملين في قسم الجيش الياباني ثلاث مرات فبلغ 270، مع أكثر من مائة يعملون في النظام JEK. خلال هذا الوقت، أثبت عمل أسابيع قليلة أن النظام 7890 والنظام 5678 يستخدمان نظام تشفير للمؤشرات مماثل، لكنه أكثر تعقيداً، ، حيث أشارت بعض خانات مجموعات الرسالة إلى قائمة مفاتيح منفصلة مطبوعة، تقدم هذه القائمة الخانات الرئيسية التي ينبغي أن تستعمل مع مربع التحويل. وكان مربع التحويل يخضع لتغيرات أيضاً غالباً، وهذا يسبب صداعا كبيرا.

لكن بضعة أشياء ساعدت: الشيء الأول الصعوبة الكبيرة للغة اليابانية نفسها. حينما تواجه عامل الشيفرة اليابانية كلمة أو اسم علم غير موجودة في كتاب الشيفرة، فيتعين عليه أن يهجئ الكلمة أو الاسم وذلك باستخدام الرموز اليابانية (الكانا)، التي يحدد لها رمزها المؤلف من مجموعات ذات أربع خانات في الكتاب المعدلثل هذه الحاجة. لكن الكلمات المهجأة بالرموز اليابانية (الكانا) هي غامضة في اللغة اليابانية، وهي لغة ذات كلمات كثيرة لها نفس الأصوات. مثلاً، فالكلمة «سينتو» يمكن أن تعني «حمام» أو «إقامة الامبراطور المقاعد»، أو «أول جدار في قلعة محاضرة»، أو «المقاتلة»، أو «المقص». في اليابانية المكتوبة توضع إشارات على الرموز لتزيل الغموض وتعرف هذه الإشارات «الكانجي» وهي مشتقة من الرموز الصينية. مع بدايات البرقيات، تم تطوير نظام برقي تجاري قياسي ليقدم معادلات رقمية للرموز الصينية. (أمضى تيلتمان أسابيع في عام 1935 وهو يعمل فيما اعتقد أنه حزمة من رسائل يابانية معترضة قدمتها وحدة الإعتراض البريطانية في

هونغ كونغ. وسرعان ما توصل إلى أن هذه الشيفرة لا يمكن اختراقها، وبدأ يعرف ويحدد مجموعات تقوم مقام أرقام؛ والسمة المهمة كانت أن النظام العددي لمجموعات الرموز يتبعه نظام خطي هوعبارة عن الرموز الصينية مكتوبة. ومضى بعيداً تماماً عندما ألقى صديق له، وهو ترجمان صيني لدى وزارة الحربية، نظرة على عمله وشرح لتيلتمان أن «ما فككه هو الرمز البرقي الصيني» المتوافر على مستوى عامة الناس).

عندما كان عامل الشيفرة اليابانية يتوقف عند كلمة ما، فإنه بكل بساطة يلجأ إلى الرمز البرقي الصيني لإيضاح معنى الكلمة السابقة المهجأة برموز «الكانا». حددت كتب الرموز العسكرية مجموعات الرموز 1951 و5734 لتعني «الرمز البرقي الصيني يتبع». حتى عند إخفاء مجموعات الرمز البرقي الصيني بواسطة الإضافات، كما يصنع بباقي النص، فقد كان ذلك خطأ أمنياً سخيفاً. وذلك بسبب شيء واحد هو ظهور مجموعتي الرموز 1951 و5734 في الرسائل بصورة متكررة، وإذا ما أضيف إليهما مجموعات الرموز لكلمة «نقطة» والكلمات الشائعة الأخرى، فإنها تقدم مدخلاً موثوقاً لمفكك الشيفرة. والشيء الآخر، بما أن مجموعات رموز «الكانا» التي تسبق المجموعة 1951، ومجموعات «الرمز البرقي الصيني» التي تتبع، تقوم مقام الكلمة نفسها، فليس من الصعب جداً أن يخمن واحدة من الأخرى.

مع تفكيك المؤشرات، والعمليات القياسية لمطابقة الرسائل، أمكن أن تبدأ أعمال أخرى بحماس، وهي اكتشاف إضافات البداية ومجموعة الرموز. في أوائل حزيران 1943، كانت الرسائل بالنظام 2468، وهو نظام نقل الماء، تُقرأ وتُقدم إلى المخابرات العسكرية. والرسائل المفككة لم تكن في الغالب آنية، ولكن لأن الكثيرين كانوا يعلنون مسبقاً تواريخ الإبحار وطرق النقل وسفن التموين، كانت المعلومات يمكن الاستفادة منها على الرغم من تأخر الوقت. ففي 20 آب، تم تفكيك رسالة من نقل الماء قبل تسعة أيام تعلن أن قافلة سوف تغادر بالاو Palau في السادس والعشرين وسوف تفرغ حمولتها في ويواك Wewak في الأول من أيلول. وفي

ويواك رحبت الطائرات القاذفة الوسطى التابعة للولايات المتحدة بخمس سفن للشحن ومدمرتين، وجاءت على ارتفاع الصارية.

كان التقدم بالأنظمة الأخرى أبطأ، وجعل التغيير المستمر في الكتابة السرية في الأنظمة الأخرى جميعها العمل كفاحاً من أسبوع إلى أسبوع. لكن خطأ آخر قد ظهر على الرغم من أن الخطط التي استخدمها اليابانيون في تشفير المؤشرات والنصوص أصبحت معقدة أكثر فأكثر. فقد جرى تقسيم شبكة الاتصالات إلى مناطق صغيرة أكثر؛ وأصبحت كتب الإضافات تتغير بسرعة أكبر؛ وبدءاً من شباط 1944 تغير نظام التشفير 2468 كلياً إلى الإجراء المتعب باستخدام «مربعات التحويل» لتشفير النص الحقيقي للرسالة. فبدلاً من استعمال الإضافات على مجموعات الرموز بواسطة الجمع دون الحمل، فإن الإضافات الآن تستخدم كمفاتيح «للمربعات التحويل».

ولكن حتى هذا الإجراء الأمني الدرامي يحوي بذرة تفكيكه. فمع العدد الكبير من التغيرات، والشبكات المتعددة والمنفصلة – والآن أعداد كبيرة من وحدات الجيش مقطوعة في جزر معزولة في المحيط الهادي – كان من المستحيل على الجيش الياباني أن يصدر مواد رموز جديد كتابة. وبدل ذلك راح يبث مربعات التحويل الجديدة، في الشيفرة وبواسطة الراديو في واحدة من السخريات الكبيرة في حرب الشيفرة، قدمت الصيغ النمطية من هذه الرسائل المشفرة ذاتها مطابقات موثوقة للتفكيك. عن تدفق الأرقام يتبعه دون أي تغيير عشر مجموعات تدقيق خاصة، وكانت كلها ذات صيغة مما جعل آرلنغتون هول فيما بعد يطور ملحقاً لآلة IBM ذا هدف خاص، وسمي هذا الملحق CAMEL، يستطيع آلياً أن يحدد أي تسلسل من عشر مجموعات يمكن أن تكون تشفير مجموعات تدقيق.

في أيلول 1943 تقدم العمل على شيفرة الجيش الياباني تقدماً كافياً بحيث انفصل ليصبح فرعاً مختصاً وسمي B – II، وكان المسؤول عنه كولباك؛ والعمل الآخر المهتم بالرسائل الدبلوماسية بشكل رئيسي تجمع ليكون B – III، «فرع التشفير العام»، وسمي روليت مسؤولاً عنه. (وكانت جميع القنابل وآلات التحليل

السريع وضعت أيضاً في B – IV. وكان الفرع الرئيسي الثالث هو B – I وتكرس بشكل حصري ليترجم الرسائل اليابانية المفككة). وتحسن تدفق الرسائل المفككة من الجيش الياباني، ووصل إلى ما يقارب الألفين في شهر كانون الثاني 1944، مع أن معظم هذه الرسائل لا تزال إشارات من نقل الماء. وبعد ذلك أصبحت موجه مد. قررت وحدة من الجنود الأخيرة من الفرقة اليابانية العشرين، وهي تنسحب من سيو Sio وغينيا الجديدة، بمطر منهمر، أن لديها مشكلات كافية تماماً دون تحمل مشقة سحب صندوق يحتوي على كتب شيفرة الوحدة. وبينما كان مهندس استرالي يفتش المنطقة بحساس معدني بحثاً عن أفخاخ يابانية ساذجة، تجمد عندما بدأت السماعة الرأسية تعطي إشارات؛ واستدعيت وحدة تدمير ورفعت التراب عن الصندوق. وقال سينكوف فيما بعد: «لقد كان مكتبة كاملة للشيفرة» للفرقة العشرين. قُدمت الغنيمة إلى المكتب CBB في بريزبان، وبدأت مجموعة سينكوف العمل حالاً، فعلقت الصفحات المبللة لتجف على حبال الغسيل وأطلقت المراوح والسخانات تياراً ساخناً عليها. وصُورت الرسائل وأرسلت نسخ عنها إلى آرلنغتون هول، وفي آذار، كانت الرسائل، التي بثت بالأجهزة الأرضية اليابانية الرئيسية، تُقرأ في بريزبان وآرلنغتون هول بالسرعة التي يقرؤها بها اليابانيون. لقد تم تفكيك ما يقرب من 36 ألفاً من الرسائل في شهر آذار. في الواقع كان آرلنغتون هول في بعض الأحيان يقرأ الرسائل أسرع مما استطاعه اليابانيون. في تشرين الأول 1943، اخترع الفرع B – II جهازاً يفكك الرسائل آلياً وذلك باستخدام آلات IBM، والآن مع اكتشاف كتب الإضافات، أقلع جهاز الإنتاج الجماعي من الرسائل المفككه إقلاعاً حقيقياً. كانت محطات الاعتراض ترسل الرسائل الخام بواسطة طابعة عن بعد إلى آرلنغتون هول مباشرة؛ كانت الأجهزة الطابعة عن بعد تثقب شريطاً من الورق ثم يدخل إلى الآلة التي تحول النص إلى بطاقات IBM؛ تقوم مكتبة من الإضافات المكتشفة ومربعات التحويل بكشف التشفير، وكان يفتش عن مجموعات الرموز الناتجة في كومة أخرى من البطاقات، وتجري طباعة النص الذي فُك تشفيره. وفي نهاية حزيران 1944، كان يتم تثقيب أكثر من 4300 رسالة على بطاقات IBM في اليوم الواحد، كما كان

أكثر من 2500 في اليوم تفكك آلياً. لقد بدأت العمل على مشكلة الجيش الياباني بطيئاً، لكنه انتهى بدويّ وضجيج.

على الرغم من أن آرلنغتون هول ومكتب CBB تعاونا تعاوناً كاملاً، كان هناك موضوع خلاف لم يحل قط. أصر ماك آرثر على أنه يجب على كل وحدة في منطقته أن ترسل تقاريرها إليه، وليس إلى وزارة الحربية. وحاول العقيد كارتر كلارك بضع مرات إنشاء قناة آمنة يستطيع المكتب CBB إرسال الرسائل المفككة بواسطتها إلى واشنطن لتتم العملية في مكتبه وترسل بعد ذلك إلى القادة. عارض ماك آرثر هذه الخطة عند كل نقطة. في كانون الأول 1943 أرسل الجنرال سترونغ، وهو رئيس المخابرات العسكرية، ضابطي اتصال إلى استراليا لإنشاء صلة آمنة؛ ويتطلب جزء من الاتفاقية مع البريطانيين للتعامل مع ULTRA صراحة بأن تقام مثل هذه الأقنية الآمنة في جميع مسارح العمليات. وطلب مارك آرثر من أحد مساعديه، أن يصدر أمراً يمنع الطرفين من إرسال رسائل بالراديو دون موافقته. بعد سنة قام كلارك، وهو يحمل رسالة شخصية من مارشال، برحلة جوية ليرى ماك آرثر ويشرح الحاجات. وصل كلارك إلى هاواي عندما طلبت قيادة ماك آرثر منه أن يعود أدراجه إلى واشنطن.

وزع موظفو ماك آرثر رسائل ULTRA بحرية أكبر من حرية وزارة الحربية أو البحرية أو البريطانيين، واشتكت البحرية أكثر من مرة نقص الأمان في إرسال مخابرات ULTRA إلى القيادات بواسطة أقنية الراديو ضمن مسرح ماك آرثر. لكن ماك آرثر كان قوة بنفسه. وأخيراً سُلمت نسخة من تعليمات جديدة لمخابرات ULTRA إلى الجنرال. وطلب ماك آرثر من موظفيه بأن يعيدوا صياغة التعليمات لتناسبه ثم وقعها وأعادها إلى واشنطن.

--- --- ---

أنقذ التدمير السريع للوضع الياباني في المحيط الهادي حينذاك طيش ماك آرثر وتهوره من تكاليف كثيرة. فقد عانت اليابان في العام 1944 من خسائر في حاملات الطائرات والطيارين المدربين لا يمكن تعويضها وتصحيحها؛ فإنهارت جميع

دفاعاتها هناك من جميع الاتجاهات، فأولاً جزر الألوشيان وبعدها غوادال كنال، وأخيراً بعد سنتين. قتال شرس في الغابات – تم اغتصاب الحلفاء لغينيا الجديدة من اليابان. وفي الحقيقة، أعطى التحليل الذكي للشيفرة دوره على كل الجبهات إلى القوة العسكرية الشرسة خلال السنة الأخيرة من الحرب. لقد نفذ تفكيك الشيفرة المعجزات عندما كانت الاستعدادات منخفضة. لقد ظهر خلال الانتصار في ميدوي مع وجود أضيق الشواذ، فكان الانتصار في زمن كان النصر فيه ضرورة لابد منها. وقد أوقف رومل وهو في طريقه في الصحراء على بعد مائتي ميل من القاهرة، وألهب سحره حماس الجيش البريطاني وثبط همته في تل الحلفا. وساعد في قلب المد في المحيط الأطلسي عند مفصلين مهمين، عندما واجهت بريطانيا خسائر لا تحتمل وكانت ستعاني من المجاعة خلال أشهر. ولكن من طبيعة المهاجمين أنهم يهتمون بالذكاء والفطنة أقل مما يهتمون بالمدافعين؛ واهتمامهم النفسي أقل كما أقل بمسألة الحسابات العسكرية البسيطة، فالحكمة التقليدية تقتضي أن المهاجم يحتاج إلى تفوق بالرجال، 3 مقابل 1 وكذلك العتاد عندما يتجه نحو موقع دفاعي معد إعداداً جيداً، والجيش الذي يجمع كل هذه القوة من الدروع والذخائر والرجال سوف يكسب بالوزن الطاغي والمسيطر، ولا يهم أي شيء. ليس من الضروري أن يكون النصر سهلاً أو رخيصاً مع ذلك. وكمثال واضح عن الوزن الطاغي والمسيطر، إرجعت القوة الصناعية الأمريكية وقوة الرجال الجيوش الألمانية في أوربا، ودفع جنرالات الحلفاء ثمناً باهظاً لانسحابهم إلى عاداتهم القديمة والمألوفة في إنفاق المزيد من الوقت في قيادة الجيش، وإنفاق القليل من الوقت في قراءة نوايا العدو. كان المكان هو المكان القديم المألوف لتصفية الحسابات بين ألمانيا والقوات الغربية غابة الآردين في بلجيكا. كانت خطة هتلر كعادته تجمع العبقرية والحماسة. سيقطع الألمان خطوط الحلفاء، ويحتلون ميناء انتويرب، ويقسمون الجبهة إلى نصفين. ويقع الحلفاء في فوضى. لا يمكن اقتلاعهم من فرنسا طبعاً، لكن برنامجهم سوف يصيبه التقطع. وتخيل هتلر أن الألمان سيتمكنون من السبق إلى الخلف عبر الجبهة الشرقية ويضربون الروس، حيث سيعود الغرب إلى عقله وينضم إلى ألمانيا ضد العدو الحقيقي المشترك، البلشفية.

كان فشل الحلفاء في توقع الهجوم الألماني المضاد، الذي بدأ بقصف مدفعي كبير على القطاع الذي يسيطر عليه الأمريكيون سيطرة ضعيفة في صباح 16 كانون الأول 1944، معقد الأسباب. فقد قدمت ULTRA تحذيرات كافية. ولكن انصافاً لجنرالات الحلفاء الذين نظروا إلى الموقف نظرة رجال عسكريين محترفين وتوصلوا إلى أن الجيش الألماني سوف يسحق بسهولة إن هو قام بالهجوم، وكانت هذه أيضاً وجهة نظر الجنرالات الألمان. وكان هتلر وحده الذي تجرأ وخالف الطرفين.

وكان على الألمان أن يرتجلوا، فقد استخدموا الخداع مرة واحدة استعمالاً كاملاً. تم إعداد وتجهيز جيش مدرعات جديد، والفرقة السادسة SS تحت تمويه وهو «استراحة وإعادة تأهيل أركان الحرب 16». جهز المغاوير الذين يتحدثون الإنكليزية ببدلات الأسرى الأمريكيين وتم إنزالهم بالمظلات لننثر بذور الفوضى. لكن الأولترا ULTRA والماجيك MAGIC اخترقتا معظم الحيل الألمانية مسبقاً: فقد نقلت رسالة من أوشيما إلى طوكيو في 4 أيلول تقريراً عن اجتماع السفير مؤخراً مع هتلر وريبنتروب؛ هتلر كان يشكل قوة من مليون رجل يضاف إليهم وحدات يجري سحبها من جبهات أخرى، وقوات جوية تسد النقص وتضرب غرباً في تشرين الثاني ربما.

كشفت رسائل الإنيغما الجوية طيلة تشرين الثاني وأوائل كانون الثاني أن المقاتلات والمقاتلات القاذفة قد أمرت بأن تتجه غرباً حيث ستزود بمعدات وذلك لدعم عمليات جوية قريبة. وكانت الأوامر التي تشدد على الحاجة إلى السرية المطلقة بحد ذاتها إشارة إلى أن عملية هجومية أكثر منها دفاعية يجري تخطيطها. في اليوم الأول من تشرين الثاني استدعى أمر من الفوهرر المتطوعين إلى قوة خاصة؛ ومعرفة اللغة الإنكليزية والمصطلحات الأمريكية شرط أساسي. وطلب من الطائرات المقاتلة حماية تحركات الجنود الكبيرة على طول السكك الحديدية في المنطقة الواقعة خلف إقليم الآردين. في العاشر من كانون الثاني تم اعتراض أوامر تفرض صمتاً على الراديو في جميع وحدات المدرعات SS.

إن حقيقة الهجوم وحتى توقيت بدء الهجوم قد أرسلت بإشارة مسبقة في هذه الرسائل المعترضة، لكن مكان الهجوم كان أقل وضوحاً، وكان هناك دائماً خطر التشويش عند استعراض الحوادث الماضية؛ كانت المؤشرات إلى حيث يمكن أن يقع الهجوم جزءاً من صور المشكال المؤلف من قطع مرايا صغيرة تعكس أشكالاً كثيرة من المؤشرات المتعاكسة التي بينت أيضاً أن إقليم آخن البعيد إلى الشمال، وكان من نواحي عديدة هو البقعة الأكثر منطقية. ومع ذلك لم يغير هذا من حقيقة عقدة خوف الحلفاء وعاداتهم القديمة في تجاهل المخابرات والتي تتحمل الكثير من اللوم عن المغامرة السيئة التي نتجت. تفحصت قيادة الحلفاء الأدلة والبراهين واستنتجت واثقة أن جيش المدرعات السادس لم يكن سوى «فوج إطفاء» قد يهرع ليحاول إطفاء ألسنة اللهب الناجمة عن تقدم الحلفاء الأخير، ولا شيء أكثر من هذا. استغرق القتال العنيف ستة أسابيع حتى أوقف الألمان وأجبروا على التراجع. وفي نقطة معينة حاصر الألمان الفرقة الأمريكية المحمولة جواً 101 بكاملها؛ وطلبوا منهم الاستسلام، لكن قائد الفرقة الجنرال أنطوني سي ماك أوليف، قال جوابه الشهير بكلمة واحدة، «لا» وتابع القتال. وعومل الألمان الذي يتحدثون الإنكليزية ويلبسون بدلات أمريكية بإجراءات أمنية مرتجلة في المعركة، وهي الباقية من أفلام الحرب العالمية الثانية: قد يعرف المغاوير الأمريكيون المصطلح الأمريكي، لكنهم لم يعرفوا بما يجيبون على أسئلة تتحداهم بذكر اسم أول لاعب بيسبول في فريق بروكلين دودجرز. أظهر الجنود الذين جاؤوا بهذه الأساليب المبتكرة ذكاء وخيالاً أكثر من قادتهم الذين تجاهلوا دليل بليتشلي بارك على الخطط الألمانية.

لقد كلفت معركة البلج Bulge هتلر مائتي ألف رجل، وستمائة دبابة، ومعظم طائراته المتبقية واحتياطاته الاستراتيجية الكاملة. لقد هُزم هتلر لكنه استمر في القتال؛ في الأشهر الأربعة المتبقية كانت الحرب في أوربا حرباً طاحنة لا مندوحة عنها لأن آلة حرب الحلفاء تقدمت، مدرعات ومدفعية ومشاة وطائرات، جميعها تعمل معاً كقوة طاغية ضد مقاومة متضائلة لكنها لا تزال تقاتل بوحدات

من SS، وبشباب مذعورين ورجال مسنين تم استدعاؤهم على عجل للالتحاق بالجيش. كان في هجوم الحلفاء بعض الفطنة والمهارة، ولكن كان هناك حاجة قليلة إلى الذكاء والحرفية في هذه النقطة. كانت تشبه الضرب بالميت أكثر ولكن لا تزال تشد بقوة أفعى الجرس أكثر من مشية الوشق (نمر صغير) الماكر مشية الخيلاء، ولم تكن تحتاج إلى رجل رياضيات من اكسفورد أو كامبريدج ليستخدم الهراوة في الصراع. لقد انتهت حرب الشيفرات في هذه الحرب على الأقل.

--- --- ---

لم يكن مفككو الشيفرة في بليتشلي بارك وواشنطن يقرؤون الرسائل التي يفككونها في معظم الأوقات؛ فكانت القراءة وظيفة أشخاص آخرين. حتى في الأكواخ 3 و4 كان فيض الرسائل وآلاف الرسائل التي تصل كل يوم، في معظمه تفاصيل إدارية روتينية تبرز أهميتها من مجرد جمع أجزاء معاً جمعاً صبوراً لإشارات كثيرة، يسبب نوعاً من العزلة المهنية. لكن هناك إشارات قليلة لم يستطع محللو الشيفرات في بليتشلي بارك وآرلنغتون هول وفي الوحدة OP–20–G أن ينسوها مطلقاً. في أواخر 1943 أو أوائل 1944 يذكر ولتر إيتان، وهو من اليهود القلة الذين عملوا في بليتشلي بارك، أنه كان يعمل في الكوخ 4 عندما جاءت إشارة وكانت اعترضت من سفينة ألمانية صغيرة في مهمة في بحر إيجة. ذكرت السفينة أنها تنقل يهوداً «إلى الحل الأخير». «لم أشاهد أو أسمع هذه العبارة من قبل، ولكنني عرفت بصورة غريزية ما هو معناها، ولم أنس قط هذه اللحظة. ولم أعلق عليها سيما لأولئك العاملين في بليتشلي بارك ولم أذكرها خارج بليتشلي بارك، لكنها تركت أثرها – حتى هذا اليوم». وفي الأول من أيار 1945 كان آليك ديكن يصنف الرسائل المفككة عندما تصل على صينية من الأسلاك في الكوخ 4، عندما التقط رسالة من أسفل رزمة من الرسائل. كانت من الرسائل «الخاصة بالضباط» إلى جميع الغواصات وبدأت بهذه الكلمات: «هتلر ميت». وبعد خمسة أيام جاءت موجة من الإشارات تأمر جميع الغواصات بأن توقف العداوات والنزاعات، وأن تتجه إلى المرافئ البريطانية لتستسلم، وأن تطيع طاعة شديدة التعليمات حتى تتجنب أي

شكل من التظاهرات. والنصوص التالية التي وردت كانت واضحة وصريحة. وسكتت «القنابل» وآلات فك الشيفرات؛ وخلال أشهر قليلة تم تفكيك الآلات بما فيها جميع «القنابل» للتأكد بأن أسرار بليتشلي بارك تم دفنها آمنة.

مارس مفككو الشيفرة في آرلنغتون هول بخبرتهم وضع أيديهم على لحظة تاريخية، وكان ذلك في 13 آب، وهو اليوم الذي أرسلت فيه الحكومة اليابانية رسالة إلى سفيرها في سويسرا وفيها تعليمات لتنقل إلى الحكومة السويسرية لتقوم بتسليمها إلى حكومة الولايات المتحدة، وكانت الرسالة قد فككت وقرئت في آرلنغتون هول قبل ساعتين من قيام الوزير السويسري بتسليمها إلى وزارة الخارجية في واشنطن.

الحرب انتهت بالفعل.

وحرب مخابرات الإشارات قد بدأت الآن في الحقيقة.

--- --- ---

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.

- وليام وايسبان: مقدمة إلى الولايات المتحدة، VENONA.
- يبدو ذلك مثيراً للاهتمام، فيليبس، مقابلة مع المؤلف، ماديا نسكي، ثناء إلى سيسيل فيليبس.
- إلقاء دوار بخاري: ملحق مؤرخ في 1942/8/1، ستيفنز إلى لندن، 1942/7/31، HW14/47، ديوان السجل العام.
- لم يُقدم طلب مطلقاً: مذكرة 1943/9/8، اتفاقيات الولايات المتحدة وبريطانيا حول جهد مخابرات الاتصالات 1942–1943، رقم 4013؛ مجموعة الرسائل السرية التاريخية، كتبت الكلمات (لم ترسل) على وجه المذكرة بقلم رصاص.
- غالباً ما تأخذ الانطباع كوردرمان من فريد 1944/11/1، ملفات كلارك رقم 4566، مجموعة الرسائل السرية التاريخية.
- توف إرسال شارع بيكرلي IB32164، ملفات كلارك، رقم 4566، مجموعة الرسائل السرية التاريخية 15.
- وكذلك كانت الرأس النحاسي: مفكرة الحرب، OP–20–G–4–D–2، ملخص للفترة من 1944/11/26 إلى 1944/12/25. و1945/1/8، OP–20G قسم

مفكرات الحرب (مختلفة). CNSG5750/159، ملفات كرين، الأرشيف الوطني بكلية بارك. كانت مجموعة رسائل بين واشنطن وموسكو، وموسكو وواشنطن بلغت 2000 رسالة تم تفتيشها بحثاً عن الاختلافات في مجموعة الشيفرات التي استخدمت كوبر هيد (الرأس النحاسي). وصنفت الأنظمة الروسية الخمسة. بـ ZZA إلى ZZE من قبل أرلنغتون هول؛ والنظام ZZE هو الذي قام فيليبس بعملية التفكيك الأصلية، والتي تبين أن الكي جي بي (نبسون، مقابلة مع المؤلف) قد استخدمها، وتغير التنظيم بضع مرات: وأخيراً أشير إلى نظام التشفير التجاري ظاهرياً بأنه ZET، وكان نظام الكي جي بي ZDI، وكانت الرسائل الروسية عموماً يشار إليها بأنها (زرقاء) من قبل أرلنغتون هيل؛ انظر التقرير السنوي لفرع تحليل الشيفرة في الوكالة العامة لأمن الإشارة، عن سنة 1945، رقم 4360، مجموعة الرسائل السرية التاريخية، 5–7.

- في السفارة البريطانية في واشنطن: تطوير قضية Homer G... (Gomer)، 1952/10/11، النشر العام لنسخ من السجلات المتعلقة بمشروع VENONA، الأرشيف الوطني بكلية بارك.
- القصة يوماً بيوم: بينسون، (دراسات تاريخية محددة VENONA)؛ مقدمة إلى VENONA الولايات المتحدة.
- رفض وايباند الاعتراف أو الإنكار: تقرير عن المكتب الميداني بواشنطن، الـ إف بي أي، 1953/11/27، «وليام وولف وايسباند» في الولايات المتحدة VENONA، 170.
- جون كيركروس: (مفككو الشيفرة) إعداد هنسلي وستريب، ص 26، 207–208.
- كان اسم الرمز BARON، ويست: VENONA.
- 3651 صفحة: عمل الشيفرة المنفذ في S.S.A على GEE، رقم 970، مجموعة الرسائل السرية التاريخية.
- دارات بشكل معقد: وسادة لمرة واحدة، رقم 1440، مجموعة الرسائل السرية التاريخية.
- 110 شخص يعملون: فرع تحليل الشيفرة من قيادة أمن الإشارة–التقرير السنوي لعام 1945 رقم 4360، مجموعة الرسائل السرية التاريخية 23–24.

- بدأ تيلتمان العمل بها: (مفكو الشيفرة) إعداد هنسلي وستريب 161؛ فوكس، مغامرات ضخمة، توت السمكة وأنا. في الحساب الثنائي بدون جمل، ينفذ الجمع قليلاً قليلاً، وفق القاعدة 1+1=0، 1+1=1. ولهذا خاصة مثيرة للاهتمام بأن الجمع تماماً كالطرح، ولذلك فإن التشفير وفك التشفير يمكن تنفيذهما من خلال الآلة ذاتها.
- مفضل لدى النقيب رالف تيستر: مذكرة حول وضعية ليست مورس، 1943/9/18، HW14/88، ديوان السجل العام، الحكومة السويدية بمساعدة عالم الرياضيات اللامع آرني بورلينغ، حققت أيضاً تفكيكاً لرسائل الطابعة الألمانية وذلك باستخدام الطرق اليدوية، في صباح اليوم التالي لغزو ألمانيا الدانمارك والنروج في 9 نيسان 1940، طلبت الحكومة الألمانية من الحكومة السويدية السماح لها باستخدام الكبل السويدي على الساحل الغربي للاتصالات بين برلين وأوسلو. ترددت ستوكهولم وتلكأت حتى لا تثير شكوكاً، ومن ثم وافقت على مضض في 14 نيسان، وبعد بضعة أيام تدخل الفنيون في التليفون السويدي في الخط واستخدم بورلنغا عمق الرسائل التي أرسلت بالمفتاح ذاته، حلل أول رسالة بعد بضعة أسابيع، ومنذ ذلك الحين حتى 1944، عندما بدأت الرسائل تبدو صعبة على الطرائق اليدوية لتحليل الرسالة، قرأ السويديون 300000 رسالة ألمانية مطبوعة عن بعد. انظر (نجاح سويدي).
- وصلت إلى نيومانري في أيار 1943، المخابرات البريطانية 3 (1): 479.
- ثلاثون ميلاً في الساعة: جاك غود (مفكو الشيفرة) إعداد هنسلي وستريب ص 163، وصف فني كامل لرينسون والعملاق يظهر في تقرير الهجوم البريطاني على (فيش) رقم 1596، مجموعة الرسائل السرخية التاريخية؛ وكذلك فلاورز، تصميم العملاق.
- يشتعل غود، أعمال مبكرة، 73–74.
- مقابل ما يقرب من ثمانين ألف رسالة إينغما: المخابرات البريطانية، 2: 29.
- لم يكن حتى يعرف الاسم: المخابرات البريطانية 4: 12.

- بالاعتماد على من تكلمت معه: يبدو أن الاسم الأصلي (سلسلة محرمة Illicit Series) وفرخ الأشكال الأخرى مع مرور الزمن، وربما كانت الأسباب أن ويليام فريدمان الذي أمضى بضعة أشهر من بليتشلي بارك من عام 1943، عرّف في تقريره حول أقسام ISOS وISK في 1943/11/25، وربما جاءت العبارة (سلسلة محرفة) غير موفقة، وربما ظهرت من حقيقة أما بالأيام الأولى انبثقت الرسائل من آلة بث يعمل بها عملاء جواسيس موجودون في دول معادية أو محايدة، ولكن في الوقت الحالي، فمعظم الرسائل على الأقل حتى الآن حيث إن المحطات الموجودة في أوربا تهتم بالتعامل بطريقة رسمية أو شبه رسمية بحيث تصبح عبارة (محرمة) و(غلاند ستاين) لا تنطبق عليها بصورة صحيحة، أنظر أيضاً النظام GEO (برتقال)، مذكرات Ger ASA على GEO (البرتقال) أي (الآلة البرتقالية) عمر الرسالة 1 رقم 4318، مجموعة الرسائل السرية التاريخية، 3.
- جهز ISK لعائدة لديلي نوكس: انظر مقدمة نيجل ويست في ماسترمان، (نظام الفحص المزدوج، xv).
- تفكيك رسائل الإينغما الأبويهر: المخابرات البريطانية 4: 108، ديفرز إينغما اللوبسترز: والكرابس، والأبويهر، هامر وسوليفان وويرود، إينغما متنوعة، 219–220.
- خمس من تلك المحاولات ISOS كشفت: المخابرات البريطانية 4: 95..
- أصبح حقيقة مؤكدة: المخابرات البريطانية 4: 108–111.
- ذهب إلى لشبونة: ماسترمان، نظام الفحص المزدوج 115–116؛ المخابرات البريطانية 4: 112.
- قافلة من ليفربول إلى مالطة: ماسترمان، نظام الفحص المزدوج 116؛ المخابرات البريطانية 4: 114.
- آسف وصلوا متأخرين، المخابرات البريطانية 5: 63.
- كان الغزو وشيكاً: بينيت، (وراء المعركة) 261.
- بعد ثلاثة أيام: ماسترمان (نظام الفحص المزدوج) 156–158.
- منح الصليب الحديدي مكافأة: ماسترمان (نظام الفحص المزدوج) 173–175.

- دارت الحرب لمدة عشرين دقيقة، بويد (ثقة هتلر باليابانيين) 118.
- استمرت تقارير أوشيما تقدم التأكيدات: بويد، (ثقة هتلر باليابانيين) 127–128.
- تقديم معلومات محروفة بصورة ذكية: ماسترمان (نظام الفحص المزدوج) 178–182.
- كل يوم الساعة التاسعة صباحاً: ليتون (كنت هناك) 473.
- نُفذ حوالي 70٪ هيو دانهام في كتاب (مفككو الشيفرة) إعداد هنسلي وستريب، ص 277.
- الأسطول المشترك CINC سيقوم بزيارة: ميدوي وياما مونو: ربما روجع، الجيش والبحرية أوراق وتعليمات مخابرات الإشارة، رقم 4632، مجموعة الرسائل السرية التاريخية.
- ليتون ويتميتز، ليتون (كنت هناك) 473–74.
- لانفير سُرّح: ميلر (حرب البحر) 371.
- أحد عشر شخصاً: قسم حل رموز الجيش الياباني، رقم 2814، مجموعة الرسائل السرية التاريخية.
- انقسم النظام الرئيس، التاريخ الفني، مشكلة الجيش الياباني، الجزء 2 التطور التاريخي رقم 2718، مجموعة الرسائل السرية التاريخية 4–10.
- شهر بمقدار ثمانية أشهر، تاريخ تحليل الكتابة السرية لرموز الجيش الياباني، رقم 3072، مجموعة الرسائل السرية التاريخية 5004.
- دزينتان فقط، قسم حل رموز الجيش الياباني، رقم 2418، مجموعة الرسائل السرية التاريخية، السرية.
- من ثلاثة ملايين إلى أربعة ملايين بطاقة IBM، تاريخ والآلات رقم 3247، مجموعة الرسائل التاريخية، 40–41، تاريخ تحليل الرسائل السرية ورموز الجيش الياباني، رقم 3072، مجموعة الرسائل السرية التاريخية 36–38.
- حسابات إحصائية، تاريخ تحليل الرسائل السرية ورموز الجيش الياباني رقم 3072، مجموعة الرسائل السرية التاريخية 104.
- BPPS RCRC، تاريخ فني، مشكلة الجيش الياباني، جزء 2 تنمية تاريخية، رقم 2718، مجموعة رسائل سرية تاريخية 4–6.

- أشكال رسائل ملتقطة، تاريخ فرع تحليل الرسائل العسكرية (حتى 30 حزيران 1944)، رقم 2719، مجموعة الرسائل السرية التاريخية، مجلد I/D/4/2، لويس، مقابلة مع المؤلف.
- مربع التحويل 10 × 10، دورة جديدة في تعليم أنظمة الجيش الياباني SSA–A، رقم 2836، مجموعة الرسائل السرية التاريخية، 33.
- CBB بعث برقية، مانيكي (أبطال هادئون) 35–36، تاريخ فرع تحليل الرسائل السرية العسكرية، (حتى 30 حزيران 1944)، رقم 2719، مجموعة الرسائل السرية التاريخية، مجلد 2 و4 و12.
- تضاعف ثلاثة أمثال ليصبح 270: قسم حل رموز الجيش الياباني، رقم 2418، مجموعة الرسائل السرية التاريخية؛ تاريخ فرع تحليل الرسائل السرية العسكرية (حتى 30 حزيران 1944)، رقم 2719، مجموعة الرسائل السرية التاريخية مجلد 2/2/4/2.
- نظام تشفير أكثر تعقيداً: قسم حل مشكلة رموز الجيش الياباني، رقم 2418، مجموعة الرسائل السرية التاريخية.
- الكلمة Sento: مايكل لووي: (مفككو الشيفرة) إعداد هنسلي وستريب، 259.
- أمضى تيلتمان أسابيع ذات مرة: بعض الذكريات، العميد جون هـ تيلتمان، الجيش والبحرية أوراق وتعليمات مخابرات الإشارة رقم 4632، مجموعة الرسائل السرية التاريخية 6–7.
- قدم نقطة دخول يعتمد عليها: تاريخ تحليل رموز الجيش الياباني، رقم 3072، مجموعة الرسائل السرية التاريخية 138–140، JAT يكتب من رسائل JMA رقم 3225، مجموعة الرسائل السرية التاريخية.
- في أوائل حزيران 1943: إنجازات وكالة أمن الإشارة في الحرب العالمية الثانية، SRH–349، الأرشيف الوطني بكلية بارك، 24–28.
- تفريغ في ويواك: إنجازات وكالة أمن الإشارة في الحرب العالمية الثانية –SRH 349، الأرشيف الوطني بكلية بارك 19–20.

- تسجيل CAMEL: تاريخ تحليل رموز الجيش الياباني، رقم 3072، مجموعة الرسائل السرية التاريخية 242.
- مكتبة كتابات سرية كاملة، مانيكي (أبطال هادئون) 40.
- تعليق الصفحات المبللة، دري، (ألترا ماك أرثر) 92–93.
- ست وثلاثون ألف رسالة: دري، (ألترا ماك أرثر) 93.
- نظام تفكيك الرسائل السرية آلي تماماً: تاريخ فرع تحليل الرسائل السرية العسكرية (حتى 30 حزيران 1944)، رقم 2719، مجموعة الرسائل السرية التاريخية، مجلد 18/D//4/2؛ تاريخ تحليل رموز الجيش الياباني، رقم 3072، مجموعة الرسائل السرية التاريخية، 13.
- ماك آرثر عارضها: دري (أُلترا ماك آرثر) 28–30.
- وزعت ألترا بحرية أكبر كثيراً: مذكرة إلى مدير الاتصالات البحرية، 1943/3/9، ملف OP–20–G، عن تعاون الجيش والبحرية، 1941 حتى 1945، SRH–200، الأرشيف الوطني بكلية بارك.
- اختراق معظم الحيل الألمانية: تحليل كامل لكافة إشارات الألترا المتعلقة بهجوم الأردين أنتجته GC+CS في 28 كانون الأول 1944، إشارات عن الهجوم الألماني في كانون الأول 1944 HW14/118، ديوان السجل العام.
- فوج الإطفاء، بينيت (وراء المعركة) 279.
- كلفت هتلر 20000 رجل: ستوكسبري (الحرب العالمية الثانية) 355.
- من أجل الحل النهائي، ولتر إيتان في (مفككو الشيفرة)، إعداد هنسلي وستريب، ص 60.
- هتلر ميت: أليك داكين في (مفككو الشيفرة)، إعداد هنسلي وستريب ص 56.
- تظاهرات من جميع الأنواع: الإشارة 5/1433/ D70 /1945/5/5/L37، ملفات تاريخية 1945/4/30–45/7/9 ملفات كرين، الأرشيف الوطني كلية بارك.
- قبل ساعتين، إنجازات وكالة أمن الإشارة في الحرب العالمية الثانية SRH349، الأرشيف الوطني بكلية بارك 19.

--- --- ---

التراث

خلال ستة أشهر كان تشرشل يحذر من أن «ستاراً حديدياً» ينزل على أوربا؛ وبعد سنتين أحتل ستالين تشيكوسلوفاكيا وحاصر برلين. وحلت الحرب الباردة محل الحرب الساخنة سريعاً جداً حيث كان قليلون في الغرب مستعدين لها، على الأقل من الناحية النفسية. فالجيوش المتعبة من الحرب أرادت العودة إلى أوطانها، وفي مانيلا وباريس وفرانكفورت تظاهر الآلاف من الجنود عندما تأخر تسريحهم فلم يكونوا راضين عن ذلك. وفي بليتشلي بارك حزمت المجندات متاعهن وذهبن إلى بيوتهن تاركات بعض العلامات لينقبن في الأكواخ بحثاً عن قصاصات من النفايات السرية التي قد تكون انزلقت خلف خزائن الملفات أو التصقت خلف أدراج المكاتب. خلع المدنيون (المجندون) في آرلنغتون هول وفي ملحق الاتصالات البحرية ثيابهم العسكرية وعادوا إلى حياتهم.

لقد كسبوا الحرب، وقد غيروا العالم، وهذا كل ما في الأمر، وربما كان ما لم يدركوه هو أنهم أنجزوا عملاً أكثر عظمة: لقد غيروا الجيش والبحرية. ولن يتكرر تجاهل الجنرالات والأميرالات للمخابرات. كانت المخابرات الآن مخابرات الإشارة، ومخابرات الإشارة كانت ماك كوي McCay الحقيقي. وكانت أيضاً سلاحاً مناسباً تماماً للحرب الجديدة، الحرب الباردة التي تقف غير بعد عنهم — حرب تدمير وتجسس، حرب نوايا وخداع، حرب تهديدات وردع. فقراءة أفكار العدو وتوقع خططه أمر مهم أكثر من أي وقت مضى في لعبة الشطرنج النووية. وكذلك حتى عندما ذهب محللو الشيفرة زمن الحرب إلى بيوتهم، بقيت المنظمات التي جمعوها من أجل هزيمة هتلر وتوجو، وبقيت تنمو بهدوء لتصبح بيروقراطيات

ضخمة ودائمة. وقام الجيش والبحرية بفعل ما لم يخطر ببال وذلك بتشكيل وكالة أمن القوات المسلحة، وبعد ذلك وكالة الأمن القومي، وبعد ذلك شكلا معاً ما أصبح مدينة حقيقية عند فورت جورج ج. ميد في ميريلاند، في منتصف الطريق ما بين التيمور وواشنطن. أصبحت الوحدة GC&CS رئاسة الاتصالات الحكومية (GCHQ) في تشيلتنهام. وكانت وكالة الأمن القومي ورئاسة الاتصالات الحكومية تستمعان إلى كل شيء – ليس إلى مجرد إشارات الراديو من قاذفات الاتحاد السوفياتي، ولكن إلى المكالمات الهاتفية عبر المحيط الأطلسي أيضاً، وحتى عندما كانت أهداف التنصت الآن مواطنين بريطانيين وأمريكيين لم يكن هناك وزراء خارجية يشتكون من قراءة بريد هؤلاء السادة.

أصبح ستار السرية المطلقة في الواقع أكثر شدة مما كان عند وضع عوائق للديمقراطية في زمن السلم. إن مقاضاة الحرب شيء، ومقاضاة مواطنين أمام المحاكم شيء آخر، فعندما قدمت رسائل فينونا VENONA المفككة الدليل على أنشطة تجسس سوفيتية قام بها آلغر هيس، وهاري ديكستر وايت، بوجوليوس روزنبرغ، تم الاحتفاظ بالدليل خارج نطاق المحكمة وخارج معرفة الجمهور. ومن المدهش، أنه حتى الرئيس ترومان جعله مساعدوه لا يعرف شيئاً. في عام 1949، اندهش رئيس وكالة أمن القوات المسلحة الجديد، والأميرال إيرل ي ستون، عندما علم بفينونا VENONA وقرر أن الرئيس ووكالة المخابرات المركزية CIA يجب إعلامهما فوراً. لكن كارتر كلارك، وهو الآن جنرال ورئيس آرلنغتون هول، عارض ذلك معارضة شديدة. وأصر على أن رئيس الولايات المتحدة لم يكن بين أولئك «الذين يحق لهم معرفة أي شيء عن هذا المصدر». وتوسل كلارك إلى الجنرال عمر برادلي رئيس أركان الجيش؛ ووافق برادلي على أن يأخذ مسؤولية شخصية في إعلام الرئيس «إذا اقتضت محتويات أي من هذه المواد ذلك». ويبدو أنها لم تفعل قط، من وجهة نظر الجيش. إن كانت الحرب مهمة جداً بحيث يجب ألا تترك للجنرالات، فإن إشارات المخابرات مهمة جداً بحيث يجب ألا تترك للسياسيين.

في زمن السلم وصلت ثقافة تحليل الكتابة السرية من عقدة الشك ذروة جديدة. في زمن الحرب كان هناك ضغط من القادة العسكريين لموازنة الأضرار التي لا تنكر والتي تنتج عن الكشف مع المكاسب التي لا تنكر والتي تنجم عن الاستعمال. في زمن السلم أصبحت السرية هدفاً بحد ذاتها، وأصبحت وكالة الأمن القومي NSA ورئاسة الاتصالات الحكومية GCHQ قوة بحد ذاتها، وأحياناً قانوناً بأنفسهما. وكان السخف كله في رفض إطلاع الجمهور الأمريكي على حقيقة الأدلة ضد هيس والآخرين، وكانت الحكومة تخفي أسرار الشيفرة كلها، وبينما كان الأمر سراً أكيداً على الجمهور الأمريكي، فلم يكن سراً على السوفييت وذلك بسبب خيانات فيلبي وفايزبند. شعرت المكارثية أن القصة الكاملة لم تُقص كاملة مما شجع اعتقادهم بأن «الوحوش» يختبئون في الخزانة وأن هناك حقاً مؤامرة شيوعية ضخمة للتسلل والسيطرة على حكومة الولايات المتحدة؛ وفي الوقت ذاته، تدع اليسار الأمريكي في معتقداته التي قد يتمسك بها لعقود من الزمن، وأن جميع اتهامات التجسس الشيوعي هي من اختراع واضعي الطعوم السامة الحمر. أصبح هيس ووايت وروزنبرغ شهداء اليسار الذين أصبحت براءتهم الكاملة مسألة إيمانية. في الواقع، كانوا مذنبين جداً ولو أن الحقيقة ذكرت في ذلك الحين لوفرت على الأمة مصائب كثيرة. ولأوقفت حتى بعض الاتهامات الأكثر سخافة بأن هيس والآخرين كانوا جزءاً من خطة شيوعية رئيسية قامت ببيع الصين إلى الحمر من خلال استعمال داخلي شيطاني للسياسة الأمريكية. كان هيس والآخرون جواسيس لكنهم لم يكونوا مرشحي منشوريا.

--- --- ---

جعلت ضرورات الحرب وارتجالها من آرلنغتون هول وبليتشلي بارك أمكنة حيث القواعد أقل أهمية من النتائج، وحيث القدرة على القيام بعمل أكثر أهمية من كون المرء عضواً في جماعة. عندما أعطى حكم النخبة المتميزه مكانه إلى البيروقراطية، وجرى شد حلقة السرية في زمن السلم لتصبح أضيق، بدأ التسامح مع المراوغات الشخصية والتجديد العقلي، الذي جعل مكاتب تحليل الشيفرة تبدو

كجامعات أكثر منها وكالات حكومية، يتضاءل ويخبو. وللتأكد من ذلك، تابعت وكالة الأمن القومي NSA صنع تجديدات في الحسابات، فبنت أول ذاكرة مغناطيسية في أعقاب الحرب مباشرة، وبعد بضع سنين، أول حاسوب في الولايات المتحدة يستخدم الذاكرة المغناطيسية الجوهرية. وأول التراث الباقي من تحليل الشيفرة في الحرب العالمية الثانية وما بعدها كان الإزدهار الكبير الذي أعطته إلى صناعة الحواسب، وحتى اليوم تبقى وكالة الأمن القومي NSA المستهلك الكبير والمجمد في حسابات النهاية العليا. واستمرت وكالة الأمن القومي NSA تظهر بعض التسامح باتجاه الفردية؛ فليس هناك اختبار صلاحية سياسية يفرض على هيئة العاملين المهنيين. إن كان هناك مسح سياسي للعاملين في آرلنغتون فإنه، إن كان هناك أي شيء، يميل إلى يسار المركز قليلاً، وكثير من محللي الشيفرة في القمة والذين مكثوا وارتفعوا إلى مراكز إدارية كبيرة في وكالة الأمن القومي NSA في الخمسينيات والستينيات والسبعينيات هم من الليبراليين السياسيين. أمضى فرانك لويس السنوات بسرور يطارد الشيوعيين ويحقق مع الموالين في الخمسينيات وهو يعمل كموظف كبير في وكالة الأمن القومي بينما كان يدير ألغاز الكلمات المتقاطعة لمطبوعة يسارية متطرفة، الأمة، ولم يستغرب ذلك أحد.

كانت قصة آلان تيورينغ قضية أخرى. كان تيورينغ غير سياسي بصورة كاملة تقريباً؛ لكنه كان شاذاً جنسياً أيضاً، وهكذا كان بالنسبة لعقل الوحدة M15 في بريطانيا ما بعد الحرب خطراً أمنياً. لم يتطرق تيورينغ بشكل خاص إلى شذوذه الجنسي، لكنه لم يكن خجولاً أو متباهياً إزاء هذا الأمر، كانت السمة المميزة له أنه يفكر بالأشياء بعقله وبعد ذلك لا يهمه بما يفكر العالم بذلك. وهكذا عندما ذهب إلى قسم الشرطة في كانون الثاني 1952 ليبلغ بأن بيته قد اقتحم وأن بعض الأشياء قد سرقت – وأنه يشك بصديق من الطبقة العاملة التقطه تيورينغ ليمضي معه بضع ليال – وعندما بدأت الشرطة تسأله بعض الأسئلة الموجهة حول بعض التناقض في قصته، وحول كيف يقوم زميل للجمعية الملكية باستضافة مساعد طباع عمره تسعة عشر عاماً في بيته، أخبرهم تيورينغ بصورة ساذجة. كان

تتبع اللصوص عملاً شاقاً، لكن اتهام الناس الذين يأتون إلى أقسام الشرطة ويدلون باعترافاتهم كان عملاً سهلاً، ولقد اعترف تيورينغ بجريمة خطيرة هي «الفاحشة الكبرى»، وهذه هي العبارة القانونية «لأعمال الشذوذ الجنسي الرضائي» بموجب قانون عام 1885 الذي لا يزال في الكتب، ويعاقب عليها بالسجن لمدة عامين. وأقر تيورينغ بأنه مذنب فأعفي من السجن إن هو قبل «المعالجة» لشذوذه بما في ذلك حقن هرمونية إجبارية.

في وقت من الأوقات عرض هيو الكسندر على تيورينغ مرتباً قدره 5000 جنيه ليعود إلى رئاسة اتصالات الحكومة لمدة سنة ليتقدم إلى عمل في فترة ما بعد الحرب على الكمبيوتر وعلى المشكلات الجديدة في تفكيك الشيفرة. في شهر تشرين الأول 1952 أسر تيورينغ إلى صديق له أنه يعرف بأنه من المستحيل عليه الآن أن يسمح له بالعمل في رئاسة الاتصالات الحكومية GCHQ. وبعد سنتين قتل نفسه بأكل تفاحة مغموسة بالزرنيخ.

وربما كان ضرورياً، مع الحماس للتغيير، أن السلطات العسكرية والسياسية اللتين أهملتا مخابرات الإشارة زمناً طويلاً ستتوصلان مع الزمن إلى المبالغة في تقديرها. إن النجاحات الكبيرة التي حققتها زمن الحرب وسحرها التقني جميعها كانت مقنعة جداً – والفشل الذريع والمستمر في السعي لإدارة عملاء من البشر الحقيقيين كان مثبطاً – لدرجة أن «الوسائل التقنية القومية» (التي ستشمل فيما بعد الأقمار الصناعية للتجسس والمستشعرات الأخرى عن بعد) جاءت لتسيطر على جمع الاستخبارات. كان هناك أوقات حيث كانت الولايات المتحدة مستعدة لتدفع مقابل التأكيدات الراجحة. وقد تصبح الندرة في المخابرات البشرية موضوعاً يتكرر في الصراع ضد مجموعات المتمردين والإرهابيين في الستينيات والسبعينات والثمانينات.

بعد مرور نصف قرن، من الممكن النظر إلى الوراء على انجازات تفكيك الشيفرة في الحرب العالمية الثانية نظرة أكثر تحديقاً. فعلى مستوى انتصار العقل البشري كان غير عادي. وعند بعض النقاط الحساسة – مثل ميدوي، وكيب

ماتابان، وتل الحلفا، وأول معارك قوافل المحيط الأطلسي – أدت القراءة المناسبة لرسائل العدو إلى تفادي كوارث كان يمكن أن تكون نكسات فظيعة لقضية الحلفاء. لا سيما في البحر، حيث معرفة مكان العدو في خضم المياه الشاسعة كانت أكثر من نصف المعركة، ولعبت مخابرات الإشارة دوراً لا يجارى، وكذلك أيضاً في تنفيذ الخداع الفعال، حيث تمثل معرفة ما يفكر فيه العدو بصورة علمية المعركة بكاملها.

ولكن هل «كسبت» عمليات تفكيك الشيفرة الحرب، كما يزعم غالباً؟ والجواب هنا أكثر التباساً. في معركة الأطلسي في عام 1941، ساعدت مخابرات ULTRA بشكل واضح في إمالة كفة الميزان في وقت وصلت فيه عمليات الإغراق معدلات خطيرة، ولكن هناك عوامل أخرى كانت تؤدي عملها أيضاً، ليس أقلها سحب الغواصات U من المحيط الأطلسي دعماً للهجوم الألماني على روسيا، ودعم سفن الحلفاء التي تقوم بالمرافقة. في ذروة المعركة في ربيع عام 1943 لعبت ULTRA دوراً أكبر، وكذلك فعلت قنابل الأعماق والرادار والقوى الجوية. إن الحسابات البسيطة التي تقارن ما بين الأطنان المفقودة من الحمولة شهرياً قبل عملية فك شيفرة «الشارك» وبعدها، وإعطاء كل الفضل إلى بليتشلي بارك في إنقاذ هذه الأطنان بواسطة تلك العملية، تشكل خطأ كلاسيكياً في الحجة والبرهان.

حتى في الحالات التي يستطيع فيها المرء أن يفرد معركة واحدة حيث كانت ULTRA العامل الحاسم بشكل واضح، فإنها تتجه نحو معتقد خطير يفترض أنه لو أن ULTRA كانت غائبة فيمكن أن تضيع المعركة بالخسارة. إن اللعبة الكاملة لتاريخ «مضادات الحقائق»، حول ماذا لو، هبوط إلى حيث لا توجد أرض أبداً. يعاش التاريخ إلى الأمام، وليس إلى الخلف، ومن الحماقة الافتراض إن تغير عامل ما عندئذ تبقى باقي العوامل التي تقرر سير التاريخ نفسها دون تغيير. لو لم يكن الأولترا ULTRA موجودة، كيف يمكننا القول إن الحاجة لن تدفع الحلفاء لاتخاذ اجراءات أخرى يمكن أن تكون فعالة مثلها، أو أكثر فاعلية في مجابهة التحديات التي تواجهها؟ على سبيل المثال، إن لم تكن هناك الأولترا ULTRA أبداً، واستمر

الإغراق في المحيط الأطلسي وهُدد خط حياة بريطانيا، فإن الضغوط من أجل تحويل القاذفات ستصبح شديدة، ولا يمكن مقاومتها، من الحملة الجوية الاستراتيجية لجعلها تحمل على تهديدات الغواصات – كما حصل فعلاً في النهاية في أي حادث. وليس من غير المتصور أن الخطوات المطلوبة كثيراً يمكن أن تأتي في وقت أبكر لو لم يوجد بليتشلي بارك موجوداً. في الحرب، كما في الحياة، وكما لاحظ ونستون تشرشل الحظ قطعة كاملة؛ ولا يعرف المرء متى ينقذ ما يبدو أنه حظ سيء شخصاً مما هو أكثر سوءاً.

والحجج التي قيلت عن الأولترا ULTRA بأنها قصّرت الحرب بضع سنوات تصطدم بالسلاح الوحيد الذي يتحدى الانتقادات القاسية للتفسير الواحد للتاريخ: القنبلة الذرية التي يجب ألا تنسى أبداً، بنيت منذ البداية وكانت النية والتوقع أنها ستستخدم ضد ألمانيا.

بعدما قلنا ذلك، كان في الحرب نقاط مفصلية حيث أضعفت هزيمة بريطانيا حزمها على متابعة المفاوضات لإنهاء العداوات التي يحتمل أنها بدأت. طبعاً كان هناك أولئك الذين فضلوا هذا المسار في صيف عام 1940 بعد سقوط فرنسا مثل اللورد هاليفكس. لقد أسهمت الأولترا ULTRA بشكل هامشي فقط في معركة بريطانيا، ولكن، للجدال، أكثر أهمية بالنسبة لحماية خطوط التموين البريطانية في المحيط في الأشهر الحاسمة من عام 1940 و1941 قبل دخول أمريكا الحرب، في الوقت الذي لم يكن فيه الغزو والانهيار غير متصور. كان تشرشل جاداً جداً عندما فكر بخطط لانتقال الحكومة إلى كندا لتتابع المقاومة إذا ما تم السيطرة على بريطانيا.

ولكن للمرة ثانية تعتم «الأسئلة ماذا لو؟» كل التفكير العقلاني: هل كان انهيار بريطانيا سيسرع دخول اليابان الحرب، وكذلك أمريكا؟ ممكن تماماً؛ ليس لمثل هذه السلسلة من التفكير أي نهاية.

وليست ضرورية حقاً. ربما كان تشرشل وستالين كلاهما قريبين جداً من الحقيقة عندما اعترفا بأن من كسب الحرب حقاً هو الجبروت الصناعي

الأميركي، وهو قوة لا يمكن إيقافها إذا ما أطلق لها العنان. لكن الحروب، مرة أخرى، تخاض عبر الزمن في اتجاه إلى الأمام. والانتصارات المحتومة في النظر إلى الوراء هي أي شيء مأمول أو متوقع، وأثناء الاحتفال بالانتصارات فإننا لا نحتفل بالنتائج فقط، ولكن بالتضحيات والذكاء والشجاعة التي تعرض على طول الطريق أيضا. في قصة تفكيك شيفرات دول المحور، عرضت كلها عرضاً وفيراً. لمناقشة الادعاءات الطبيعية والكثيرة حول نتائج عمل تفكيك الشيفرة لا تأخذ المرء ويجب ألا تأخذه بعيداً عن انجازاتهم الرائعة والمهمة.

--- --- ---

إن السؤال الآخر الذي يجول بالخاطر حول الشيفرة هو لماذا كانت منحازة جداً في النهاية. في أكثر من مناسبة كان الجواب بسيطاً بساطة مؤلمة؛ كما قال غوردون ويلشمان، «كنا محظوظين». لو أن تصميم آلة الإنيغما كانت متغيراً قليلاً في بعض دقائقها، أي الدقائق التي كانت أقرب ما تكون إلى قرارات تصميم إجبارية تقريباً، لكانت مهمة الحلفاء أكثر صعوبة بصورة كبيرة.

ولكن يبدو أن هناك أكثر من الحظ وراء العديد من الأخطاء التي ارتكبها الألمان، وبالنظر إلى الماضي وجد بعض المؤرخين من المغري أن يقولوا إن صلابة الألمان والأيديولوجية النازية منعتا توظيف المفكرين المطلوبين من أجل تحليل الشيفرة تحليلاً فعالاً؛ لم يكن يوجد في مكتب المخابرات الألماني B–Dienst مثل آلان تيورينغ. من السهل أيضاً أن يفكر المرء أن المجموعات المحاربة العديدة ضمن بيروقراطية النازية قد أعاقت التقدم في كل من تفكيك شيفرة الحلفاء وفي تحري الأخطاء في شيفراتهم.

ومع ذلك ليست الأمور بيضاء أو سوداء. لكن غورينغ❖ Göring من حماقته كان يكره العلم والتكنولوجيا، كما فعل كثيرون من قادة الحلفاء. وبالتأكيد لم يشاركهم دونيتز هذه الحماقات؛ حتى هتلر كان مغرماً «بالسلاح السري» كما

❖ غورينغ: سياسي نازي.

كان تشرشل كذلك. لم يكن لدى ألمانيا النازية أي صعوبات في تعبئة مواهب الأمة العلمية والهندسية لإنتاج المحركات النفاثة والصواريخ؛ وخلال الحرب كانت ألمانيا في مقدمة العالم في هذين المجالين. وعندما نصل إلى الحرب الضروس البيروقراطية، فإن من الصعب أن تجد من يساوي جيش الولايات المتحدة وبحريتها؛ عند نقطة من نقاط الحرب اكتشف الجيش أن البحرية ترفض تحرير الرسائل إلى آرلنغتون هول الرسائل المفككة من شيفرة البحرية اليابانية لمدة ستة أشهر، وهي التي لا تقدر بثمن في تفكيك شيفرة الجيش الياباني التي غالباً ما كانت تحتوي على تشفير مكرر لتلك النصوص ذاتها. وفي بليتشلي بارك، كانت البحرية الأمريكية تسعى لمنع ضباط جيش الولايات المتحدة من الدخول إلى المناطق التي يجري العمل فيها على الإنيغما.

لم يكن مفككو الشيفرة الألمان متخلفين طبعاً عندما يتعلق الأمر بالفهم الفني. فقد كانوا يعرفون طرائق IBM معرفة كاملة، وكانوا يوضحون في وقت باكر في عام 1943 أنه من الممكن من الناحية النظرية أن يتم اكتشاف إعدادات الإنيغما ذات القوابس إذا ما توفرت مطابقة. في عام 1944 صنع الملازم ر. هانز – جوشيم قروفاين من فرع أمن اتصالات القيادة العليا للبحرية (R. Hans – Joachim Frowein)، طريقة سجلت كتالوجاً من تغيرات قرص دوار للإنيغما على سبعين ألفاً من بطاقات IBM؛ وأظهر كيف يمكن استخدام البطاقات (بطريقة مماثلة لطريقة عصيات نوكس) لتشفير نص بسيط بشكل جزئي، ويماثل نص الشيفرة ويتفحص الأزواج الناتجة من التشفير من أجل تناقضات منطقية. (طبقت طريقة «Scritching» التي استخدمتها الحواسب المحللة للشيفرة في آرلنغتون هول والمعروفة بـ Autoscritcher وSuperscritcher). وهكذا فإن البعض في مكاتب الشيفرة الألمانية كانوا مدركين للأخطاء الأصيلة في الإنيغما.

جرى اقتراح التحسينات على الإنيغما وذلك للتغلب على نقاط ضعفها الكبيرة خلال الحرب. وفي عام 1944 بدأت القوى الجوية الألمانية بتقديم العاكس الذي يمكن أن يوصل بقابس والذي يمكن أن يشكّل بحسب الإرادة، وهذا فعلاً ما

جعل مفككي الشيفرة لدى الحلفاء لا يتوصلون إلى نهاية للمشكلة. تم تطوير بضع آلات لأغراض خاصة من بينها Scritchers آرلنغتون هول كمحاولة لاحتمال هذه المسألة؛ تطلبت الطريقة القياسية للهجوم مطابقة ذات مائة حرف، وحتى عندئذ لم يكن هناك أي تأكيد للنجاح. وجاء تغيير آخر في 10 تموز 1944 عندما أصبحت بعض مفاتيح القوى الجوية لا يمكن قراءتها دون أي سابق تحذير. أشارت رسالة مفككة في ذلك اليوم إلى بعض الرسائل التي تم تشفيرها بجهاز غير معروف مسبقاً يدعى «إنيغما أوهر». اشتغل فريق في الكوخ 6 ثماني وأربعين ساعة دون توقف وقرر أن الأوهر Uhr – التي تعني «الساعة» بالألمانية – يحتمل أنها إضافة يمكن أن توصل بواسطة قابس في لوحة القوابس، وبواسطة مفتاح تدوير تولد أربعين تغييراً مختلفاً بين عشرة قوابس مختارة لذلك اليوم. وكانت بعض هذه التغييرات غير متبادلة، وهذا شيء جديد تماماً: فيمكن وصل الحرف B مع الحرف E، ولكن الحرف E يوصل بالحرف H بواسطة القوابس، وهذا يعني أنه من المستحيل الآن استخدام «القنبلة» بلوحة قطرية (محورية). ولكن يمكن استخدام «القنبلة»، ولكن بعد فصل اللوحة القطرية (المحورية)، وكانت المطابقات الأطول من العادية ضرورية.

لكن تم تقديم هذه التحسينات تقديماً فاتراً ومتأخراً وشيئاً فشيئاً، وخلال الحرب أظهرت مصالح الشيفرة الألمانية إضراباً حول ما كان يعتمد عليه أمن الإنيغما.

احتلت الإنيغما كجهاز شيفرة حيزاً من الأرض في منتصف الطريق بين عالمين، عالم تقليدي وعالم حديث فيما يخص الشيفرة، وهنا تكمن الفوضى، كانت الإنيغما حديثة في تصور الطريق الفترة الرئيسية الطويلة التي صممت لتهزم هجوماً إحصائياً؛ لكنها كانت تقليدية في الطريقة التي اعتمد على سرية التصميم والوسائل التي قدمتها (مثل إعداد الحلقة) للاختباء من العيون المحدقة في اعدادتها اليومية. إن الكثير من المخاوف الأمنية التي واجهها الألمان أجيب عليها بتحسينات في أمن الآلة «وسريتها» وتكوينها الفيزيائي، بينما هم لم يفعلوا شيئاً حول عدم

أمنها من الناحية الإحصائية. وبالفعل، كثير من هذه الإجراءات جعلت الأمور أسوأ. فالقوانين التي منعت استخدام الدولاب نفسه من نقطة البدائية نفسها في أيام متتالية، أو تلك التي تطلب أنه لا يجوز استخدام حرف الوضع الابتدائي نفسه أكثر من مرة في الشهر في المفاتيح «الخاصّة بالضباط»، تصبح ذات معنى إن كان ما يخشاه المرء هو بعض الجواسيس أو الخونة الذين يلمحون إعدادات الآلة لأحد الأيام، ولكن كل ما فعلوه، بحسب ما اهتم به بليتشلي بارك، هو أنهم جعلوا عملهم أسهل وذلك بإضاءة عدد من الاحتمالات التي يحتاجون إلى تجريبها عندما ينقضي الشهر. اليوم تعتمد خطط التشفير على الأمن الإحصائي فقط؛ إن الفكرة الرئيسية هي أن باستطاعة المرء أن يشيع خطط التشفير، ويتأكد فقط من وجود مجموعات كثيرة جداً يستطيع أي كمبيوتر أن يديرها خلال فترة معقولة من الزمن. لذا دفع الألمان الثمن من نواح عدة وذلك لكونهم رواداً؛ وتبنوا شيفرة الآلات باكراً جداً، وألزموا أنفسهم بتصميم، حتى عندما أتخذ خطوات واسعة في عصر التشفير الجديد لكنه كان يحتفظ بقدم يجره وراءه في التصميم القديم.

ومع ذلك تبقىحقيقة لا يمكن منافستها، وهي في حرب الشيفرة، انتصرت دول الحلفاء، وترنحت دول المحور. ارتكب الحلفاء أخطاء وتم شفاؤهم منها، ولكن لم تفعل ذلك دول المحور. بدأ الحلفاء الحرب بإهمال وكره لمخابرات الإشارة بكل جزء عظيم عظمة ألمانيا واليابان؛ وخلال سنوات قليلة صححوا حماقاتهم الماضية، بينما فشل الألمان واليابانيون بذلك فشلاً ذريعاً. كان دونيتز الاستثناء بين قادة المحور وليس القاعدة من حيث الأهمية التي علقها على المخابرات؛ ولم يبدو على معظم القادة الألمان واليابانيين أنهم يلتقطون الفكرة. سرحت البحرية اليابانية مصلحة مخابراتها في عام 1932، وحتى بعد ذلك أعيدت إلى الحياة بعد خمس سنوات لم يظهر أي دليل على أن القيادات اليابانية تعطيها اهتماماً كبيراً. بقيت عمليات تفكيك الشيفرة اليابانية خلال الحرب لا مركزية ومجزأة. لم ينجح مفككو الشيفرة اليابانيون في قراءة الشيفرة الصينية العسكرية والديبلوماسية، وبعض الشيفرة البريطانية من المستوى الأدنى والمتعلقة بالطقس والسفن التجارية –

وربما كان أهم نجاح لهم – شيفرة تنقلات الطائرات الأمريكية، التي كانت تذكر أرقام الطائرات وأنواعها وميناء المغادرة والوصول إلى القواعد الجوية في مسرح جنوب غرب المحيط الهادي. وكان معظم العمل تنفذه أقسام مخابرات خاصة منفصلة وملحقة في جيش المنطقة أو الجيش الجوي مع ذلك فإنها لم تحقق التنسيق أو التجمع الحاسم للموهبة والجهد المركزي، اللازمين لتفكيك شيفرات الحلفاء من المستوى العالي.

لم تكن محض صدفة أنه عندما ترنحت دول الحلفاء، كما فعلوا عندما أخفقوا بالتفكير بالتحذيرات في هجوم الآردين، وفعلوا الشيء ذاته عندما انتفخت رؤوسهم بالنصر وثقتهم المبالغ بها ببراعة قواتهم العسكرية وحدها. لكن هذا فشل يلازم الأنظمة الجماعية والعسكرية. وفي النهاية إن الدول الجماعية في الهجوم تميل إلى تصديق دعاياتها بتميزها القومي وأنها لا تُغلب. وتحليل الشيفرة عمل كبرياء علوي يلطف من غلوائه تواضع علوي: إن الاعتقاد بأن أسرار أعداء المرء التي يحميها بشكل لصيق يمكن أن تكشف بواسطة تدريب صاف لقوى العقل، والاعتقاد بأن تلك الأسرار جديرة بأن تُعرف.

--- --- ---

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.

- حتى الرئيس ترومان أبقي في الظلام: موينهان: (السرية) 70–72.
- تجديدات في الحساب: تأثير منظمات الكتابة السرية في صناعة الحاسوب الرقمي، SRH–003، الأرشيف الوطني بكلية بارك، 5–8، بروك، تقرير بندرغاس.
- كانوا ليبراليين سياسيين: فيليبس، مقابلة مع المؤلف.
- يعالجون أحجيات الكلمات المتقاطعة: لويس، مقابلة مع المؤلف.
- أخبرهم تيورنغ بسذاجة: هودجز (تيورنغ) 496–497.
- عرض مرتباً قدره 5000 جنيه: هودجز (تيورنغ) 496–497.
- 334 كنا محظوظين: ويلشمان (قصة الكوخ السادس) 169.
- رفض لمدة ستة أشهر: كارتر وكلارك، مذكرة للجنرال بيسيل، الموضوع: اتفاقية الجيش والبحرية بخصوص الألترا، 1944/3/4، الجيش والبحرية أوراق وتعليمات مخابرات الاتصالات، رقم 4632، مجموعة الرسائل السرية التاريخية.
- هانس، جوشيم فراوين، مخابرات شارة المحور الأوروبية في الحرب العالمية الثانية كما كشفتها أبحاث TICOM والتحقيقات مع أسير حرب آخر ومواد مصادرة،

وبصورة خاصة ألمانية، المجلد 2 – ملاحظات حول الكتابة السرية وتحليلها عالية المستوى من ألمانيا، وكالة أمن الجيش، 1946/5/10، المتحف الوطني للكتابة السرية.

- عاكس يمكن وصله بقابس، عملية 25 D تموز 1944، HW14/108، ديوان السجل العام، إينغما الجيش الألماني والقوى الجوية الألمانية، 27 آذار 1945، الإينغما (مؤتمرات، نظرية ومعلومات ذات علامة). رقم 1737، مجموعة الرسائل السرية التاريخية؛ مذكرة حول الاجتماع، 29 آذار 1944، فرانك روليت، "ملف– سجلات إدارية لوكالة أمن الجيش، فرع تحليل الرسائل السرية المعادية" رقم 3070، مجموعة الرسائل السرية التاريخية.
- من دون تحذير بعض مفاتيح لوفتواف: الإينغما أوهر، الكوخ السادس، 17 تموز 1944، HW14/108، ديوان السجل العام.
- الدليل على أن القادة اليابانيين قد فكروا بذلك كثيراً: بارنهارت المخابرات اليابانية، 426–428.
- لقد نجح محللو الرسائل اليابانيون: نظام المخابرات الياباني SRH–254، الأرشيف الوطني بكلية بارك، نجاح اليابانيين في قراءة أنظمة الكتابة السرية لحركة الطيران، رقم 2727، مجموعة الرسائل السرية التاريخية، تقييم مخابرات الإشارة اليابانية، رقم 4547، مجموعة الرسائل السرية التاريخية.

--- --- ---

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

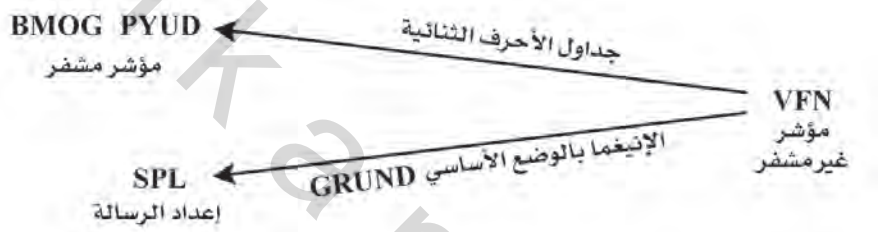
وتقسم الأحرف بعد ذلك إلى حرفين وتكتب أفقياً:

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

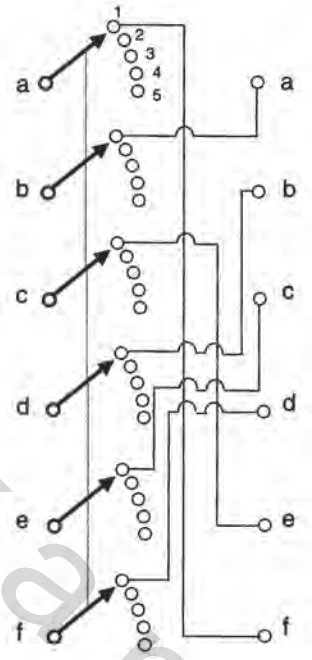
فمن الممكن البدء بصنع تحديدات باستخدام معرفة التكرار الحقيقي للأحرف a وb وd وh وo وr في نص ياباني بالرموز الرومانية. إن الحرف o أكثر الأحرف الستة تكراراً، وبعده يأتي الحرف o. وهكذا من المحتمل أن يكون الحل بالنسبة للمركز الرئيس 1 هو D = 0؛ وللمركز 2 هو H = 0؛ وللمركز الثالث هو

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.

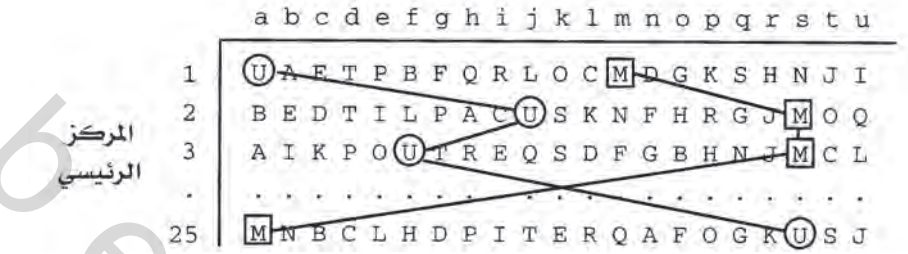


إن عملية توصيل أسلاك مفاتيح «الخطوة» لفتاة «الأحرف الستة» في الآلة البنفسجية، تصور الصلات البينية لمفتاح المركز 1 في جدول البدائل أعلاه. تتحرك المفاتيح الستة معاً بتزامن خلال 24 مركزاً، ثم تعيد الدورة.

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).

--- --- ---