طبيعة الوحش

عرفت الكتابة السرية منذ معرفة الكتابة تقريباً. لكن علم فك الرموز غير المعروفة نشأ مع ازدهار الرياضيات وتأليف المعاجم في العالم العربي في العصور الوسطى. ففي القرن الرابع عشر أسس الفلاسفة العرب المبدأ الأساسي لكشف هوية الأحرف في الشيفرة البسيطة، وهو المبدأ الذي قلما طرأ عليه أي تحسين خلال القرون التي تلت. فاستبدال مجموعة أحرف أو رموز بأخرى لا يمكن أن يخفي حقيقة هي استعمال بعض الأحرف أكثر من غيرها في اللغة الأصلية. لاحظ العرب أن حرف الألف أكثر الحروف تكراراً في الكتابة العربية، كما لاحظوا أن حرف الظاء أقل استعمالاً؛ كما لاحظوا أيضاً أن اجتماع بعض الأحرف معاً يحدث في كلمات بينما اجتماع بعض الأحرف الأخرى نادر بل ومستحيل؛ وهكذا يمكن تعداد المرات التي يتكرر فيها كل رمز في رسالة مشفرة يمكن أن يساهم ذلك في معرفة الهوية الحقيقية للرمز. تنصح مقالات عربية من العصور الوسطى بصنع تعداد التكرار في الخطوة الأولى لفك رموز رسالة مشفرة؛ وهذا ما فعله وليام فريدمان في «عناصر تحليل الشيفرة»، وهو درس بدأ بإعداده في العشرينيات.

في اللغة الإنكليزية، تحتوي قطعة نثرية اختيرت عشوائياً على حرف «*e*»، وهو أكثر الحروف تكراراً (بنسبة 12٪)، جاء بعده حرف «*t*» (بنسبة 9٪) وبلغت نسبة الحرف «*a*» و«*o*» (8٪)، كما بلغت نسبة تكرار كل من الحرف «*i*» و«*n*» و«*s*» (7٪) وحرف «*r*» (6٪)؛ ونأتي إلى أحرف المؤخرة وهي «*j*» و«*k*» و«*x*» (بنسبة 0.5٪ لكل منها) وحرف «*q*» و«*z*» (بنسبة 0.3٪ لكل منهما). فكلما طالت الرسالة اقتربت أحرفها من نسب التكرار هذه، ولكن الرسائل القصيرة لا يحتمل أن تشذ

عن ذلك كثيراً؛ فالرموز الأكثر تكراراً في رسالة مشفرة قد لا تكون الحرف «e»، ولكنها يستبعد أن تقوم مقام «q» أو «z».

وجمع الأحرف مع بعضها عامل للكشف كبير. فهنا 26×26 احتمالاً مختلفاً لاجتماع حرفين معاً من أحرف الهجاء الإنكليزية. وإذا وضع تكرار الأحرف مع كل من هذه الاحتمالات لاجتماع حرفين في رسالة مشفرة يمكن أن يضيق مجال الحل الممكن. فبعض أحرف الانكليزية لا تتضاعف في نص منا (مثل *hh*، *ii*، *jj*، *kk*، *qq*، *uu*، *ww*، *yy*) ولذلك يستبعد هذا الاحتمال في معرفة هويات أي رموز في رسالة مشفرة تظهر المضاعفات؛ وتظهر الأحرف الصوتية «*a*، *i*» و«*o*» مجاورة لأحرف أخرى أكثر مما تظهر مجاورة بعضها بعضاً، وهذه فكرة هامة تماماً في تحديد هوياتها، والحرف «*n*» أكثر احتمالاً أن يسبق بحرف صوتي أكثر من أي حرف ساكن آخر.

وتتكرر بعض أزواج من الأحرف بنظام معين ولا يظهر هذا النظام إلا نادراً أو لا يظهر أبداً (*ea* مقابل *ae*، و*lm* مقابل *ml*، و*rn* مقابل *nr*). وعندما تتحدد هوية عدد من رموز شيفرة بهذه الطريقة، تبقى معرفة الأحرف الباقية تعتمد على مهارة مساوية لمهارة حل ألغاز الكلمات المتقاطعة، فتملأ الفراغات لتشكل كلمات محتملة؛ ويمكن إلغاء الإجابات غير الصحيحة عندما ينجم عنها تناقض مع مكان آخر في الرسالة. فعلى سبيل المثال لو تم تحديد الرمز «X» في رسالة مشفرة على أنه «*a*» والرمز «G» على أنه «*u*» في الرسالة التالية:

النص المشفر Q G T L G X A L Z L F P P

النص البسيط – u – – u a – – – – – – –

يستطيع المرء الغاء الكلمة «kumquat» ككلمة أولى وذلك بجعل الرمز «L=*q*»، وهذا يتضمن تتابع الأحرف تتابعاً غير محتمل أبداً.

Q G T L G X A L Z L F P g
k u m q u a t q – q – – –

من جهة أخرى «Fun Guam» (والتي تتضمن أن L=*g*) تبدو أكثر صواباً وفائدة.

```
Q G T L G X A L Z L F P P
f u n g u a m g – g – – –
```

وبإملاء الفراغات الباقية لتشكيل الكلمة «gigolo» قد ينتج تحديد حرف إضافي (z = *i*, F = *o*, P = *l*) ويتم فحصها مرةً آخرى مع مكان آخر في الرسالة.

مثل هذه الشيفرات البسيطة أو المعتمدة على استبدال واحدللحروف كانت تستخدم في العوالم القديمة والوسطى. وقلما تتحدى خبيراً (أو هاوياً) في تحليل الشيفرة في الوقت الذي بدأت فيه هيربرت يارولي مهنته كمحلل للشيفرة، لكن اكتشاف أسلوب ذي نظام لحل جميع الشيفرات حتى هذه البسيطة يكون ذا نظرة عميقة في حل الشيفرة ذات القوة الأساسية بحيث لا تستطيع جميع التجديدات في صنع الرموز في القرون اللاحقة هزيمتها هزيمة كاملة. لقد خرجت الهرة من الحقيبة. لا يهم مهما كان صنع الشيفرة معقداً بحيث يمزج النص الأصلي ليخفيه، فإن شبحه يظهر على الدوام من خلال الشيفرة: فتكرار الحروف غير المتساوي صفة مميزة في جميع اللغات يترك آثاره الواضحة، ولن تختفي ابتسامة هرة شيشاير (1) أبداً.

لقد عرف صانعو المعاجم العرب بضع حقائق بدهية فيما يتعلق بالتشفير. فمنذ القرن الثامن عرف الخليل وهو من علماء اللغة من مدرسة البصرة أن الشكل النمطي الذي بدت به معظم الرسائل شكّل نقطة ضعف كبيرة يمكن استخدامها في حل الشيفرة. سمى محللو الشيفرات فيما بعد هذه الطريقة «الافتراض» – إجراء تخمين علمي لبعض الأحرف الرئيسة ومن ثم مشاهدة إن كانت هذه الأحرف المحددة تعطي نصاً قابلاً للقراءة في أماكن أخرى من الرسالة. وقال الخليل إنه حل رسالة يونانية مشفرة أرسلها له إمبراطور بيزانطة وذلك عن طريق افتراض أنها بدأت بعبارة «بسم الله»، تميل الرسالة العسكرية والديبلوماسية إلى استخدام عبارات نمطية، ويؤكد المرة تلو المرة على مبادئ رئيسية لسلامة الشيفرة ليستخدمها عاملو الشيفرة على مدى قرون عدة – ومن ثم تجاهلوها المرة تلو المرة مما أدى إلى سقوطهم – أولاً وهي الحاجة إلى تجنب استخدام عبارات مصنفة لديهم استخداماً ثانياً. وبمبدأ آخر لسلامة الشيفرة جاء مباشرة من مكتشفات العرب وهو كلما

طالت الرسالة، زادت الاحصاءات التي تقدمها إلى أولئك الذين سيعملون في حل الشيفرة حول تكرار الأحرف، وزادت سهولة حلها.

أعطى قدوم البرق في عام 1814 أهمية وإلحاحاً للاتجاهات المتنافسة في مجال تطوير الشيفرة الذي يتطور ببطء منذ عصر النهضة. فقد جعل البرق لأول مرة الاتصالات السريعة أمراً ممكناً، حتى وإن جعل الاتصالات أقل آمناً مما كانت. فالرسالة إن حملها مراسل قد يتم اعتراضها، لكن الرسالة البرقية كانت إعلاناً عاماً عملياً. كان عدد كبير من الناس متأكدين من رؤية أي رسالة برقية عندما تسلم للموظف الذي يقوم بإرسالها بواسطة الأسلاك، والأسلاك ذاتها يمكن اختراقها أيضاً من قبل شخص يمتلك مقداراً من تقنيات «اعرف كيف». خلال الحرب الأهلية الأمريكية أرسلت جيوش الاتحاد أكثر من ستة ملايين برقية، تم اعتراض عدد كبير منها (على الرغم من أنها لم يتم حلها أو تفكيكها من قبل القوات الانفصالية. لقد وضع هذا الحجم من المراسلات عبئاً غير مسبوق على عاتق جهاز الشيفرة، وكان من الواجب أن تكون الشيفرة بسيطة وسريعة لاستخدامها في الميدان، وإلا فإن الوقت الذي يمضي في ترميز الشيفرة وحلها لن يناسب السرعة الذي جعلها البرق أمراً مناسباً. ولكن يجب أن تكون آمنة تماماً تقاوم محللي الشيفرة حتى وإن كان من المحتمل أن يكون أمام العدو آلاف الرسائل المشفرة التي يجب معالجتها.

كانت معظم الخطط والطرق التي تعد لتواجه هذه المطالب المتناقضة عبارة عن تنوع فيما أصبح يعرف بشيفرات الأبجديات المتعددة. فبدلاً من استعمال بدائل أبجدية واحدة، أمكن استعمال سلاسل مختلفة من أبجديات الشيفرة التي تأتي بعد كل حرف من الرسالة كل منها بدوره. بعبارة أخرى، يمكن أن يرمز لحرف a بحرف x عندما يظهر كأول حرف في الرسالة؛ وعندما يظهر ثانية بعد عدد قليل من الحروف قد يرمزله بحرف G. إن طريقة كهذه تعود بالفعل إلى القرن الخامس عشر، وقد وُجدت لتُنسى ثم ليعاد ابتكارها في أواخر القرن التاسع عشر هي في الواقع جدول فيجنير.

ويتألف هذا من مخطط يحوي سلاسل من أبجديات شيفرة من ست وعشرين حرفاً، في كل منها ينتقل حرف واحد عن السلسلة السابقة. توضع أحرف «النص البسيط» في قمة المخطط؛ ومن الأعلى إلى الأسفل توضع الحروف «الرئيسة» التي تقرر أي حرف ترميز يجب استخدامه:

النص البسيط

الحرف الأساسي	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
A	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
B	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	a
C	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b
D	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c
E	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d
F	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e
G	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f
H	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g

وهكذا

وهكذا للقيام بتشفير النص البسيط «*p*» بالحرف الرئيسي «B»، وهو الحرف الموجود في العمود «*p*» والصف «B» وهو «Q». تحدد الحروف الرئيسة في الغالب بواسطة تذكر الكلمة أو العبارة المكتوبة فوق النص البسيط:

الحرف الرئيسي (المفتاح)	S W O R D F I S H S W O R D F I S H S W
النص البسيط	m y h o v e r c r a f t n e e d s o i l
النص المشفر	E U V F Y J Z U Y S B H E H J L K V A H

إن مزايا التشفير بالأبجديات المتعددة ظاهرة مباشرة. ففي هذا المثال، كان ترميز الحرف «*r*» بواسطة الحرف «Z» عند ظهوره أول مرة، وبواسطة الحرف «Y» عند ظهوره ثانية. والنص المشفر «H» يقوم مقام الحرف «*t*» في مكان، وفي مكان آخر «*l*». والمحاولة المباشرة لتحليل تكرار الحرف تنحرف بواسطة هذه الهويات المتعددة. في الشيفرة المبنية بناء جيداً من الأبجديات المتعددة، يظهر فيها كل حرف بتكرار متساو مع الأحرف الأخرى. بعبارة أخرى يصبح تكرار الحرف أكثر عشوائية. تتبع الشيفرة المصنوعة على أساس الأبجدية الواحدة توزعاً منحرفاً في اللغة البسيطة ذاتها ويتراوح ذلك من 12٪ بالنسبة إلى أي رمز في الشيفرة يقوم مقام

حرف «e»، إلى 0.3٪ بالنسبة للرمز الذي يقوم مقام «z». إن الشيفرة المثالية التي تعتمد الأبجديات المتعددة ذات توزع منبسط لتكرار الحروف؛ فكل رمزله فرصة واحدة من ست وعشرين فرصة، وحوالي 3.8٪ لظهورها في نص الشيفرة.

ميزة أخرى لهذه الطريقة هي السهولة النسبية في استعمالها وحتى إن اكتشفت طريقة التشفير للعدو، لا يستطيع قراءة أي رسائل معترضة دون الكلمة الأساسية – التي يمكن أن تتغير، شئنا أم أبينا، كل أسبوع أو كل يوم أو حينما تتطلب السلامة. وقد تبقى الكلمة الأساسية في الذاكرة ولا يوجد عليها أي دليل مكتوب يمكن افشاؤه. وأخيراً، تقدم شيفرات الأبجديات المتعددة جاهزية للتوليد بأجهزة ميكانيكية. واحدة من أقدم هذه الأجهزة آلة التشفير الأسطوانية التي جعلها توماس جيفرسون شهيرة، وفيها سلسلة من الأقراص، وكل من هذه الأقراص يطبع على أطرافه أبجدية غير منتظمة، ومركب على محور؛ تدور هذه الأقراص حتى تكون أحرف النص البسيط على نسق واحد، فيقرأ نص الشيفرة عندئذ من أي نسق.

حتى في أفضل شيفرات الأبجديات المتعددة لا يزال شبح النص البسيط ماثلاً تحتها. في عام 1935 أنتج سلومون كولباك ما يزال يعتبر حتى اليوم أنه التحليل الرياضي القاطع للشيفرة ذات الأبجديات المتعددة، وكان كولباك حينئذ أمضى خمس سنوات فقط في تحليل الشيفرات، ولكنه حصل على شهادة الدكتوراة في الإحصاء من جامعة جورج واشنطن في تلك الأثناء. ومن دراسته لسلسلة من الصفحات التي كتبها رئيسه وليام فريدمان، أوضح كولباك أنه يمكن معالجة أكثر شيفرات الأبجديات المتعددة تعقيداً بواسطة التحليل المتكرر – ما دام لدى المرء نصوص كافية ليعالجها.

كانت نظرة فريدمان الثاقبة، والتي وسعها كولباك، واحدة من تلك الومضات الذكية التي تميز الكتابة السرية من وقت لآخر. كان من المعروف منذ زمن طويل أن نقطة الضعف الأساسية للتشفير بالأبجديات المتعددة تكمن في نقطة ما عندما يكرر الحرف الأساسي نفسه. إن كان الأساس بطول عشرة أحرف،

فيكون الحرف الأول، والحادي عشر، والواحد والعشرين، والواحد والثلاثين (وهكذا) من أحرف الرسالة يشفرون من الأبجدية ذاتها. ويكون ذلك أيضاً بالنسبة للحرف الثاني، والثاني عشر، والثاني والعشرين والثاني والثلاثين الذين يشفرون من الأبجدية الثابتة – وهكذا دواليك. ومن هذا، إن أي شيفرة تعتمد الأبجديات المتعددة ذات أساس مؤلف من العدد «*n*» يمكن من حيث المبدأ تخفيض المشكلة إلى تفكيك عدد «*n*» من شيفرات بديلة مؤلفة من أبجدية واحدة.

إن المشكلة في أن الرسالة الواحدة يجب أن تكون طويلة لتعطي عدداً من الأحرف يكفي لتعداد التكرار تعدداً صحيحاً لكلٍ من شيفرات الأبجدية الواحدة التي تؤلفها. للحصول على إحصاء جيد، نحتاج إلى نص من خمسين حرفاً. فكلما طال الأساس، زاد عدد الأبجديات المنفصلة للشيفرة، وصغر حجم نص الشيفرة لكل منها، وفي العادة لا يكون لدى محلل الشيفرة طريقة لمعرفة حتى طول الأساس في البداية. وما يحتاجه فعلاً هو تكديس عدد كبير من الرسائل المنفصلة والتي شُفرت بالأساس نفسه، ومن ثم وضعها فوق بعضها بعضاً بحيث تكون الأحرف في العمود الواحد قد شفرت بالحرف الأساسي ذاته والنص المشفر في كل عمود يمثل مشكلة واحدة من استبدال أبجدية واحدة.

ولكن صف رسائل متعددة بهذا الشكل عملية أسهل قولاً مما هي من حيث العمل. فما من عامل شفرة مهما كان غبياً يبدأ كل رسالة بأول حرف من النص الأساسي. إنه يتبع طريقة ما للانتقال بالنص الأساسي في كل شيفرة؛ تبدأ بعض الرسائل النص الأساسي كما يلي Swordfish، وثم ينتقل ليصبح Wordfishs ومن ثم Ordfishsw وهكذا.

لكن فريدمان أدرك أنه دون حل جزء صغير من الشيفرة، ودون معرفة طول النص الأساسي، ودون معرفة النظام المستعمل لانتقال النص الأساسي من رسالة إلى أخرى، فإنه من الممكن أيضاً وضع الرسائل في صف بحيث يكون لكل حرف في عمود من الأحرف نفسها عند تشفيرها. يتضمن هذا المبدأ ما يسمى بجدول المصادفات، ويكمن الذكاء في معرفة الطريقة التي تشبه الشبح الذي يكمن

خلف عدم استواء اللغة الذي لا يمكن أن يختفي تماماً. و«الصدفة» هنا تعني كم عدد المرات التي يأتي بها نصان مشفران يوضعان فوق بعضهما سيكون فيهما الحرف نفسه في العمود نفسه. إذا قورن خطان عشوائيان من شيفرة الأبجديات المتعددة بهذه الطريقة، فسوف تكون هذه الصدف متواجدة بفعل قوانين مباشرة للفرصة (أو الصدفة). ففي أي نقطة من رسالة ما، يكون للحرف «A» فرصة واحدة من 26 فرصة للظهور؛ وفرص ظهور الحرف «A» في النقطة نفسها في الرسالة الثانية هي أيضاً 1 من 26؛ فهكذا تكون فرصة ظهور «A» في كلتا الرسالتين في النقطة ذاتها في الوقت نفسه هي 1/26×1/26 وهذا يساوي 0.15٪. إذن إن فرصة أي صدفة لظهور (A وA، أو B وB، أو C وC وهكذا) ستحدث في نقطة مفترضة هي أكبر بست وعشرين مرة: 1/26×1/26×26، أو 3.8٪.

ولكن عندما يوضع صفان من نص مشفر استخدم في تشفيرهما النص الأساسي نفسه صفاً صحيحاً، فسوف يحدث شيء مختلف اختلافاً دراسياً. في هذه الحالة كل زوج عمودي تم تشفيرهما بالبديل من أبجدية واحدة ذاتها. في أي عمود سيظهر الحرف e في الرسالة الواحدة نفسه في النص المشفر كحرف e في الرسالة الثانية. وهذه الأحرف ذات التكرار الكبير ستحرف شواذ الصدفة الحادثة. إن أي حرف من النص المشفر يقوم مقام الحرف e في أي عمود ذو نسبة تكرار هي 12٪، وإن فرص حدوثه في الرسالتين في آن معاً هي العشوائية الصافية. يقوم حرف الشيفرة في كل عمود مقام الحرف ذي التكرار النادر (مثل Z) وسيكون ذا فرصة أقل للظهور في كلتا الرسالتين (فنسبة تكرار Z أقل من 0.001٪). لكن الحروف ذات التكرار العالي تحرف الشواذ التي تؤثر في نتيجة الحروف ذات التكرار المنخفض. عند جمع الشواذ للفرص المحتملة الست والعشرين، يكون مجموع فرص الصدف الحادثة بين رسالتين بالانكليزية موضوعتين بصورة صحيحة حوالي 6.7٪، أي ما يقرب من ضعف معدل الصدف للنص المشفر والمصفوف عشوائياً.

وهكذا يصبح في رسالتين مسألة رياضية آلية بحتة. يوضع النصان بوضع تجريبي، ويجري تعداد الصدف، ويقسم المجموع على عدد الأحرف. إن كان

اصطفاف الرسائل صحيحاً ستكون النتيجة حوالي 6.7٪؛ وإن صفها غير صحيح ستكون النتيجة أقرب إلى 3.8٪ ، ويمكن نقل الرسالتين بمقدار حرف واحد بالنسبة لبعضهما ويجرى الفحص مرة أخرى.

وضع الرسائل على خط مستقيم – أو «بالعمق – فوق بعضهما» – هو أسلوب لتحليل الكتابة السرية ذو قوة كبيرة، وقد يثبت أنه المفتاح في تفكيك بعض أصعب الشيفرات التي واجهت مفككي الشيفرة في أمريكا وبريطانيا خلال الحرب العالمية الثانية. أي، جميعها ما عدا الأصعب منها جميعاً ألا وهي: آلة التشفير «اللغز Enigma».

--- --- ---

كانت بولونيا ، بديكتاتوريتها العسكرية وبعداوتها المتصلبة تجاه روسيا وباضطهادها للأقلية اليهودية ، شاركت حكام ألمانيا بأشياء كثيرة في الثلاثينيات، ففي عام 1926 استولى المارشال جوزيف بيلسودسكي على السلطة في وارصو بانقلاب عسكري، وجرد البلاد من النظام الديمقراطي البرلماني الوليد ، وبعد أقل من سنة على تسلم هتلر السلطة في ألمانيا ، وقع مع الحكومة النازية اتفاقية عدم اعتداء مدتها عشر سنوات، وعندما ضم هتلر «سوديتين» من تشيكوسلوفاكيا في 1938 ، شاركت بولونيا في عملية السلب واقتطعت مقاطعة حدودية «تيشين» من تشيكوسلوفاكيا. قال تشرشل عن عملية السلب البولونية «نصر بالعصيان والدمار، وحقارة وعار في الانتصار. أشجع الشجعان يقودهم أكثر الأشرار شراً».

لقد كانت روسيا المضطهد التاريخي لبولونيا ، ولما تلبدت غيوم الحرب الأكيدة في الغرب في عام 1939 نفضت بولونيا أي محادثات بشأن حلف دفاعي يلمح إلى القضية المشتركة مع الاتحاد السوفياتي. ولاحظ المؤرخ (جيمس ستوكسبيري) كان البولونيون يكرهون الروس أكثر مما يخشون الألمان. ولكن بولونيا لم تكن غافلة عن أطماع ألمانيا في الشرق ولا عن الحقيقة البسيطة التي تتمثل في حدودها التي لا يمكن الدفاع عنها. كان تاريخ بولونيا تقطيع أوصالها

مراراً وتكراراً من قبل جيرانها الأقوياء من جميع الاتجاهات؛ وسرى القول بأن بولونيا ليس لها تاريخ مطلقاً، بل جيران فقط. في أواخر القرن الثامن عشر اشتركت ألمانيا والنمسا وروسيا في تقطيع أوصال بولونيا، وبقيت بولونيا قرناً كاملاً غير موجودة كدولة ذات سيادة. أعادت معاهدة فيرساي بولونيا إلى الوجود لكن الحكومات الألمانية منذ عام 1919 لم تخف رغبتها في «مراجعة» الحدود الغربية من بولونيا.

قامت ألمانيا في عام 1925 بالتوقيع على معاهدة لوكارنو التي تحترم حدود ما بعد الحرب مع كل من فرنسا وبلجيكا لكنها رفضت التفكير في معاهدة لوكارنوا الشرقية التي ستفعل الشيء ذاته بالنسبة لوبولنيا والنقطة المؤلمة الأخرى هي الممر الذي أعطي إلى بولونيا ليصلها ببحر البلطيق عند ميناء دانزيغ الذي وضع تحت سيطرة دولية؛ ويقطع أيضاً بروسيا الشرقية عن أرض الأجداد. فقد كانت بروسيا هي موطن الأجداد من العسكرية الألمانية؛ احتل الفرسان التوتون البلاد منذ العصور الوسطى ولا تزال موطن السلالات القوية المعروفة باسم جنكرز التي سيطرت على هيئة ضباط ألمانيا. بالنسبة لأمثال هؤلاء الرجال، كان الممر إهانة شخصية لكرامتهم. ولكن في الحقيقة لم تكن حدود بولونيا وحدها، بل بولونيا ذاتها لا يحتملها الألمان. ففي تاريخ مبكر يعود إلى 1926 كان الجنرال هانزفون سيكت، قائد الجيش الألماني، يلح على حكومته بأن وجود بولونيا ذاته «لا يتعايش مع الشروط الأساسية لحياة ألمانيا». وكان استنتاجه: «على بولونيا أن تذهب وسوف تذهب». لم تكن مخططات هتلر بالنسبة لبولونيا طمعاً محموماً للنازية، لكنها كانت أعراضاً تاريخية للقومية الألمانية.

لدى بولونيا مليون رجل تحت السلاح، منهم 12 فرقة فرسان، وهذه القوة جبارة نظرياً، وكذلك من وجهة نظر الجنرالات البولونيين الرومانسيين الذين كانوا مقتنعين بمبدأ يقول بالشجاعة والخيول الكافية يمكن فعل أي شيء. ولكن كان هناك عدد صغير من الضباط الذي يتمتعون ببعد النظر تمكنوا من الوصول إلى حقيقة غافلة عن نظرائهم البريطانيين والأمريكيين. إن المخابرات ولا

سيما فك الشيفرة يعبر عنها في عصر متأخر «بالعبارات العسكرية» بأنها «مضاعفة للقوة». فمعرفة كيف يطور العدو المحتمل نفسه وينشر قواته العسكرية يمكن أن تجعل من القوات المحدودة قوات ذات فعالية أكبر، وهي ليست بسلاح يمكن لدولة وليدة حديثاً وضعيفة مثل بولونيا أن تهمله. وهكذا فمنذ البداية وضعت المخابرات البولونية عيناً ثابتة على القوات المسلحة الألمانية. وكان من الواضح أن بولونيا في مركز جيد لالتقاط الإشارات العسكرية والبحرية الألمانية المرسلة بالراديو، وفي أوائل 1926 كان مكتب الشيفرة – وهو المكتب الثاني (المخابرات) للقيادة العامة للجيش في وارصو – ينتج سيلاً ثابتاً من الرسائل المفككة من الرسائل الألمانية التي تجمع عن طريق محطات التنصت.

ولكن فجأة توقف هذا النجاح تماماً. ففي شهر شباط من عام 1926 أصبحت رسائل البحرية الألمانية غير مقروءة؛ وفي تموز 1928 لحقت بها رسائل الجيش. شك البولونيون بأن الرموز الألمانية الجديدة للتشفير إنما تولدها آلة، لكنهم كانوا في طريق مسدود.

لقد دفع اختراع الراديو فكرة استخدام آلة لصنع الشيفرة إلى الأمام. فقد فتح عرض شركة ماركوني للبرقية العابرة للمحيط الأطلسي بالراديو في 1901 الطريق لقفزة إلى الأمام في حجم وسرعة حركة الرسائل العسكرية والبحرية والديبلوماسية وهذا تقدم عظيم على البرق كما كان تقدم البرق عظيماً على الرسائل المكتوبة. وحتى الشيفرات المتطورة التي تستخدم أبجديات متعددة وعبارات أساسية طويلة وتغيير المفتاح (الأساس) تغييراً متعدداً انهارت تحت ثقل حركة انتقال الرسائل التي يتوقع أن تقوم بنقلها الآن. إن كان البرق كوسيلة اتصالات قد أصبح إعلاناً عاماً، فإن الاتصالات بواسطة الراديو شيء يقترب من أن يكون مشهداً عاماً. فاستطاع كل الناس الاستماع وقد فعلوا كما أثبتت الحرب العالمية الأولى.

كان ضعف الشيفرات اليدوية في هذه الظروف ذات طبقتين. الأولى، إن المفتاح (الأساس) يكرر نفسه بشكل ضروري وهذا سمح للرسائل بأن توضع في العمق (فوق بعضها). والثانية، حتى عندما يتغيير المفتاح (الأساس) فإن التشفير يقوم على

مجموعة محدودة من الاحتمالات. فمثلاً يستخدم جدول فيغنر ستاً وعشرين أبجدية شيفرة مختلفة فقط. وزيادة هذه المجموعة قد تخلق نظاماً يمكن أن يصبح صعب الاستعمال في هذا المجال. وقد يتطلب إجراءات أساسية معقدة للحفاظ على المسار ولبيان أي أبجدية شيفرة تخدم ولأية رسالة؛ قد يتطلب ذلك مخططات متقدمة للتشفير وفك التشفير.

حاولت آلات الشيفرة المتنوعة التي اخترعت ما بين 1910 و1930 أن تتغلب على هذه العوائق وذلك باستخدام جهاز ميكانيكي يولّد آلياً المفتاح (الأساس) لهذه الأطوال الغريبة التي يمكن بواسطتها إرسال مئات بل آلاف من الرسائل دون استخدام امتداد المفتاح نفسه مرتين. وهكذا لا يمكن وضع الرسائل في العمق. وفضلاً عن ذلك، لم تكن الآلات محددة بست وعشرين أبجدية للشيفرة؛ وعدد تتابع المفاتيح المختلفة الذي ينتج عن التسلسل الميكانيكي مع ملايين الأبجديات في التبدلات المتنوعة التي تصل بسهولة إلى ملايين الملايين في أبسط جهاز من أجهزة الشيفرة الأولى هذه. إن تغيير المفاتيح سهل سهولة إعادة وضع مفتاح، أو تبديل قابس، والنتيجة درامية مثل اختراع شيفرة جديدة تماماً. وأفضل شيء هو أن هذه الآلات قد ألغت الكثير من التعب في ترميز الرسائل وفكها، فكان نص الرسالة يطبع على مجموعة مفاتيح آلة كاتبة، ويظهر النص المشفر آلياً، والعكس صحيح أيضاً.

لم يكن للآلة المشفرة المعروفة باسم «اللغز Enigma» بداية واعدة، فقد صنع المهندس واسمه آرثر شيربيوس الاسم وحقوق الملكية ولكن هذين الشيئين كانا بمثابة قبلة الموت للشركة التي حصلت على الحقوق. عرض نموذج مبكر من الآلة Enigma في مجمع اتحاد البريد العالمي في 1923 في بيرن، سويسرا، حيث قدمت إلى رجال الأعمال على أنها طريقة لحفظ محتويات برقياتهم سرية عن أعين المنافسين. كانت الآلة عملاً رائعاً من الناحية الميكانيكية والرياضية، أما من الناحية التجارية فقد كانت فشلاً.

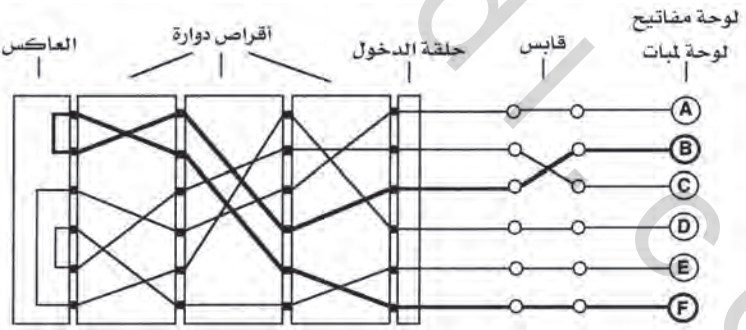
وكما كانت بعض آلات تشفير أخرى مسجلة في كل من السويد والولايات المتحدة في الوقت نفسه تقريباً، كان جوهر تصميم شيربيوس سلسلة من أقراص دوارة تعمل على خلط أبجدية الشيفرة. لكل من هذه الأقراص الدوارة حلقة من ست وعشرين نقطة تماس كهربائي على كل وجه. وتحرك لوحة مفاتيح آلة كاتبة عدداً من المفاتيح الكهربائية التي تبدأ عملية التشفير. بالضغط على الحرف A يغلق أحد هذه المفاتيح، فيصل تيار كهربائي إلى واحدة من نقاط التماس الكهربائية الست والعشرين على حلقة ثابتة ومجاورة لست وعشرين نقطة تماس على الوجه الأيمن من القرص الدوار اليميني. في داخل كل قرص دوار عدد كبير من الأسلاك تصل الوجه الأيمن بالوجه الأيسر بصيغة عشوائية. فيمكن مثلاً أن توصل النقطة 1 من الوجه اليمين بالأسلاك مع النقطة 22 على الوجه الأيسر؛ وكذلك يمكن وصل النقطة 2 بالأسلاك مع النقطة 5؛ والنقطة 3 مع النقطة 6 وهكذا. وعندما يصل التيار الكهربائي إلى الوجه الأيسر من القرص الدوار، فإنه يتدفق إلى نقاط التماس على الوجه الأيمن للقرص الدوار المجاور في الوسط، حيث تحدث عملية خلط أخرى. ويُدخل الناتج من القرص الدوار المتوسط في القرص الدوار الأيسر الأخير.

والقسم الذكي في هذا التصميم هو ما يحدث بعد ذلك. بعد خروج التيار من الوجه الأيسر للقرص الدوار الثالث يدخل «عاكساً»: وهو قرص بنصف العرض وفيه نقاط تماس على وجهه الأيمن فقط. والأسلاك الداخلية في العاكس تصل ما بين نقاط التماس على الوجه اليميني، الواحدة بالأخرى فتكون أزواجاً. وهكذا، عندما يصل التيار إلى نهاية الخط ينعكس عائداً إلى القرص الدوار الأيسر، ولكنه الآن في نقطة تماس مختلفة على وجهه الأيسر. ثم ينتقل التيار عبر الأقراص الدوارة الثلاث مرة أخرى، وهذه المرة من اليسار إلى اليمين ويقوم بعملية خلط أخرى. وعندما يصل التيار إلى الوجه الأيمن للقرص الدوار الأيمن، فإنه يمر مرة أخرى من خلال نقاط التماس لحلقة الدخول الثابتة ومن هنا ينتقل بالأسلاك إلى

واحدة من ست وعشرين نقطة إضاءة، وكل نقطة من هذه النقاط تحمل حرفاً من أحرف الأبجدية، يبين هذا الحرف حرف التشفير الذي ضغط على مفتاحه.

للعاكس ميزة تؤكد أن الحرف لا يمكن تشفيره بذاته. فالحرف A لا يمكن أن يقوم مكان A. إضافة إلى هذا، يضمن العاكس أنه بالنسبة لوضع الأقراص الدوارة الثلاث، تربط نقاط التماس على الحلقة الثابتة بشكل أزواج، كل اثنين معاً. فالضغط على الحرف A يضيء الحرف E، والضغط على الحرف E يضيء الحرف A. وكان هذا تقدماً كبيراً من الناحية العملية لأن ذلك يعني أن الآلة نفسها تركب بالطريقة ذاتها وتستخدم في العمليتين: تشفير الرسالة وفكها.

إن الآلة Enigma، مثلها مثل جميع الآلات الدوارة، قد صممت لتغير الخلط لكل حرف على التوالي في النص الذي يطبع. ففي كل مرة يضغط على مفتاح فأول ما يحدث هو أن يتقدم القرص الدوار اليميني وضعاً واحداً، أي 1 من 26 من الدورة، وبذلك تنتقل نقاط التماس فيه نقلة واحدة. نظام من ثلم ولسينات يجعل القرص الدوار المتوسط ينتقل إلى وضعه التالي بعدما يكمل القرص الأيمن دورة كاملة.



منظر مبسط لآلة انيغما Enigma يري ستة أحرف فقط. عندما يضغط على حرف ما يتدفق تيار من خلال نقاط تماس فيسبب إضاءة النقطة المقابلة. ويبين الخط العريض الغامق مسار هذا التوصيل بين الحرفين B وFg. عندما يضغط أي من المفتاحين تتحرك الأقراص الدوارة إلى وضع جديد وتقوم بخلط جديد

وعندما يكمل الدوار المتوسط دورة كاملة، يتقدم القرص الدوار الأيسر موضعاً واحداً. في كل مرة يتقدم قرص دوار واحد أو قرصان، ويتغير الوصل فيما بينهما، وبذلك يسير التيار في ممر جديد من خلال الخلاطات. كل حرف من رسالة يتم تشفيره من أبجدية تشفير مختلفة. وعندما تكمل الأقراص الثلاثة دورةكاملة يعود المفتاح فيكرر نفسه. وهذا يعني أنه يمكن طبع 17000 حرف دون استعمال طول أساسي (مفتاح) مرة أخرى.

يوضع على محيط كل قرص دوار في آلة اينغما Eniga وعلى حلقة متحركة أرقام من 1 إلى 26 أو أحرف من الحرف A إلى الحرف Z؛ ويمكن بدء الرسالة من أي نقطة في الدائرة الرئيسية (المفتاح) وذلك بتدوير الأقراص الثلاثة في الآلة إلى الوضع المطلوب. وباستخدام قائمة مبرمجة مسبقاً أو مؤشر مرسل في الرسالة نفسها، يضع المرسل والمستقبل الأقراص الدوارة بحيث يظهر مؤشر الحرف الثلاثة المختارة (AZG أو YSD أو أي شيء آخر) من نافذة في أعلى لوحة الآلة. وما دامت نقاط البداية هذه تبتعد جيداً من رسالة إلى أخرى، يتم تشفير كل رسالة بقطعة فردية تماماً من الأساس (المفتاح). ويستحيل وضع الرسائل في العمق مطلقاً.

لزيادة عدد توالي الأسس (المفاتيح) المختلفة والمتوافرة، فقد وضع في تصميم الآلة مصادر تبديل إضافية. ويمكن إخراج الأقراص الدوارة، وكل منها يحوي أسلاكاً داخلية مختلفة، من فتحاتها ويعاد إدخالها في نظام مختلف فمن اليسار إلى اليمين. وهذا يوجد ستة تغييرات: فيمكن وضع أي من الأقراص الدوارة في الفتحة اليسرى، وبذلك يترك خياران للفتحة الوسطى؛ فأي قرص يكون في الجهة اليسرى ويدخل في الفتحة اليمنى ينتج $3 \times 2 \times 1 = 6$ مجموعات مختلفة من الأقراص الدوارة من اليسار إلى اليمين (أو أنظمة الدولاب كما سمي فيما بعد من قبل محللي الشيفرة المتحدين). ولصنع مزيد من التغيرات يمكن إضافة أقراص دوارة إضافية وتبديلها بالنسبة لواحد أو أكثر من الأقراص الثلاثة. وللاختيار من بين خمسة أقراص يكون لدينا $5 \times 4 \times 3 = 60$ نظام محتمل من أنظمة الدولاب.

إضافة إلى ذلك يمكن نقل الظفر الموجود على كل قرص لتشغيل آلية الدوران إلى وضع جديد. كان الظفر موضوعاً على الحلقة المتحركة التي يوجد عليها الأحرف من A إلى Z؛ فبعد تحرير الملقط يمكن أن تدور الحلقة بشكل مستقلٍ عن القرص الدوار في الداخل، مثل انزلاق إطار مطاطي على الدولاب. وعند إعادة وضع الحلقات التي نقلت النقطة خلال دوران كل قرص دوار ذي أسلاك وعندها يتقدم القرص الموجود إلى يسارها، وهذا يكسر كل توالي للأساس (المفتاح) إلى 26 × 26 أو 676 تجمع ممكن. والقدرة على تغير وضع الحلقات ذات ميزة إضافية في إخفاء وضع البداية الحقيقي للأقراص الدوارة ذات الأسلاك بالنسبة لأي مؤشر؛ وبذلك يكون إخبار المتلقي بأن يضع الأقراص الدوارة في وضع البداية AFG معلومات غير كافية ليبدأ بفك الشيفرة فكاً ناجحاً إلا إذا كان يعرف أيضاً كيف تم وضع الحلقات بالنسبة للأقراص الدوارة ذات الأسلاك – ويوجد 26 × 26 × 26 طريقة ممكنة لفعل ذلك.

وأخيراً، في النماذج المتأخرة من الآلة انيغما Enigma أضافت سلسلة من القوابس طبقة أخرى للخلط، وهي التي ولّدت بلايين التغييرات الإضافية في توالي المفاتيح (الأساس). وعوضاً عن وصل لوحة المفاتيح واللمبات مباشرة مع حلقة الدخول الثابتة التي تلامس الوجه الأيمن للقرص الدوار الأيمن، تضع آلات إنيغما ذات القوابس لوحة ذات ستة وعشرين زوجاً من الروافع الصغيرة. كانت الكابلات ذات القوابس، مثل الكابلات في مقاسم الهواتف القديمة، تصل بين حروف مختارة. فعند إدخال قابس موجود في طرف الشريط في قابس الحرف F والطرف الآخر في قابس الحرف W، فإن الحرفين يتبادلان الهوية في أي شيفرة بديلة تولدها الأقراص الدوارة. في عشرة كابلات، يحتمل وجود 150 مليون مليون تغيير.

إذا لم تقدم هذه الآلة أماناً كافياً فمن الصعب تخيل ما يمكن أن يقدمه. حتى وإن وقعت الآلة بأيدي الأعداء، فإنها لن تعطي محلل الشيفرة أي شيء تقريباً ليتابع عمله. إن العدد الفريد لتوالي المفاتيح (الأسس) التي تستطيع الآلة توليده، والسهولة التي يمكن تغيير هذه المفاتيح كل يوم أو أسرع من ذلك، وطول كل مفتاح يمنع رسالتين من التشفير بطول المفتاح نفسه – هذه الملامح جميعاً تجعل الأدوات الرياضية التقليدية لتحليل الشيفرات عقيمة.

إذا لم تتأثر الأعمال التي تقلق بشأن أسرارها التجارية بكل ذلك، فقد تأثر زبون بذلك أخيراً. بعد تألمهم من الإلهامات البريطانية في العشرينات ونجاحهم في قراءة الشيفرة خلال الحرب العالمية، تمسك الجيش الألماني والبحرية الألمانية بالشيفرات المصنوعة بوساطة آلة كطريقة للتأكد من أن الإخفاقات مثل ماغدبيرغ لن تحدث مرة ثانية. عندما بدأ مكتب سيفروف يلتقط رسائل ألمانية لا يمكن فكها في أواخر العشرينات، كانت فكرتهم الأولى أنها رسائل غير ذات معنى تطلق في الهواء لتخدع أي محلل للشيفرة يحتمل أنه يقوم بالتنصت. كان النص عشوائياً تماماً؛ ولا يحمل شبح تواتر الأحرف المنحرف بأن الشيفرة الحقيقية تفشيها دائماً. وعندما أصبحت حركة الرسائل أكثر عمومية وأخيراً استبدلت كل الشيفرات الأخرى للجيش الألماني والبحرية الألمانية، أدرك محللو الشيفرة البولونيون ضد أي شيء يعملون.

مثلما كانت جميع مكاتب الشيفرة في العالم، كان البولونيون مدركين لآلة إنيغما نتيجة لفشل تسويقها تجارياً. في عام 1928 حصل البولونيون على تأكيد مباشر على اهتمام الألمان بالآلة إنيغما. وصل طرد مرسل من ألمانيا إلى دائرة جمارك وارصو وذلك لتفتيشه تفتيشاً عادياً. وعلى الفور وصل احتجاج من ألمانيا يقول إن الطرد قد أُرسل خطأً ويجب إعادته حالاً غير مفتوح. وكان هذا طبعاً كافياً ليثير فضول أي شخص، فوصل فنيون من المكتب الثاني لإلقاء نظرة على الطرد. وتبين أنه يتحوي على آلة تجارية «إنيغما». وقام مكتب سيفرو باستخدام عنوان مستعار وطلب آلة له من الصانع الألماني. ولكن عندما قام محللو الشيفرة البولونيون بتجربتها على رسائل معترضة، أنتجت كلاماً غير مفهوم. لكن ذلك لم يكن مدهشاً لأنها ليست النسخة العسكرية من الآلة، فقد أجرى الألمان تعديلاً على الأسلاك الداخلية في الأقراص الدوارة.

على الرغم من أن السرية النهائية لشيفرة الآلة انغيما لم تعتمد على الاحتفاظ بأشكال الأسلاك تلك، فإنها بالتأكيد أسهمت بإضافة مصدر آخر للصعوبة بالنسبة لمن يحاول أن يفك شيفرة من البداية. كان عدد الطرق المختلفة التي يمكن

بواسطتها توزيع وربط الأسلاك داخل الأقراص الدوارة حوالي 8010 أي العدد واحد مضاف إليه ثمانون صفراً. يصعب فهم مثل هذا العدد بالعبارات اليومية. فإذا وضع مليون مليون حاسب على كل كوكب من مليون مليون كوكب في كل مجرة من مليون مليون مجرة مليون مليون سنة يحاول أن يوجد كل تجمع محتمل لأسلاك ثلاثة أقراص في آلة إنيغما فإن ذلك يستغرق واحد على مليون من واحد على مليون من الثانية لاختبار كل تجمع، ولا يزال هناك أقل من فرصة في المليون مليون لإيجاد تجمع صحيح في ذلك الوقت.

عندما واجه البولونيون هذه الأبعاد الرهيبة قرروا أنه حان الوقت الذي يجب عليهم فيه أن يستعينوا بعلماء الرياضيات. وفي عمل يدل على بعد النظر ولا مثيل له في تلك الأوقات – وبالنسبة للبولونيين لم يكن لديهم أمل في أن ذلك سيؤدي إلى نتائج سريعة – وصل ضابطان من المكتب الثاني إلى جامعة بوزنان في كانون الثاني 1929 ليشرحا لعشرين طالب رياضيات من السنة الثالثة والرابعة بأن أساتذتهم قد اختاروهم ليحضروا دورة خاصة في علم الشيفرة. وأن هذا الصف يعقد مرتين بالأسبوع؛ وبأنهم سيداومون على دروسهم المعتادة في صفوفهم، وأن مجرد وجود صف علم الشيفرة يجب أن يبقى بالغ السرية.

لقد اختيرت جامعة بوزنان لهذه التجربة ليس بسبب الشهرة التي يتمتع بها معهد الرياضيات فيها فقط، بل وبسبب موقعها أيضاً. فكانت بوزنان في الجزء الغربي من البلاد، وكان هذا الجزء تحت سيطرة الألمان حتى عام 1919، وقد درس جميع طلابها تقريباً في سنوات شبابهم في مدارس تدرس باللغة الألمانية. وفي منعطف تاريخي مناسب انتقل معهد الرياضيات في بوزنان إلى قلعة تشبه قلعة الفرسان التوتون Teutonic Knights وقد بناها القيصر ويلهلهم الثاني في نهاية القرن كسكن رسمي لولي عهد ألمانيا، كجزء من الجهد لجعل الأراضي البولونية ألمانية.

مع تقدم الدورة انسحب الطلاب الواحد تلو الآخر. وأخير بقي اثنان فقط من اصل عشرين فقد بقي هذان الاثنان: جيرسي روزيكي وهنريك زيغالسكي. وكان طالب ثالث، ماريان، بيجيفسكي، قد غادر بوزنان في آذار 1929 قبل إنهائه الدورة وذلك

ليسجل في برنامج جامعي في رياضيات التأمين والاحتمالات في غوتنجن في ألمانيا. لكنه (ريجيفسكي) أظهر خلال هذين الشهرين مهارة في استيعاب رياضيات تحليل الشيفرة، وقد استغرق بضع ساعات في فك رموز شيفرة ألمانية معقدة ذات تبديل مضاعف كان الأستاذ قد أعطاها للصف ليشتغلوا بها، ولما عاد ريجيفسكي إلى بوزنان في صيف 1930 ليشغل وظيفة مساعد أستاذ، علم أن روزياكي، وزيغالسكي لا يزالان طالبين ويعملان الآن لصالح الأركان العامة اثنتي عشرة ساعة أسبوعية في قبو بناء القيادة العسكرية في المنطقة، بجانب الجامعة تماماً في شارع سانت مارتن. . دعي ريجيفسكي سريعاً للانضمام إلى المجموعة. كانت الرسائل المعترضة تسلم من وارصو بواسطة ساع ومن محطة مراقبة في ضاحية قريبة من ضواحي بوزنان؛ وكان على هؤلاء الرياضيين أن يركزوا على حل مفاتيح الشيفرة الجديدة في مختلف الشيفرات الألمانية اليدوية عندما تتغير المفاتيح وأن يرسلوا الحلول إلى وارصو. وكان هؤلاء الثلاثة يسمون موقعهم مازحين «الغرفة السوداء». في أيلول 1932 تخرج زيغالسكي ورزياكي فأغلقت الأركان العامة مركز الشيفرة في بوزنان وأخذت الرجال الثلاثة إلى وارصو. في صبيحة أحد الأيام من شهر تشرين الأول ربما، استدعى الرائد ماكسمليليان سيزكي، وهو رئيس القسم الألماني في مكتب سيقروف، ريجيفسكي إلى مكتبه وسأله إن كان لديه بعض أوقات الفراغ الإضافية في المساء. وقال ريجيفسكي إن لديه ذلك. فقال سيزكي في هذه الحالة أرغب في مجيئك إلى هنا مساء أيضاً. ولكن لا تخبر زملاءك بذلك. كان على ريجيفسكي أن يأتي لمدة ساعتين يومياً بعد أن يذهب زملاؤه إلى بيوتهم. وكان ينتظره في ذلك اليوم مساءً ملفات المكتب سيفروف حول الآلة إنيغما. فقد حاول محللو الشيفرة العسكريون الذين يديرون المكتب أن يحلوا المشكلة وفشلوا بذلك، ولذلك أحالوا الأمر إلى عالم بالرياضيات يبلغ السابعة والعشرين من العمر، الذي كان عليه أن يدرس ما يستطيع فعله في وقت فراغه. وأما هم فكان من الواضح أنهم شعروا بأنهم ليس لديهم ما يخسرونه في هذه المحاولة، ومضت أربع سنوات من العمل ولم يتوصلوا إلى أي مكان.

كانت الشيفرة الآلية وليدة ثورة الاتصالات. وكذلك كانت أنواع الرموز المختلفة جداً التي ظهرت في المقدمة في سنوات ما بين الحربين. وكان من المعترف به

دائماً أن استخدام آلاف الرموز المختلفة لتقوم مقام الكلمات أو العبارات – وهذا هو تعريف الرمز تماماً – أكثر أماناً أصلاً من استخدام ستة وعشرين رمزاً مختلفاً لتقوم مقام حروف الأبجدية. بمجرد وزن الأعداد وقيمتها يكون الرمز البسيط أكثر صعوبة على التحليل من أي شيفرة من أبجدية واحدة. لكن الرموز تحتاج إلى كتب كبيرة يجري جمعها بعناء كبير، وثقيلة عند حملها وهي عرضة لأن تقع بين الأعداء. ومع أن للرموز صعوبات، فإنها في نهاية المطاف ليس اختراقها أصعب من اختراق الشيفرة العادية. إن الكلمات التي تؤلف اللغة تصاغ كما تصاغ الحرف التي تؤلف الكلمات، ولا أكثر. وإعادة بناء كتاب للرموز هو فن لغوي أكثر وتمرين رياضي أقل من تفكيك شيفرة، لكن عملية «فك الكتاب» عمل مستقيم تماماً. إن مجموعة الرموز التي تمثل كلمات أو عبارات مستعملة باستمرار («إلى» و«من» وأسماء الأمكنة والأشهر والسنين») تفضح نفسها بظهورها المتكرر في المكان نفسه في رسائل متعددة. فعندما تكتشف مجموعة الرموز لكلمة (stop)، توضع النصوص ضمن وحدات قواعدية يمكن إعرابها إعراباً سهلاً ويمكن تخمين المعاني، من قبل من يعرف قواعد ترتيب الكلمات والقواعد التي توجد تحت اللغة. والعادات الصافية لعاملين الرسائل في ترقيم الرسائل يمكن أن تكشف مجموعات الرموز التي تقوم مقام الأرقام؛ لو بدأت الرسائل المعترضة بما يلي:

الرسالة 1:	**ZOXIL**	**GEZOR**	**...**
الرسالة 2:	**ZOXIL**	**KUMQT**	**...**
الرسالة 3:	**ZOXIL**	**ORANG**	**...**
الرسالة 4:	**ARDVK**	**FABOL**	**...**

ليس من الصعب أن تخمن أن GEZOR هي «سبع»، وKUMQT هي «ثمانية»، وORANG هي «تسعة» وFABOL هي «صفر» والكلمتان ZOXIL وARDVK هما أرقام متتالية.

لا فرق في أن تمثل مجموعات الرموز بأحرف أو بأرقام في خطة المجابهة. لكن الرموز التي توضع فيها معان وتحدد بمجموعات رموز بترتيب أبجدي تعطي موطئ قدم آخر؛ فإن اكتشف أحدهم أن 52980 تعني «tunnel»، أو أن 52976 تعني

«tuna»، فإن 52978 يجب أن تكون كلمة تقع في الترتيب الأبجدي بين هاتين الكلمتين في هذا الجزء من الرمز (أو ما يسمى لأن الترميز وتحليل الرموز يمكن تنفيذهما من الكتاب نفسه).

لقد مال البحارة والديبلوماسيون إلى تفضيل الرموز على الشيفرات لأسباب عملية وعادية. وكان خوفهم من فقد كتب الرموز ووقوعها بأيد العدو أقل من خوف الجيش من ذلك؛ ولكن من أجل الاطمئنان كان من الأمور التقليدية أن تضع البحرية كتب الرموز بين صفحتين من الرصاص أو أن تطبعها بحبر ينحل بالماء وبذلك يمكن التخلص منها أو جعلها عديمة الفائدة إذا ما هددت بالأسر. انحصرت الرموز التي استعملتها بعد الحرب العالمية الأولى المصالح البحرية والديبلوماسية الرئيسية في العالم في جزئين من الرموز (سماها البريطانيون «الرموز المغطاة»)؛ كانت مجموعات الرموز توضع بترتيب غير أبجدي، ترتيب عشوائي، وهذا يعني أن من الضروري وجود كتابين منفصلين للرموز وذلك لعملية الترميز وعملية فك الرموز. يرتب كتاب الترميز المعاني ترتيباً أبجدياً، ويرتب كتاب فك الرموز مجموعات الرموز ترتيباً عددياً.

إن النوع البسيط من الرموز المشفرة الذي استخدمته البحرية الألمانية في الحرب العالمية الأولى، وفيه استخدم البديل من أبجدية واحدة لجميع مجموعات الرموز في كتاب الرموز بكامله، جرى استبداله على المستوى العالمي تقريباً في العشرينيات بأشكال أكثر تعقيداً من قبل مستخدمي الرموز في العالم. استخدم بعضهم صيغة تبديل معقدة لخلط هويات مجموعات الرموز. واستخدم آخرون التشفير بواسطة مفتاح من الإضافات يقدمه كتاب مفتاح منفصل أو كتاب إضافات تماماً كما تضمن آلة الإنيغما Enigma أن يخفى كل حرف بواسطة بديل سري، فإن استعمال الكتاب الإضافي في رمز مشفر يضمن أن كل مجموعة رموز تخفى بتشفير مختلف. احتوت الكتب الإضافية التي صدرت في العشرينيات بشكل طبيعي على عشرات الآلاف من الأرقام العشوائية. كانت عملية التشفير صعبة لكنها من الناحية النظرية فعالة جداً في ضمان الأمان. فيقوم عامل الشيفرة أولاً

بكتابة نص رسالته، ويخرج مجموعة الرموز المعادلة لكل كلمة أو عبارة. وبعد ذلك يكتب تحت كل مجموعة رموز سلسلة من الإضافات العشوائية مبتدئاً باختيار قسري لصفحة وسطر من الكتاب الإضافي. مثلاً:

النص البسيط: FROM KAA ESTIMATED TIME OF ARRIVAL 2130

(من كاغا الوقت المقدر للوصول 2130)

صندوق الأحرف الكبيرة

	from من	follows يتبع	Kage	stop نقطة	ETA زمن الوصول	2130	stop نقطة
نص الرمز	02923	48322	01905	38832	87039	11520	38832
الإضافات	02923	41338	00989	15861	28959	23693	18229
الرسالة مشفرة	23859	89650	01884	43693	05988	34113	46051

لتبسيط الأمر وللحفاظ على الأعداد الناتجة في النص المشفر جميعاً ذات خمس خانات، يتم الجمع في كل خانة على حدة، أي دون حمل من خانة إلى أخرى (مثلاً 9 + 4 = 3). وعندما ينتهي الموظف يكون لديه سلسلة من أرقام ذات خمس خانات، وتبدو هذه السلاسل بالنسبة لملاحظ عادي أو سواه عشوائية ولا معنى لها. مع أن مجموعة الرموز التي تعني (نقطة) تتكرر مرتين في هذه الرسالة، فإنها تظهر في الإشارة النهائية (43693) في مكان ما وتظهر (46051) في مكان آخر. وفي رسالة أخرى قد تظهر برقم مختلف تماماً.

يبدو هذا النظام غير قابل للاختراق حقاً. فما من صيغة من اللغة المختفية تظهر من خلالها ولا توجد طريقة للتخمين أي رقمين يجمعان ليعطيا مجموعة مشفرة. فأي مجموعة مشفرة تقوم مقام أي مجموعة رموز.

قد يبدو هذا النظام أنه الأطول بين المحاولات الطويلة للتخمين ولكن هناك طريقة مجربة وصحيحة لاستخلاص المعنى من رمز مشفر. إن شُفرت رسالتان بمجموعة واحدة من الإضافات، يمكن أن توضعا بالعمق – تصطف بحيث تكون المجموعات في كل عمود مشفرة باستعمال الإضافات ذاتها. وهنا يمكن أن تبدأ عملية بطيئة ومجهدة للاستخلاص وتبدأ بوضع مجموعات الرموز المجردة تحتها. إن المفتاح الرئيسي في هذه العملية معرفة أن زوجاً من مجموعات الرموز في عمود واحد

يحتفظان بصفة واحدة وهي أنه ما من تشفير يمكن أن يختفي. بغض النظر عن الإضافة المطبقة عليهما، إن الفرق العددي ثابت بين مجموعتين من الرموز مفترضتين في العمود نفسه. والبحث عن الفروق المتكررة بين أعمدة الرسائل في العمق هو الوتد الذي شق الرمز المشفر. فمثلاً، إذا عرفت ثلاث رسائل كالرسائل التالية بأنها وضعت في العمق بشكل صحيح:

	1	*2*	*3*	*4*	*5*
الرسالة 1:	0256	7892	8835	7923	0470
الرسالة 2:	0003	6286	5684	9901	5236
الرسالة 3:	8263	0017	5431	4329	5565

إن الفرق المتكرر في العمود (الرسالة 1 ناقص الرسالة 2 يساوي 0253) وفي العمود 3 (الرسالة 2 ناقص الرسالة 3 يساوي 0253) مؤشر قوي على أن مجموعتي الرموز ذاتهما تظهران في كل من المكانين. وهذا الاكتشاف بدوره يعطي مباشرة قيماً نسبية ليس لهاتين المجموعتين من الرموز المسؤولتين عن التكرار (الذي يمكننا من اعطاء قيم نسبية قسرياً للحرف A=0000 والحرف B=0235) وحسب، بل للإضافات أيضاً في هذين العمودين، وكذلك لأي مجموعة رموز أخرى تكون في هذه الأعمدة:

	1	*2*	*3*	*4*	*5*
الإضافات:	0003	....	5431	....	....
الرسالة 1:	0256	7892	8835	7923	0470
النص المرمز:	**0253(B)**	....	3404(C)	....	....
الرسالة 2:	0003	6286	5684	9901	5236
النص المرمز:	**0000(A)**	....	**0253(B)**	....	....
الرسالة 3:	8263	0017	5431	4329	5565
النص المرمز:	8260(D)	....	**0000(A)**	....	....

إن معاني مجموعات الرموز غير معروفة حتى الآن. ولكن عندما يكتشف مزيد من مجموعات الرموز والإضافات فإن العملية تكبر مثل كرة الثلج. ويعطي اكتشاف مجموعات الرموز 8260 و3404 أعلاه فروقاً ثنائية إضافية بين مجموعات الرموز المعروفة والمتزايدة التي يبحث عنها في الأعمدة الأخرى:

8260 – 0253 = 8017؛ 3404 – 2503 = 1901؛ 8260 – 3404 = 5244

(نذكر مرة أخرى أن عمليات الجمع والطرح تتم على أساس كل خانة على حدة، دون حمل). يظهر هذا الفرق الأخير في العمود الخامس (الرسالة 1 ناقص الرسالة الثانية)، ويفسح المجال لاكتشافات أخرى لتملأ الفراغات:

	1	*2*	*3*	*4*	*5*
الإضافات:	0003	....	5431	....	7076
الرسالة 1:	0256	7892	8835	7923	0470
النص المرمز:	0253	....	3404	....	**3404**
الرسالة 2:	0003	6286	5684	9901	5236
النص المرمز:	0000	....	0253	....	**8260**
الرسالة 3:	8263	0017	5431	4329	5565
النص المرمز:	8260	....	0000	....	8599

وهكذا تقرأ الرسالة الأولى: C .... C... B...؛ والرسالة الثانية: B...D ...A؛ والرسالة الثالثة: E ...A ...D. وعندما تعرف مجموعات الرموز للكلمات الشائعة وعلامات الترقيم (مثل النقطة)؛ يكون من الممكن تسريع العملية وذلك بطرح قيمتها من مجموعة الرموز في الرسالة لتوليد سلسلة من «الإضافات المفترضة»، ومن ثم طرح الإضافات من الرسائل لنحصل على مجموعات الرموز. وعندما يحصل هذا النجاح فإن «النقطة» احتمال يوضع في الرسالة في المكان الصحيح.

عندما يتم اكتشاف إضافات كافية تسمح بأن تجرد معظم الرسائل أو كلها وتكشف مجموعات الرموز وراءها، تستخدم عندئذ العملية اللغوية

لتفكيك الكتب ذاتها والتي تعمل على الرموز العادية غير المشفرة لتقوم بتحديد المعاني.

اللقطة هنا تحقق العمق للبداية بالعمل. فإن كانت الرسالة العادية عبارة عن خمس عشرة مجموعة وإن كان كتاب الإضافات يحتوي ثلاثين ألف مجموعة، كما كانت رموز البحرية اليابانية تحتوي، فإن الفرصة الاحصائية لالتقاط رسالتين عشوائيتين فيهما تراكب (مجموعة متكررة)، وحتى بمجموعة واحدة، هي فرصة خجولة تبلغ واحدة من ألف. لتقليل فرص التراكب هذه، يعطى عمال الشيفرة أوامر مشددة لأخذ نقاط بداية مختلفة لكل رسالة يقومون بإرسلها؛ وكانت البحرية اليابانية في بعض الأحيان تحدد لكل عامل شيفرة نقاط بداية مختلفة، موزعة بالتساوي في كتاب الإضافات، وتخبرهم بأن يعملوا بها بشكل مباشر، وبتلك الطريقة يضمنون أن الرسائل موزعة بالتساوي خلال الكتاب. وبذلك تقدم الرموز المشفرة جيداً فرصاً أقل لبناء تراكب للبدء به.

حتى وإن تراكبت الرسائل، كما قد يحدث في النهاية عندما تطول مدة استخدام كتاب الإضافات، لا توجد طريقة واضحة لاكتشاف الحقيقة. ولإعلام من تُوجه إليه الرسالة برقم الصفحة والسطر في كتاب الإضافات حيث بدأت التشفير، يضع عامل التشفير مجموعة رموز إضافية ضمن الرسالة، وتقوم هذه المجموعة بدور «المؤشر». وكان المؤشر عادة يستخدم نظاماً خاصاً لهذا الغرض فقط. إذا ما تم تفكيك ذلك المؤشر يكون عامل التفكيك قد أنجز عملاً حينئذ؛ يمكن أن توضع كل رسالة في كتاب الإضافات بصورة محددة. لكن المؤشر يخبأ ليبدو تماماً كأي مجموعة من مجموعات رموز الشيفرة في الرسالة المبثوثة؛ وتوضع في موضع مدروس مسبقاً من الرسالة ولا شيء يلفت الانتباه إليها ولا يذكر أنه شيء مغاير لما في نص الرسالة.

والطريقة الأخيرة التي يلجأ إليها محلل الشيفرة هي ما يعرف «بالقوة العمياء». وهي عبارة عن البحث عن إبرة في كومة من القش. أو بالأحرى، البحث عن القشة ذاتها في كومتين من القش. تبدو هذه الفكرة أولاً وكأنها انتصار للتفاؤل على

الحس العام. ولكنها بعد مرور الآلاف فوق الآلاف من الرسائل لابد وأن يحدث في النهاية أن لا تتطابق رسالتان فقط – وهذا يعني أن الرسالتين تحتويان على مجموعات رموز تم تشفيرها بواسطة الإضافات ذاتها – ولكنهما ستحتويان على مجموعة الرموز ذاتها والمشفرة بالإضافات نفسها. عندما يحدث هذا تكون مجموعة الرسائل الناتجة متشابهة. طبعاً من الممكن تماماً أن رسالتين تحتويان على مجموعات متشابهة لا تتطابق، مع مدى عام من الإضافات الرئيسة إطلاقاً؛ قد تجعل الصدفة وحدها من وقت لآخر مجموعة رموز ومجموعة إضافات تساوي مجموعة مختلفة تماماً من الرموز ومجموعة مختلفة تماماً من الإشارات. وما يبحث عنه محلل الشيفرة الذي يستخدم طريقة القوة العمياء هو إضافة أطول – زوج القش نفسه في كل من الكومتين. وهذه الإصابة المزدوجة يقل احتمال بروزها من مجرد الصدفة، وتزيد من احتمال إشارتها إلى تطابق حقيقي؛ على سبيل المثال:

الرسالة 1: 3419 2100 **7364** 5642 9468 **2316**

الرسالة 2: 7464 0924 **2316** 0072 7130 **7364**

هنا إشارة شبه أكيدة أن هاتين الرسالتين يمكن وضعهما بالعمق بشكل صحيح:

الرسالة 1: 3419 2100 **7364** 5642 9468 **2316**

الرسالة 2: 7464 0924 **2316** 0072 7130 **7364**

ولكن من المحتمل أن تدرس عشرات الآلاف من الرسائل لإيجاد عدد صغير من هذه الإصابات المزدوجة. ويمكن أن يتخذ صانع الشيفرة بعضاً من الإجراءات البسيطة ليقاوم مثل هذا البحث، وذلك بجعل القشة أصغر حجماً والكومة أكبر. كانت تعطى التعليمات دائماً إلى صانعي الشيفرة في البحرية اليابانية بأن يبدؤوا تشفير الرسالة من منتصف النص وبذلك يغيرون الأماكن العادية الممكنة للعناوين أو التواقيع بحيث لا تبدو واضحة. وأما الكلمات أو العبارات أو علامات الترقيم التي تستخدم دائماً والتي يمكن أن تولد الإصابات المزدوجة فكانت تعطى عدداً من المترادفات في كتاب الرموز حتى لا تظهر مجموعة رموز واحدة عدداً من المرات.

فاسم المكان (مثل مانيلا) يمكن أن يعطى خمسة أشكال من الرموز على الأقل: مثلاً يمكن أن يعطى مجموعة واحدة من الرموز تقوم مقام الكلمة كلها، أو أن يعطى ثلاث مجموعات رموز تقوم مقام المقاطع الثلاثة التي تؤلف الكلمة، أو أن تطعى بضع مجموعات من الرموز وتقوم بمقام الكلمات اليابانية التي تشكل جناساً مع الكلمة، أو أن تعطى ست مجموعات رموز يمثل كل منها الأحرف الأبجدية اللاتينية والتي تشكل تهجئة انكليزية، أو أن تعطى تحديداً مرمزاً خاصاً.

--- --- ---

في صباح يوم مشبع بالبخار في واشنطن من حزيران 1930، حضر وليام فريدمان إلى قبو بناء الأسلحة حيث أمضى «ثلاثة عاملين في الشيفرة» تابعين له الشهرين الأخيرين وهم يشقون طريقهم عبر نسخ مطبوعة بالفحم من آخر مسودة من دورة تحليل الشيفرة من تأليف فريدمان.

اتخذ نظرة غموض أقرب ما تكون إلى نظرة مسرحية، طلب فريدمان من كولباك ونسكوف ورووليت أن يتبعوه، ونزل الدرج ومشى في الممر إلى ما يشبه جناح مهجور من البناء، وهناك فتح بابين معدنيين كبيرين آمنين باجتماعهما وأقفال ذات مفاتيح. وكان القبو في الداخل مظلماً ولم يكن فيه نوافذ. وكما لو أنه يستمر في تمثيل مشهد من رواية قوطية رديئة، أشعل فريدمان عود ثقاب في الظلام فكشف بذلك الضوء الخافت غرفة يعلوها الغبار ويملؤها صفان من خزائن الملفات. وقال «أهلاً بكم أيها السادة» – ولم يبد أي منهم دهشة بهذا الأداء وما كانوا ليدهشوا لو قال لهم: «في قلعة داركيولا – في الأرشيف السري للغرفة السوداء الأمريكية».

خلال الأسابيع الأولى في عملهم قيل لهم إنهم سيطلق عليهم النار إن هم اقتربوا من خزائن الملفات في دائرتهم، والآن تُركوا مع أكثر أسرار الحكومة الأمريكية التي حفظت عن كثب، إنها سجلات ياردلي وغرفته السوداء، وقد حُزمت وغُلّفت ووضعت لدى وحدة الجيش MI – 8 عندما أغلق المكتب في السنة السابقة.

شرح لهم فريدمان ما سيعملون في خزائن الملفات ويرون ما يستطيعون التوصل إليه حول شيفرة اليابان الديبلوماسية. وكان هناك فرصة صغيرة لأن تبقى الشيفرة اليابانية التي فكها فريق ياردلي تستعمل حتى الآن، لكن أمل فريدمان الكبير هو أنه من المحتمل إن تغيرت الشيفرة أن يبقى استمرار كاف – في كتب الرموز أو في طريقة التشفير أو في الطريقة التي تستخدم فيها المؤشرات لتحديد المفتاح – وأن عمل الغرفة السوداء في الأنظمة السابقة سيقدم أفكاراً مفيدة تساعد في إلغاء استحالة الشواذ الطويلة ضد فك الرموز الجارية. كان الحفاظ على الاستمرار المبدأ الرئيسي لتحليل الكتابة السرية، فنادراً ما تتغير الرموز تغيراً كاملاً.

ولكن في حالة اليابان، تغيرت تغيراً كاملاً. طبعاً، أظهرت بعض شيفرات الدبلوماسية اليابانية ذات المستوى المتدني الخصائص العامة نفسها للشيفرات التي تمكنت الغرفة السوداء من حلها، وحقق فريق فريدمان بعض التقدم البطيء في تحليل الشيفرة الحديثة. لكن الوسائل المعترضة التي بدأت بالوصول عن طريق محطة الراديو في قبو موبورن في سان فرنسيسكو كانت من شاكلة مختلفة جداً تقريباً. كانت الرسائل الديبلوماسية اليابانية المتبادلة بين طوكيو والعواصم الكبيرة في العالم – واشنطن ولندن وروما وباريس وموسكو ووارصو وأنقرة – تتألف الآن من سلاسل من خمسة أحرف يسبقها مؤشر من خمسة أرقام، ولم يكن في ملفات ياردلي شيء يشبه هذا ولو من بعيد.

لقد كان ذلك إعادة شبه تامة لما جرى مع مكتب سيفرو على بعد قارة وقبل بضع سنوات في قراءة شيفرة القوات المسلحة الألمانية، وكان السبب هو السبب نفسه أيضاً. لقد استخدم اليابانيون الدروس من قراءة ياردلي وتبنوا آلة تشفير، على الأقل، في اتصالاتهم الديبلوماسية الحساسة.

كان أحد الحلول عند مجابهة مثل هذا التحدي في تحليل الشيفرة طبعاً اللجوء إلى اللصوصية. فقد قام مكتب المخابرات البحرية في الولايات المتحدة بالتسلل إلى القنصليات اليابانية والشركات والمنظمات الثقافية في عمل دائم، ولم يكن ذلك دون نتيجة، ولولا ذلك لواجه سافورد وروش فورت تحدياً يكاد لا يقهر في تفكيك

شيفرة البحرية اليابانية من البداية، لكنهما تلقيا عوناً كبيراً من نسخ من الكتاب الأحمر للرموز الذي صوره فريق الحقيبة السوداء من المخابرات البحرية خلال سلسلة كاملة من عمليات التسلل إلى القنصلية اليابانية في نيويورك في عام 1920 وعام 1926 وعام 1927. وقد بقيت مهمة تفكيك نظام التشفير فقط، وهذا اختصار كبير بالفعل. عندما انحلت رموز الكتاب الأحمر في نهاية عام 1930 في جزئين من كتاب التشفير (وسجل عليه «أزرق» – كان اللونان يشيران إلى الغلافين اللذين سجل فيهما العاملون في تفكيك الشيفرة من البحرية مجموعات الرموز المكتشفة)، كان هناك استمرارية كافية ليتمكن الفريق الذي تقوده الآنسة آجي Aggi من تفكيك نظام التشفير ولو استغرق ذلك ما يقرب من عامين من الجهد المتواصل فقط.

إن التسلسل إلى السفارات الأجنبية خرق فاضح للالتزامات الديبلوماسية، تبدو أمامها قراءة بريد شخص آخر مادة كمواد الأطفال. فليس لهذه المخالفة أي غطاء قانوني. كان هذا في الوقت الذي كان الجيش والبحرية يستميتان في إبعاد وزارة الخارجية عن معرفة أنهما يتنصتان على الرسائل الديبلوماسية بواسطة الراديو. في أوائل الثلاثينيات عندما كان الجيش لا يزال يتظاهر بأن أنشطة اعتراض الرسائل هي لأغراض البحث والتدريب فقط. بعدما بدأ موبورن عملياته الاعتراضية بوقت قصير حدث ما يشبه الفشل الذريع عندما علم رئيس الخطط الحربية في سلاح الإشارة بخطط مصلحة المخابرات السرية (SIS) للتوسع في مراقبة رسائل الديبلوماسيين الأجانب. فقام بإحالة الأمر إلى وزارة الخارجية بنية حسنة، فقامت الوزارة بالاحتجاج مباشرة على تدخل الجيش في مثل هذه الأنشطة. ونتج عن هذا لكزة سريعة تحت الطاولة قامت بها البحرية التي كانت تعقد اجتماعات سرية مع الجيش لمناقشة التنسيق بين الطرفين حول جهود المخابرات في الراديو. قال مرؤوس غاضب في مذكرة موجهة إلى رئيس الاتصالات البحرية في العاشر من نيسان 1933، "إذا كان الجيش لا يمكن الوثوق باستخدامه ما يشبه التعقل والتمييز في

كشف هذه الأمور خارج الدوائر العسكرية فإننا حينئذ سنخسر كل شيء في سعينا للتنسيق".

لكن مزايا السرقة كانت على وشك أن تأخذ مجراها في كل الأحداث. ففي الوقت الذي قدم فيه اليابانيون الشيفرة الجديدة (وقد تغيرت جذرياً) للاسطول البحري لتحل محل الكتاب الأسود بعد سنوات قليلة، قاموا بإصدار نظام شيفرة منفصل للملحقين البحريين اليابانيين، وقد استخدم هذا النظام آلة الشيفرة؛ ولم يكن من المحتمل أن تحتفظ القنصليات بنسخ من كتاب الرموز الجديدة التي تستخدمها البحرية فقط وتوجد لديها. وكان التسلسل إلى القنصليات، بغض النظر عن القانون والحصانة الديبلوماسية، دائماً سلاحاً ذا حدين. فلا يمكن ضمان النجاح، والعمل غير المتقن أسوأ من عدم القيام بأي عمل. جرت محاولة في 1935 لالقاء نظرة على آلة التشفير لدى الملحق البحري الياباني وكانت فشلاً ذريعاً بالفعل. فقد تحرت الرقابة في شقة الملحق الفخمة في واشنطن في بناء (آلبان تاورز) الواقع على الشارعين ويسكاونسن وماساشوستس صوت طقطقة غامضة. بينما كان الملحق وزوجته يتناولان العشاء ذات يوم من تموز – وذلك بحسب خطة أعدت مسبقاً فقد دعيا من قبل ضابط بحرية من الولايات المتحدة يعرفاهما – دخل الرائد البحري جاك هولت ويك ورئيس رجال الراديو البحري البناء على أنهما كهربائيان وتسللا إلى مكان إقامة الملحق وشقة مكتبه. على الرغم مما زعمه عدد من الكتاب إن" هولتويك" قد حصل على واحدة من الآلات، فإنه في الواقع لم يجد شيئاً مطلقاً يشبه آلة تشفير، يحتمل أن يكون هذا أحد المزاعم أيضاً. وما من شيء آخر يمكن أن يجعل اليابانيين ينتقلون انتقالاً رشيقاً إلى شيفرة جديدة أكثر أماناً. ونتيجة لذلك أظهرت حكمة ترك عمل الحقيبة السوداء الثقيل وحيداً. حوالي عام 1938 وظفت القطعة البحرية الثانية عشرة في سان فرنسيسكو مخبراً خاصاً اسمه سيمان غاديس، ويدعوه أصدقاؤه «صوبي Soapy»، لفتح الأقفال والتسلل إلى المكاتب اليابانية المختلفة على الساحل الغربي. في أيار من 1941، ركب الباخرة التجارية اليابانية بوصفه عميل جمركي من ميناء سان بيدرو، و«اكتشف» مخدرات مخبأة

كان قد زرعها في صندوق القبطان ونتيجة لذلك صادر محتويات الصندوق – وبينها نسخة من كتاب شيفرة السفينة التجارية اليابانية. صورت البحرية الكتاب قبل إعادته، وما كان اليابانيون ليفشلوا بإدراك ما كان يجري. ففيروا الشيفرة سريعاً. في ذلك الحين أصبح الجيش مدركاً أن محاولات تسلل أخرى تقوم بها البحرية قد تعرض للفضيحة عمل سنوات على ما هو أهم في آلات التشفير الديبلوماسية، وتوسل الجيش إلى البحرية أن تقاوم قناعها وطعنات خناجرها، ويبدو أن البحرية قد وافقت على ذلك.

--- --- ---

كانت الآلات التي قدمها اليابانيون إلى ملحقيهم البحريين وللرسائل الديبلوماسية العالية المستوى أبسط من آلة إنيغما. لكن محللي الشيفرة في الوحدة OP-20-G وفي مصلحة مخابرات الإشارة التابعة لفريدمان لم يعرفوا ذلك في البداية وذلك لأن الآلات اليابانية «الحمراء» (الديبلوماسية) و«MI» (للملحق البحري) تختلف عن إنيغما لأن تصميمها غير معروف كلياً. حتى مبدأ تشغيلها سر غامض. لكن بضعة أشياء غريبة ظهرت فوراً بعد فحص للرسائل المشفرة ذاتها. وأكثر الأمور ملاحظة هي الأحرف الصوتية الستة: A, E, I, O, U, Y فقد دلت على نصف الأحرف التي ظهرت تقريباً. وشك فريق مصلحة المخابرات السرية SIS بذلك لأن الآلة شفرت الأحرف الصوتية كأحرف صوتية، والأحرف الصامتة كأحرف صامتة. تشفر هذه الطريقة النص المشفر بكلمات ملفوظة، وهذه صفة للرموز العديدة التي تستخدم مجموعات الرموز من أبجدية واحدة أيضاً، وقلل هذا من فرص كتابة الأخطاء، وكذلك تطالب شركات الكابلات كلفة أقل لقاء معالجة البرقيات المشفرة التي تتألف من كلمات مثل: «LOVVE ZOXIL YUMUP» مقابل « XHDGH WJDQW KJGDG».

أمضى روليت وكوباك أربعة أشهر وهما يعالجان رسائل الآلة الحمراء بالأساليب الإحصائية التي يتعلماها تعلماً كاملاً. كانت هذه هي الطريقة المنهجية والعلمية. ولكن في وقت متأخر من إحدى الليالي وبينما كان روليت مستلقياً لا

يستطيع النوم خطر له أن من بين الرسائل التي كدساها ثلاث رسائل طويلة جداً، وقد بثت جميعها في اليوم نفسه وعلى الشبكة ذاتها. لو كانت هذه الرسائل مشفرة باستخدام وضع الآلة ذاته، فقد يكون من المحتمل بطرق الحدس والتخمين والحس والحذر أن يجدا بعض الصيغ والأشكال للأحرف الصوتية والأحرف الصامتة التي تبدو مثل الكلمات اليابانية. كان من الواضح أن اليابانيين يستعملون الأحرف الرومانية في تهجئة الكلمات اليابانية في الجهاز، وبينما لم يكن كولباك ورولیت محترفين في اللغة، فقد تعلما بعض الأمور الأساسية وعرفا المقاطع وكيف تتجمع.

كان رولیت وكوباك فريقاً غريباً. كان «كولي»، كما هو معروف، طلق اللسان وبلدوزر كلام من نيويورك. كان مظهره ممتلئ الجسم ويبدو ذلك مبالغاً فيه لأنه أكثر من أشعث الشعر والثياب وكاد أن يكون آخر رجل على الكرة الأرضية يتمسك بالرسميات. والعلامة المميزة التي يتذكرها زملاؤه كرار ورق الحمام الذي أخذه من حمام الرجال ووضعه على طاولة مكتبه ليستعمله لمسح أنفه وتنظيفه عندما يصاب بالرشح والبرد. وكان دائماً يجرح المشاعر عن غير قصد، لكنه يوازن تلك الفظاظة الخارجية بلياقة أساسية وعدم استياء من الآخرين مما أكسبه ولاء دائماً ممن خدموا تحت إمرته فيما بعد. أما رولیت فكان أكثر تحفظاً وصعب الإرضاء في أموره الشخصية وفيما يخص عمله أيضاً. وكان منفتحاً ناعم الكلام ومجاملاً ولطيف المعشر كرجل من الجنوب، ويتمتع بعادات الدقة كصاحب حرفة – وبالفعل كان، فقد كان رولیت الميكانيكي الماهر في المجموعة الذي يستطيع تجميع الآلة الدقيقة عندما يتطلب الأمر. وكان أيضاً حساساً جداً حول إحساسه بما يستحقه، وتحول هذا الإحساس إلى حدود الوسواس وهو يكافح على مدى عقود معركة للحصول على الاعتراف بالفضل والتعويض المالي من الحكومة على اختراعه آلات التشفير عندما كان يعمل تحت إمرة فريدمان. كونه الشخص الوحيد غير اليهودي بين المحترفين الأربعة في مصلحة المخابرات السرية SIS، وحقده على الإهمال والاستخفاف سواء كان حقيقياً أو

متخيلاً كانت كلها تتخذ لون المعاداة للسامية. لم يكن من السهل مصادقة كولباك ولا روليت من طرق مختلفة.

لكنهما قبلا التحدي الفكري بالطريقة ذاتها، فبعد ظهور روليت في منتصف الليل، انهمكا في الرسائل الطويلة الثلاث يبحثان عن الكلمات الممكنة والمحتملة. وعند الظهر حددا الكلمات المتكررة في الرسائل حيث ظهرت الكلمة Oyobi، ومعناه «and – و»، ولمعت أحرفها الصوتية من خلال بحر من الكلمات. ومن هنا جاء الكشف الحاسم سريعاً. وكان شكل التبديل حيث تخلط الأحرف الصوتية، يمر من خلال دوران اسطواني متكرر؛ وفي الواقع كان جدول فيجينير 6 × 6 في الأساس. وينتقل الجدول باتجاهه نحو الأسفل وضعاً واحداً عندما يجري تشفير كل حرف من حروف النص. لو شفر الحرف «*a*» بحرف E في الحرف العاشر من الرسالة، ومن ثم الحرف «*a*» الذي يظهر كالحرف السادس عشر سيشفر بحرف E. وتبدأ «مقاطع شبيهة» تتضح في النص – أي كل مجموعتين في النص المشفر يبدو أن تمثل الكلمة ذاتها في النص البسيط. مثلاً، هذان المثالان:

QIVVDA

TUZZHY

يبدو أنهما من خلال الأحرف الصوتية والأحرف المضاعفة عبارة عن «مقاطع متشابهة». ويكشفان عن خاصة مثيرة أخرى: في التسلسل الأبجدي لستة وعشرين حرفاً صامتاً بعد إزالة الأحرف الصوتية الستة، يبتعد حرف T ثلاثة أحرف وراء Q، ويبتعد الحرف Z ثلاثة أحرف بعد V، وحرف H بعد حرف D بثلاثة أحرف. بعبارة أخرى، إن أبجدية التشفير تنزلق على ثلاثة مواقع. فتشفر الأحرف الصامتة بموجب دول فيجينر أيضاً، وهذا هو 20× 20؛ وينتقل أيضاً موقعاً واحداً عند طباعة الحرف الذي يليه. وقصة الحروف المضاعفة في النص المشفر أنها نتيجة لشكل النص البسيط مثل *ts* أو *sr*؛ فعندما تخضع لمفتاح الانتقال تنتج هذه الحروف المجاورة الحرف المشفر نفسه.

النص المبسط

الحرف الأساسي	b	c	d	f	g	h	i	j	k	l	m	n	p	q	r	s	t	v	w	x	y	z
1	B	C	D	F	G	H	I	J	K	L	M	N	P	Q	R	S	T	V	W	X	Y	Z
2	C	D	F	G	H	I	J	K	L	M	N	P	Q	R	S	①	V	W	X	Y	Z	B
3	D	F	G	H	I	J	K	L	M	N	P	Q	R	S	①	V	W	X	Y	Z	B	C
4	F	G	H	I	J	K	L	M	N	P	Q	R	S	T	V	W	X	Y	Z	B	C	D

وهكذا

من الظاهر أن الآلة هي جهاز قرص دوار بسيط. فتوضع الأحرف الستة والعشرون على لوحة مفاتيح توصل إلى مجموعتين منفصلتين من الأقراص الدوارة، واحد للأحرف الصوتية الستة، وواحد للأحرف الصامتة الستة والعشرين؛ عندما يطبع كل حرف يدور القرص الدوار موضعاً واحداً، وينتج عن ذلك انتقال سطر واحد إلى الأسفل في جدول التبديل. هناك ثنيات إضافية في عمل الآلة أضافها روليت وكولباك سريعاً. يمكن استخدام لوحة قوابس لتبديل هويات الأحرف الصوتية والأحرف الصامتة فيما بينها قبل الدخول في القرص الدوار. لقد بدل هذا هويات الأحرف التي تم خلطها، لكنه لا يبدل الصيغة التحتية التي تستخدمها الأقراص الدوارة لبدء هذه التغيرات، عندما تتحدد الصيغة التي ستخلط بموجبها أحرف التشفير بحسب جدول فيجنير، يصبح تحديد هويات الأحرف لقابس كل يوم مسألة بسيطة تتعلق بتعداد التكرار.

واكتشفا أيضاً أن أتقدم لم يكن ثابتاً دائماً في بعض الأحيان يبدو أن القرص الدوار يسير موضعين بدلاً من موضع واحد عند انتقاله من حرف إلى آخر، فيترك سطراً إضافياً من الأسفل في جدول فيجنر. في الآلة الحمراء يضبط التقدم «بدولاب كسر» ذي سبعة وأربعين مسماراً، يمكن إزالة بعضها لإحداث التقدم المضاعف. لكن الإجراءات اليابانية في وضع المفتاح اليومي حددت مدى ضيقاً من الخيارات، واكتشف روليت وكولباك هذه الصيغة للتقدم عبر الصفوف في جدول فيجنير وأنها تتبع دورة من (واحد وأربعين، واثنين وأربعين وثلاثة وأربعين).

في يوم واحد حللا آلة شفيرة، مشهد لم يحصل من قبل. كان فريدمان في فورت مونماوث Fort Monmouth في نيوجيرسي، في مخبر سلاح الإشارة في الجيش لبضعة أيام، ودهش للخبر الذي استقبله عند عودته صباح اليوم التالي.

أوقف هذا النجاح مؤقتاً بعض العواصف التي تهب بين البحرية والجيش، ولكن ليس إلى وقت طويل. فقبل بضعة أشهر قامت الوحدة OP-20-G بحل آلة الملحق البحري، التي يبدو أنها تشترك مع الآلة الحمراء بعدد من المواصفات الأساسية، لكن رئيس الوحدة OP-20-G الملازم جوزيف وينغر رفض الكشف عن نتائج البحرية، فادعت البحرية أن الجيش يشبه الغربال لأنه يطلع الكثيرين من المدنيين على أسرار عديدة، لكن ذلك تبرير أكثر من أن يكون تفسيراً حقيقياً. كان التفسير الحقيقي أن المصلحتين تتنافسان منافسة مريرة. وكان أكثر ما استطاع فريدمان أن يتوصل إليه مع وينغر هو الإقتراح بأن يبحثا في النصوص المشفرة عن دورة هي أكثر من أربعين وأقل من خمسين في تقدم التبدلات الأبجدية. وعندما بدأ العاملون في مخابرات الجيش يرسلون نصوصاً محللة من رسائل الآلة الحمراء إلى مكتب المخابرات البحرية، حاولت البحرية في أكثر من مناسبة أن تهزم الجيش في نشاطه بتسليم بعض المواد الساخنة إلى وزارة الخارجية (وهي الآن بعد ستيمسون)، وهذا ما كان يغضب محللي الشيفرة في مصلحة المخابرات السرية SIS.

نتج عن تحليل رموز الآلة الحمراء والكتاب الأحمر والكتاب الأزرق بضعة أعمال للمخابرات ذات أهمية من الدرجة الأولى. كانت الضربة الناجحة قبل الحرب سلسلة من الرسائل البحرية جرى تحليلها في صيف عام 1936 التي نقلت نتائج محاولات بحرية للسفينة ناغاتو. وكان هذا إعادة تجديد سفينة من الحرب العالمية الأولى كانت الولايات المتحدة تعتقد أنها لا تستطيع تحقيق أفضل من ثلاث وعشرين عقدة. ولكن بعدما جهزت بعنفات جديدة ذكر أنها حققت سرعة مقدارها 26 عقدة. وكانت السفن الحربية الأمريكية الجديدة تصمم لأن تكون سرعتها القصوى 24 عقدة. أمرت البحرية فور تلقيها تقرير الوحدة OP-20-G أن

تعاد تصاميم السفن الحربية من طراز نورث كارولينا لتحقق 27 عقدة، وأن تكون سرعة الفئات اللاحقة 28 عقدة. قال لورنس سافورد فيما بعد وهو يبرر، لقد كان عملاً من أعمال المخابرات الذي عوض كل ما أنفق على مخابرات الراديو «بأكثر من ألف مرة».

ولكن تلبدت غيوم الحرب وبدأت النظرة تتراجع سريعاً. ففي تشرين الثاني 1938 حلت شيفرة جديدة محل الكتاب الأزرق بوصفه الكتاب الرئيسي لفرقة البحرية اليابانية. ومع أن هذه الشيفرة الجديدة (AD) مشابهة للكتاب الأزرق، فقد تغيرت مجموعات الرموز كافة. كانت عودة إلى المجموعة المربعة. في 18 شباط 1939 تم تحليل رسالة حمراء تعلن أن الآلة الجديدة «B» ستحل محلها خلال يومين. وبعد يومين ظهر الجهاز الذي سمته مصلحة المخابرات السرية «الأزرق». أعطى هذا الجهاز شيفرة أعقد كثيراً مما أعطته الآلة الحمراء، وكان من الواضح أنه لا يوجد حل سريع ممكن. وفي الأول من حزيران 1939 ظهرت شيفرة بحرية جديدة تماماً وتختلف عن أي شيفرة يابانية أخرى اعترضتها الوحدة OP-20-G. وكان واضحاً من تحليل الرسائل المكتوبة بالشيفرة «AN» (وعرفت فيما بعد بأنها JN-25) أنها عملية التشفير الرئيسية للعمليات من المستوى العالي للبحرية اليابانية جميعها. فقد كانت لا يمكن اختراقها تماماً.

وفي صيف عام 1939، كانت أمريكا عمياء.

--- --- ---

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.

- مقالة عربية من العصور الوسطى: كاهن (مفككو الشيفرة) 97–98.
- الخليل: كاهن (مفككو الشيفرة) 97.
- 6 ملايين برقية: كاهن (مفككو الشيفرة) 220.
- تحليل رياضي محدد: سلمون كولباك "طرق احصائية في تحليل الرسائل السرية" srma-13، الأرشيف الوطني.
- "أكثر الشرور شراً": تشرشل (الحرب العالمية الأولى) 323.
- كرهت الروس: ستوكسبري، الحرب العالمية الثانية، 64.
- "يجب أن أذهب وسأذهب" شيرر (صعود وهبوط) 212.
- أصبحت الرسائل غير مقروءة: بلوك " الاينغما قبل الأولترا: عمل بولوني" 145.
- سلسلة من الشركات: كاهن (مفككو الشيفرة) 421–422 ديفاورثر وكروه (تفكيك الرسائل السرية آلياً) 94.
- ما يقرب من 17000 رسالة: فيوجد 26 × 26 × 26 أو 17576 مجموعة مختلفة محتملة لثلاثة أقراص دوارة. ولكن في العمليات الحقيقية للإينغما، إن مجمل الأسباب الآلية "انتقال مزدوج" ليحدث في منتصف القرص الدوار: وفي كل مرة

يتقدم فيها القرص الأوسط إلى المركز حيث يثير دورة إلى القرص الأيسر، فإنه يتقدم مباشرة عندئذ مرة أخرى (مع القرص الأيسر) عندما يتم إدخال الحرف التالي. فلو حدث الانتقال ما بين الحرف E والحرف F على القرص الأوسط، والحرف V والحرف W على القرص الأيمن، فيكون التوالي الحقيقي للقرص كما يلي: ADU، ADV، AEW، BFX، BFY، BFZ، BFA، وهكذا يكون طول المفتاح في الإينغما الطبيعية بالفعل 26 X 25 X 26. أو 16900. وعندما تتقدم الأقراص ذات الانتقالات، فيقصر طول المفتاح أكثر. انظر هامر "الإينغما".

- 150 مليون تغيرات مسبقة: ميلر (رياضيات الإينغما) 9.
- ليخدع فقط: كوزاكزوك (الإينغما) 9.
- "اهتمام ألماني بالإينغما" (قصة الكوم السادس)207–208، ويتاك "محادثة مع ماريان ريجيفسكي"58
- دورة في تفكيك الرسائل السرية: كوزاكزوك (الإينغما)1–4.
- "لا تخبر زملاءك" ويتاك "محادثة مع ماريان ريجيفسكي" 52–53، توجد تقارير متناقضة حول متى بدأت ريجيفسكي العمل بالإينغما. تذكر ريجيفسكي أنه في وقت متأخر من تشرين الثاني 1932، ولكن بحسب إعادة التركيب المقنع الذي قام به بلوك، "الإينغما قبل الأولترا": عمل بولوني، 148، لا بد أن الوقت كان حوالي 15 تشرين الأول.
- رموز "مشتركة": قاموس لتفكيك الرسائل السرية" رقم HCC 4559.
- من كاغا: المثال التوضيحي جرى تعديله من هنسلي وستريب (معدان) (مفككو الرسائل السرية) 278.
- مرمزة بأشكال خمسة مختلفة على الأقل (تاريخ GYP 1)، CNSG.5750 /202، ملفات كرين، الأرشيف الوطني.
- "أهلاً بكم أيها السادة" روليت (قصة سحر) 19–34–35.
- سلسلة مجموعات كل منها خمسة أحرف: روليت (قصة سحر) 87، 111.

- نسخ من كتاب الرموز الأحمر: لورانس سافورد، "الحرب غير المعلنة، تاريخ R.I 15" تشرين الثاني 1943 3095 ,SRH. الأرشيف الوطني بكلية بارك 11–12، ليتون (كنت هناك) 31–32، 45–46.
- "تشابه بالتعقل" ج. وماكلاران: مذكرة إلى المدير، 10 نيسان 1933، ملف G–OP–20 حول تعاون الجيش والبحرية، 1931 إلى 1945، SRH 200، والأرشيف الوطني بكلية بارك، 600.
- سيمان غاريس: ليتون (كنت هناك) 109–110، " شكوك اليابانيين" رقم 1812، مجموعة الرسائل السرية التاريخية.
- يقاوم دوافع العباءة والخنجر: روليت (قصة سحر) 189.
- استلقى روليت لا يستطيع النوم: روليت (قصة سحر) 112–122.
- بلدوزر شخص من نيويورك: فيليبس، مقابلة المؤلف: لويس، مقابلة المؤلف: رسالة شهرية ثانية: الكابتن جيفري ستيفنز، 17 آب 1942، HW 14/94؛ ديوان السجل العام، 2.
- كان روليت أكثر تحفظاً: فيليبس، مقابلة المؤلف؛ لويس، مقابلة المؤلف؛ روليت (قصة سحر)، 252.
- معركة طولها عقود: لقد كافأ الكونغرس فريدمان بمائة ألف دولار في عام 1956 لتطويره آلة سيغابا الكهربائية للشيفرة ولاختراعات أخرى لكنه لم يستطع الاستفادة من المكافأة نظراً لسرية المخترعات بصورة مباشرة. وألح روليت إنصافاً على أن الأفكار الحاسمة في سيغابا هي أفكاره. وفي آخر المطاف كافأه الكونغرس بمائة ألف دولار في 1964.
- "أشياء متشابهة" ثم بدأت تتوضح: ديفرز وكرو (آلة الكتابة السرية) 212–220.
- ملاطفة من وينفر: كولباك: تاريخ شفوي: روليت (قصة سحر) 112–113.
- هزم الجيش بقوة: روليت (قصة سحر) 129–130.
- "ألف مرة انتهت": الحرب غير المعلنة، تاريخ SRH–350,R.I، الأرشيف الوطني بكلية بارك، 13.
- الرمز "AD": ليتون (كنت هناك) 77.

- آلة "B" جديدة: "تاريخ مجموعة الأمن البحرية إلى الحرب العالمية الثانية"، SRH–355، الأرشيف الوطني بكلية بارك 1.
- 1 حزيران 1939: تاريخ 1–، GYP، 202/5750/GNSG، ملفات كرين، الأرشيف الوطني بكتابة بارك 1.

--- --- ---