جرّ الخطى نحو التشفير

كان واضحاً حين أطل عام 1995، أن ميدان الكريبتوجرافيا ـ بكل أبعاده ـ قد تبدلت ملامحه بشكل مؤثر، بالرغم من كل ما بذلته الحكومة من أفضل جهودها لإبقاء الأمور على استقرارها. فقد كانت تقنية التشفير، مندفعة بقوة الكومبيوتر والاكتشافا ت الجديدة التي طلع بها أمثال هويت ديفي في العالم، تتحرّك بسرعةا لمحرك التوربيني، منتقلة من عربة السفر التي تجرها الجياد إلىٰ زمن الإنترنيت. فبالرغم من التذكير ا لمتزايد باطراد بشبحا نتشار فوضى التشفير، حيث تنتشر الرموز وتفلت من عقالها إلىٰ حد لا تستطيع معه حكومة أَو مؤسَّسة أن تأمل في معالجة تجارة رقمية أَو قانون، فقد استمر الصراع القديم بين الإجراء ونقيضه. إن الغرباء وحدهم الذين لهم يد في هذه اللعبة.

قبل قرن ونيف كان إدجار ألان بو قد أصبح شبهمأ خوذ بموضوع علم الشّيفرة فكتب: «يمكن التأكيد مرة أخرى أن العبقرية الإنسانية، لا تستطيع أن تركّب شيفرة، يستعصي على عبقرية الإنسان أن تأتي بحل لها». من الناحية الرياضية كان بو على خطأ؛ فورق الحل لمرة واحدة التي عُرفت بمناعتها في محاولا ت الاختراق هي اللازمة الشعرية التي تفيد بأن زعمه مضى وانقضى إلىٰ غير رجعة. وفوق هذا وقبل كل شيء كان تنفيذ ورقة الحل الو حيدة أمراً مجهداً

لمن يتصدى له؛ وهو بالتأكيد غيرمنا سب في التطبيق إذا كان نطاق العمل واسعاً. وإذن هل كان الشاعر، من الناحية العملية، مصيباً في ما ذهب إليه؟ وكان مذهب مارتين جاردنر حين اقتطف قول بوفي مقاله الشهير عن الخوارزمية رسا في مجلة العلوم الأمريكية Scientific American، أن الشاعر أخطأ في ما ذهب إليه.

إنّ لسؤال قد أثار بلا ريب شجون فيل زيمرمان. فقد كان يشعر في أعماقه، أن خوارزمية التشفير في صميم برنامجه «منتهى السرِّيَّة» بي جي بي سليمة متينة. ولذلك حين فكّر بتسمية البرنامج اختار هذا الاسم، والحق أنه يمكن لمستخدمي هذا البرنامج أن يطمئنوا إلىٰ منعته أمام محاولات من يعملون في تفكيك الشيفرات. وقدأشارت الحكومة أيضاً إلىٰ متانته، في تصريحاتها العلنية على الأقل. ففي ربيع عام 1995 شهد لويس فريه من مكتب لتحقيقا ت الفيدرالي ووليم كرويل من وكالة الأمن القومي في جلسة استماع سرِّيَّة في ا لكونجرس بأن من الصعب تفكيكالر سائل المشفَّرة بمفاتيح طويلة. وكانت شكوى فريهأنه ليس لدى [مكتب التحقيقات] لاا لتكنولوجيا ولا القدرة على استخدام القوة الغاشمة لبلوغ هذها لمعلومات». أما كرويل فمضى إلىٰ أبعد من هذا، إذ قال، مستنداً إلىٰ التطورات الراهنة التي بلغتها تكنولوجيا الكومبيوتر الشخصي، أن«تفكيك ر سالة مشفرة بمفتاح من 128 بت، الذي يستخدمه برنامج «منتهىا لسرِّيَّة» بي جي بي يستغرق 8,6 تريليون أمثال عمر الكون».

ولكن زيمرمان كان يعلم أن هجوماً بالقوة الغاشمة، على خوارزميةآيديا International Data Encryption Algorithm IDEA ـ خوارزمية تشفيرالبيا نات العالمية ـ ليست الطريقة الوحيدة لتحويل شيفرته إلىٰ ما يمكن وصفه «بمحاولة جيدة لبلوغ السرِّيَّة». فقد كان هناك ما لا يحصى من الطرق لتفكيك الشيفرة. ولربما كان بالإمكان إنجاز عملا لمفتاح العام من البرنامج بخوارزميات أشد فاعلية في تحليل العوامل وعتاد كومبيوتر ضخم أقوى. أو قد يكون في تفاصيل

تنفيذ برنامج «منتهى السرّيّة» مثالب، وهذا أرجح، توفر لمحلل للشيفرة طريقاً مختصراً للوصول إلىٰ النص الأصلي الواضح.

ولقد شاءت الصدفة، أن يجتمع بضعة من الاختصاصيين بالشّيفرة ذات مساء في مؤتمر لهم سنة 1995، في سانتا بربارة، وهم في زيهم التقليدي من قمصان رياضية، وينتعلون الصنادل، وأخذوا يتحلّقون حول أحد المتحدثين البارزين في تلك الليلة. وكان هذا روبرت موريس الأب، ولم يسبق له أن حاضر في جميع، إلاّ اللهم من كان مخولاً بالاطلاع على أسرار الحكومة الأمريكية. وكان موريس قد تقاعد لتوه، وهو في منصب كبير العلماء في فورت جورج ميد. فاجتذبتهم شهرته، وقد باتت ضخمة بسبب الإنجازات التي تنسب إليه ولا سبيل إلىٰ معرفتها لأنها في خدمة مملكة الأشباح إلىٰ طاولته. ولما ذكر أنه لا يمانع في لقاء فيل زيمرمان، أسرع من ينادي الرجل ذا للحية المشذبة والحادي والأربعين من العمر.

بادره رجل المخابرات السابق ـ وهو ينفث دخان سيجارته بشدة ـ بالحديث: «دعني أطرح عليك، يا فيل، سؤالاً. لنفترض أن زيداً من الناس استخدم [برنامجك] «منتهى السرّيّة»، لبث رسالة يترتب عليها ضرر شديد. فكم ستكون كلفة تفكيكها؟».

أجاب زيمرمان، وقد بدا عليه الضيق: «قد سبق أن وجّه إليَّ هذا السؤال من قبل. وردي هو أن ذلك ممكن».

«ولكن كم ستكلف؟».

كان هذا الموضوع بعيد كل البعد عن الموضوعات الأثيرة لدى زيمرمان، إلاّ أنه قبِل بمسايرة محدِّثه. فقال على سبيل التخمين أن الاعتماد على حجم المفتاح ليس السبيل الأفضل لشن الهجمات على برنامج «منتهى السرّيّة»، بل الأجدى العناية بنقاط الضعف الأخرى. وذهب إلىٰ أن المرء قد يجد اضطراباً في بنية البيانات، كما أن في تقويم الأخطاء فيها ضعف.

هز موريس رأسه ولم يعلق بكلمة. فمن ذا الذي يعلم إن كانت وكالة الأَمن القومي قد اكتشفت فعلاً عيباً بسيطاً أتاح للمساحات الكبيرة من السيليكون في القبو العتيد في مقرها لفظ النص الواضح الأصلي الذي بثّه المناضلون الأحرار الذين يُزعم بأنّهم يستخدمون برنامج زيمرمان؟ ولكن في اليوم التالي ضمن موريس في حديثه تعليقاً موارباً على علماء الشّيفرة الجدد ورؤاهم الفوضوية للشيفرة. ولم يكشف في ذلك أية أسرار مهنية، لكنه بروح حكماء الشرق قدم حكمتين تصدقان في كل زمان ومكان ـ قولان من عقيدة الشّيفرة ـتو مئان إلىٰ المصالحة التي لا بد أن تتحقق بين «المنصفين»، وهي مصلحة تتجاوزا لصراعات السياسيَّة الراهنة. وكانت تلك لمحة من مشهد مجتمع ما بعد المقراض في القرن القادم.

القول الأول (الموجه إلىٰ مفككي الشّيفرة): لا تقلّل من تقدير عزم خصمك على بذل المال والوقت لتفكيك الشّيفرة التي تستخدمها. وكان جوهر حديث موريس أن من لأ فضل أن تدع الكريبتوجرافيا لذوي العقل الذي يحكمه جنون البارانويا، أولئك الذين يؤمنون إيماناً قاطعاً جازماً بأن خصومهم مجرد قوم ذوي ثراء فاحش وذكاء شديد وعزيمة ماضية، كلاب صيد تجري في أثر الطريدة. وهؤلاء سوف يشنّون هجماتمبا شرة على شيفرتك المعتمدة، وغالباً ما ينتصرون.

القول الثاني (الموجّه إلىٰ مفككي الشّيفرة): ابحث عن نص أصلي واضح. وكان هذا طمأنة للحاضرين، بأنّه مهما بلغ تفكيك النّص من الصعوبة الشديدة، فإن الحقيقة هي أن الذين يناط بهم أمر هذه الأَنظمةا لمعقدة، إنما هم بشر عاديون. وهكذا، قد تتضمن شيفرة تبدو مستعصية على الاختراق، خليطاً من قصاصات من الشيفرةا لقياسية الأمريكية، لتبادل المعلومات ASCII على المرء أن يطوعها لتخرج بلغة البشر، فيقع فيها المرء من حيث لا يتوقع على

مقطع أَو رسالة كاملة غير مشفَّرة، إن سهواً وإن مصادفة. فيمكنك أن تطالعها بأيسر ما يكون.

كان موريس يقول لفوضويي الشّيفرة: «حذار، فليس سهلاً أن تقيموا عالم شيفرة مثالياً». وهكذا تدور اللعبة القديمة. ولكنه بإلقائه الدرس على الغرباء كان يقر ضمناً بأن المستقبل ليس حكراً على حكماء وكالة الأَمن القومي، وإنما هو من شأن هؤلاء ذوي الشعر المسترسل، الذين يرتدون القمصان الرياضية في سانتا بربارة أيضاً.

لقد صدرت أقوال موريس، في وقت كان التوتر فيه على أشده بين الشّيفرة الشعبية والشّيفرة الحكومية، وزاد في الطين بلةً ظهور تحول مستمد حديثاً، فبعض القوى الصاعدة في مجال التشفير كانت قد تجاوزت الترميز، وغاصت عميقاً في تحليل الشيفرة؛ وفي حين أن هذا أمر نهض به حشود المهتمين بالتشفير من قبل، والأشهر في هذا يتجلّى في الهجمات على خطة ميركل المسماة الحقيبة المتعددة التكرارات، ظهر الآن نوع من الجهد جديد كل الجدة، ولا يمتثل للقواعد التقليدية التي صيغت في عالم وليم فريدمان أَو ألان تيورينج... وكان هذا تفكيك للشّيفرة يقوم على التراكم، أي جهد ضخم مشحون بالقدرات المضخمة التي تتسم بها الشبكة وكان رواد هذا المجهود هواة الشّيفرة، طبعاً ولم تكن هذه السلالة من مفككي الشّيفرة لتعنى بالجريمة أَو التجسّس، وإنما لطرح فكرة سياسية، وتحقيق أقصى المتعة.

بدأت أولى هذه الجهود ببرنامج «منتهى السرّيّة» بي جي بي، الذي طلع به فيل زيمرمان. وكان مستخدمو هذا البرنامج، قد شغلتهم شكوكهم الملحة بمتانته طويلاً قبل أن يثير موريس التساؤل حوله في مؤتمر الكريبتو 95. وقد عكس هذا القلق الأساسي الذي يشغل بال الكريبتوجرافيا الثورية: هل تستطيع أن تثق ببرمجيات طورت بدون ترخيص من مؤسَّسة مشهود لها بإنتاج الشيفرات المأمونة؟ كان هذا هو السؤال، الذي طرحه على نفسه ديريك أتكينس، وهو ما

يزال طالباً في العشرين من عمره، على مقاعد الدراسة في كلية الهندسة الكهربائية في معهد ملما تشوسيتس، سنة 1992. وقد كان رد فعله المبدئي على مشروع زيمرمان الانضمام إلىٰ الحملة الدائرة، ثم غدا عضواً في فريق التطوير الذي تكون بصورة عفوية لابتكار أشكال جديدة من البرمجيات. وأخذ اتكينس بعدئذ يتساءل أي شكل من الهجمات يمكن أن تؤثر في تلك البرمجيات.

وكما أشار بوب موريس في حديثه، فقد كان ثمة طريقتان لتفكيك نظام للتشفير: الأولى بالقوة الغاشمة، أي أنتتو سل بكل الحلول الممكنة، حتى تعثر على الحل الصحيح. والثانية تتطلب البحث عن طريق مختصر، أي نقطة ضعف غير مقصودة قد تتيح لك تفكيك رموز الرسالة المشفرة. وكان أن اختار اتكينس، بعد أن خاض في الموضوع مع أصدقائه ـ ومنهم مايكل جراف الأستاذ في جامعة آيوا ستيت. وبول ليلاند بجامعة أكسفورد ـ أن يسلك الطريق الأول في الهجوم. ولكن محاولة العثور على ثغرة أو عيب كانت أمراً يتجاوز طاقاتهأو تجربته. (مع أن هذا الطريق الذي حاولت الوكالة، كما ألمح موريس، أن تعرفه على الأرجح). ومن جهة أخرى، بدا الجميع متفقين على أن الخط المباشر، وربما الممكن، لتفكيك برنامج «منتهى السرِّيَّة PGP» هو الطريق الذي يسير عكس أي برنامج يستند إلىٰ خوارزمية رسا: أي طريق تحليل العوامل.

كان رايفست وشامير وأدليمان قد أدركوا، أ نه إذا اكتشف المرء طريقة سريعة لتحليل لعوامل: رأي تعيين العددين الأوليين الأصليين للذين جاء المفتاح منحا صل ضربهما، فإن نظامهم يصبح غير ذي جدوى. ولئن كانوا يتو قعون ظهور خوارزميات أفضل لتحليل العوامل فقد كان الفكر يزين لهم أنَّه ليس هناك في الأفق، ما يعد باحتمال تفكيك خوارزمية رسا. ومع ذ لك فقد شاء اتكينس وأصدقاؤه امتحان هذه الفكرة. وجنحوا يومذاك إلىٰ الظن بأنَّهم باعتمادهم على مصدر لم يكن متوفراً من قبل ـ أي آلاف الكومبيوترات المتوفرة

للناس الذين يتصلون بالإنترنيت ـ قد يستطيعون أن يبدأوا تاريخاً لتحليل العوامل. كل نت تلك حجة آسرة، من حيث قوة الحساب المتضاعفة لمستخدمي الإنترنيت بما يجعلها أشبه بسوبر كومبيوتر عملاق، ولعل هذا هو ابن عم لتلك الكومبيوتر المفترض أنّها موجودة في قبو فورت ميد. ولقد طرحوا الفكرة على أرجن لينسترا، عالم الرياضيات الخبير بجامعة بيلكور في نيو جير سي. فكان جوابه أن الأعداد الأولية الضخمة المستخدمة عموماً في «منتهى السرّيّة» (والنسخ التجارية من خوارزمية «رسا»)، أضخم من أن ينجح معها هجوم. ثم اقترح عليهم تحدياً آخر: الخوارزمية رسا 129.

ولقد بلغت فكرة لينسترا قلب القضية مباشرة، وهي هل يمكن للكريبتوجرافيا (التشفير) أن تكفل الأمان الكامل. وكان التحدي الذي يتجلى في «رسا 129» هو الذي طرحه مارتين جاردنر في عموده في مجلة العلوم الأمريكية عام 1977 ـ فالعمود الذي بدأ باستنكار قول [الشاعر إدجار الان] بو، أنه ليس هناك من شيفرة حصينة منيعة لا تلين إذا ما هوجمت. وظل هذا التحدي قائماً لا يجد من ينهض له طوال تلك السنين، وقد قدر الزمن الذي يستغرقه كومبيوتر جبار متفرغ لتحليل العوامل لرقم بهذا الحجم 40 كودريليون سنة. ولكن حتى وإن لم تقبل بهذا الرقم (ورايفست يقول الآن أنه كان خطأ رياضياً) فإن عدداً دون ذاك بكثير ـ ولنقل بليون أو بضعة ملايين من السنين ـ يعني أن من يتنفس اليوم، سيكون قد صار هباء منثوراً منذ عهد بعيد قبل أن يظهر سر رسالة مشفرة بخوارزمية رسا مؤلفة من مفتاح من 129 رقماً.

ومع ذلك فقد جمع اتكينس وجلر ف وليلاند ولينسترا بعد خمسة عشر عاماً قواهم مع الإنترنيت، للفوز بالمئة دولار في غضون شهر.

كان أول ما احتاجه هؤلاء، وربما الأهم، هو خوارزمية جيدة لتحليل العوامل. وكانت قد تحقّقت بعض التطورات النظرية في هذا المجال منذ أن نُشر مقال جاردنر، ويخص بالتنويه ما ابتكره أحدهم، وهو الحرا ف غربال

ا لممدد التربيعي لعدد أولي كبير مضاعف متعدد الحدود». وهذا يتضمن بحثاً في عالم الأعداد يعرف با لفضاء المتجهي Vector Space لأعداد تُعرف بـ«ا لشعاع الأحادي» Univector. ويمكن رسم العلاقات الرياضية، بجمع هذه الأعداد، على نحو يؤدي إلىٰ معرفة الكثيرين الأوليين الأصليين. «وليس عليك، كما يقول اتكينس، أن تستقصي كل مجال الاحتمالات، بل حسبك جزء بالغ الصغر من الفضاء. ولك أن تشبه الأمر بأننا كنا نبحث عن ثمانية ملايين إبرة في تل من القش مليء بما لا يحصى من الإبر، وإن لم تكن تبحث عن إبرة بعينها، وإذن حسبك من الأمر أن تجد ما يكفي من هذه الإبر ثم تقوم بجمعها بوسيلة رياضية معينة، بما يساعدك على تحليل العدد إلىٰ ا لعوامل الأولية التي يتألف منها». وقد كان هذالأ سلوب مثالياً لهجوم إنترنيتي موزع حيث تتجمع قوى مئات الناس مع بعضها البعض لحل المعضلة».

في صيف 1993، كان البرنامج قد تم واكتمل، وكان اتكينس يجري هذا البرنامج على كومبيوترات مخابر الإعلام في معهد ماساتشوسيتس، وبات بالإمكان بعد هذا، تجنيد المتطوعين مع لكو مبيوتر. وكانت الاستجابة عظيمة، إذ أخذ أكثر من 1600 آلة بالعمل في حل المسألة، على امتداد العالم، وفي كل قارة عدا القطب المتجمد الجنوبي. وقد تفاوتت هذه الكومبيوترات من حيث الحجم، من الكومبيوتر الشخصي الصغير، حتى السوبر كومبيوتر ماسبر المعالج 16000 في مخابر بل.

تقاس قدرة الكومبيوتر بمليون أمر MIPS في العام ـ أي أنه آلة تستقبل مليون من التعليمات في الثانية على مدار العام. وقد استخدمت في تجربة خوارزمية «رسا 129»، ما بين أيلول/ سبتمبر 1993 ونيسان/ أبريل 1994 حوالي خمسة آلاف من أعوام MIPS هذه. وكان في تلك الفترة أن فطن اتكينس والآخرون إلىٰ أنّه بات لديهم ما يكفي من الأشعة الأحادية للقيام بالحسابات

لمن يتصدى له؛ وهو بالتأكيد غيرمنا سب في التطبيق إذا كان نطاق العمل واسعاً. وإذن هل كان الشاعر، من الناحية العملية، مصيباً في ما ذهب إليه؟ وكان مذهب مارتين جاردنر حين اقتطف قول بوفي مقاله الشهير عن الخوارزمية رسا في مجلة العلوم الأمريكية Scientific American، أن الشاعر أخطأ في ما ذهب إليه.

إنّ لسؤال قد أثار بلا ريب شجون فيل زيمرمان. فقد كان يشعر في أعماقه، أن خوارزمية التشفير في صميم برنامجه «منتهى السرِّيَّة» بي جي بي سليمة متينة. ولذلك حين فكّر بتسمية البرنامج اختار هذا الاسم، والحق أنه يمكن لمستخدمي هذا البرنامج أن يطمئنوا إلىٰ منعته أمام محاولات من يعملون في تفكيك الشيفرات. وقدأشارت الحكومة أيضاً إلىٰ متانته، في تصريحاتها العلنية على الأقل. ففي ربيع عام 1995 شهد لويس فريه من مكتب لتحقيقا ت الفيدرالي ووليم كرويل من وكالة الأمن القومي في جلسة استماع سرِّيَّة في ا لكونجرس بأن من الصعب تفكيكالر سائل المشفَّرة بمفاتيح طويلة. وكانت شكوى فريهأنه ليس لدى [مكتب التحقيقات] لاا لتكنولوجيا ولا القدرة على استخدام القوة الغاشمة لبلوغ هذهٔا لمعلومات». أما كرويل فمضى إلىٰ أبعد من هذا، إذ قال، مستنداً إلىٰ التطورات الراهنة التي بلغتها تكنولوجيا الكومبيوتر الشخصي، أن«تفكيك ر سالة مشفرة بمفتاح من 128 بت، الذي يستخدمه برنامج «منتهىا لسرِّيَّة» بي جي بي يستغرق 8,6 تريليون أمثال عمر الكون».

ولكن زيمرمان كان يعلم أن هجوماً بالقوة الغاشمة، على خوارزميةآيديا International Data Encryption Algorithm IDEA ـ خوارزمية تشفيرالبيا نات العالمية ـ ليست الطريقة الوحيدة لتحويل شيفرته إلىٰ ما يمكن وصفه «بمحاولة جيدة لبلوغ السرِّيَّة». فقد كان هناك ما لا يحصى من الطرق لتفكيك الشيفرة. ولربما كان بالإمكان إنجاز عملٔا لمفتاح العام من البرنامج بخوارزميات أشد فاعلية في تحليل العوامل وعتاد كومبيوتر ضخم أقوى. أو قد يكون في تفاصيل

تفكيك الخوارزمية «رسا 129» أبعد ما يكون عن الصعوبة، مقارنة برموز الرسا المستخدمة في النشاط التجاري. فعندما يستخدم نظام الرسا 129، عدداً يكون طول المفتاح 245 بت. لكن مفتاح الرسا المعياري ـ وهو الذي تستخدمه برمجيات الشركة ـ كان طوله 1024 بت. ولو كان فريق اتكينس يقوم بالعمل ذاته بمفتاح بذاك الطول لكانت كومبيوتراتهم ما تزال تعمل على حلّ المعضلة، لأمد من بضعة ملايين أخرى من السنين.

ومع ذلك فقد كان هذا العقم متوقعاً لرسا 129. فهل يمكن للتقنيات الجديدة في تحليل عوامل الأرقام أن تذوب أثخن مفاتيح الرسا؟ قد يكون هناك فتوحات في الرياضيات يمكن بها تسريع تحليل العوامل، إلاّ أن الخطر الأعظم على قوة أنظمة التشفير برز مع تطوير ما يُعرف بالكومبيوتر الكمية Quantum Computers، وهي آلات تفيد من فيزياء الجزئيات، لتجري بسرعة أعظم مما تعمل به النماذج الحالية. (قارن فارق السرعة بين السلاحف وأشعة الليزر). وكانا لعلماء يخطونا لخطوات الصعبة لتنفيذ هذه الكومبيوتر بعد أنكا نت موضوعاً نظرياً. فإذا تمت الرحلة وخرجت الكومبيوتر الكمية صار بوسعك عندئذ أن تضرب صفحاً عن نظام الرسا في التشفير. وهاك ما كتبه الكريبتوجرافي جايلز براسارد في عام 1996: «أعتقد أنني سوف أرى في حياتي أداة كمية خاصة لتحليلا لعوامل. فإذا تحقق هذا فسوف يكون هجر «الرسا» واقعاً. «وقد ورد هذا، في نشرة كريبتو بايتس التي تصدرها آر إس إيه داتا سيكيوريتي.

ولكنذ لك ظل من قبيل لاحد س. أما الواقع فهو أن ديريك اتكينس وزملاءه التقطوا ما بدا لهم مسألة مستعصية على الحل واستطاعوا تفكيكها، دون أن يجمعهم جامع رسمي، وبواسطة مجموعة متنوعة من الكومبيوتر، كيفما اتفق. وخلاصة ما قاله: «ما تعلمنا هو أنّه بوسع مجموعة من الهواة أن يجتمعوا معاً وينفذوا هذا الأمر». أما المزاعم ونسبة العصمة فينبغي النظر إليها بعين الشك.

أما الهدف التالي فكان لا يقاوم: نظام تشفير من 40 بت سمحت للحكو مة بتصديره. والموضوع هو محض سياسي هذه المرة. إذا تم توجيه أسلوب حشد القوى الذي استخدم في تحليل الرسا، ضد ذلك المفتاح الضعيف الذي كان مدار التفاوض مع اتحادنا شري البرمجيات عام 1992 (ولم يعدل في السنوات اللاحقة، بالرغم من الوعود التي قطعتها الحكومة)، فإن ذلك المفتاح مصيره السقوط، ولسوف يكون من الواضح الجلي الحاجة إلى نظام تشفير أقوى.

وبعد أن طرح أحد زعران الشّيفرة فكرة «حلقة لتفكيك المفتاح» حثّ تيم ماي على القيام بعمل، معتقداً أن قدرة «وحدة المعالجة المركزية CPU في هذه القائمة» قابلة ستغلال على نحو مؤثر في تفكيك المفتاح خلال ستة أشهر (المدة ستة أشهر نتيجة التخمين. ولكن مقارنة الجهد الحسابي اللازم لها بتفكيك خوارزمية الر سا هي أشبه بالمقارنة بين المفتاح والبرتقال لـ ستقصاء مدى المفتاح مقابل تحليل العوامل).

كتب آدم باك، وهو شاب في الخامسة والعشرين يدرس علوم الكومبيوتر بجامعة كستير في إنجلترا: «تمهلوا فلقد كنت قطعت فترة في هذا العمل...». وكان قد بدأ بكتابة النصوص، بُعيد اطلاعه على أول إرسالية، ليتيح للناس المشاركة في تفكيك الشّيفرة جماعياً. كان يدرك ما هو بصدده، لأنه كان يعالج قبل حين الخوارزمية آر سي ـ 4 ـ الشّيفرة الحقيقية التي نفذت التشفير في 40 بت المسموح بتصديرها من الحكومة ضمن برامج مايكروسوفت واللوتس.

إن الهجوم بالقوة الغاشمة على شيفرة منفذة ككتلة مثل الآر سي ـ 4 أو معيار تشفير البيانات يتطلب من المفكّك معالجة النص بكل تركيبة رقمية ممكنة. كذلك يتطلب العثور على المفتاح البحث في كل مجال الاحتمالات؛ وهناك في حالة المفتاح المركب من 40 بت، حوالي تريليوان حتمال مما يكفي

لتشغيل دستة من الكومبيوتر أياماً بطولها، ليتم العثور على المفتاح. وهاك ما كان يدور في عقل آدم باك: جهد يقوم به عدة أشخاص، ولكل منهم جزء من حيز المفتاح يقوم باختباره، ثم يتوسع في البحث. وتستمر هذه العملية حتى يعثر أحدهم على المفتاح. فيقوم بإرسال نصوصه إلى صفحة الشبكة فيتنادى مجموعة منا لمتآمرين من مختلف أنحاء العالم بسرعة للاجتماع. وفي النهاية يحاول تسعة وثمانون من زعران الشّيفرة العثور على مفتاح من 40 بت في برنامج مايكروسوفت Access أكسيس القائم على إدارة قاعدةالبيانا ت.

ولكنمحاو لة التدخّل في برنامج مايكروسوفتأكسيس فشلت؛ إذ لم ينجح أي من ملايين المفاتيح المحتملة في فكّ الرسا لة، بالرغم من «اجتياح» كامل حيز المفتاح. وتبين أن من حاول التلصص قدا صطدموا بنقطة فنية حالت دون حصولهم على النّص العادي، (يقول باك في هذا أن المشكلة كانت في الافتقار للمواصفا ت، فلم نكن نعلم الشكل الذي كان عليه الملف).

ومع ذلك فقد خرج زعران الشّيفرة، من الهجوم الفاشل على برنامج مايكروسوفت بشيء من برمجية اختراق جماعي، أيتنظيم فضفاض إنما مثابر في جهوده ورغبة مستمرة في الكشف عما كانوا يعتقدون أنه غش يدعو للأسف في التشفير المُعد للتصدير. ثم وقع زعران الشّيفرة عندئذ على هدفأ فضل لشنّ هجوم بالقوة الغاشمة: نيتسكيب.

في عام 1993 جلس طالبان من جامعة إيلينيو، يتبادلان الحديث في أحد المقاهي، وكان حديثاً لميغيّر مجرى الشبكة العالمية، الإنترنيت، التي مضى عليها اثنان وعشرون سنة، وحسب وإنما كان له أعمق الأثر في الأخذ بالتشفير. كان أحدهما طالب جامعي قصير القامة بدين يدعى مارك اندريسين، وقد عرف حديثاً بنظام جديد على الإنترنيت أطلق عليه مخترعه عن رعونة اسم وورلد وايد ويب World Wide Web (شبكة العالم الفسيح)، وكان ذاك المخترع يدعى تيم بيرنرز ـ لي، وهو عالم كومبيوتر بريطاني يعمل في سويسرا. وكان نظام ويب

هذا طريقة فذة للطباعة والوصول إلىٰ معلومات عبر شبكة الإنترنيت، غير أنه لم يكن يأخذ بهذا النّظام سوى قلّة من طائفة الفنيين الاختصاصيين. ولكن أندريسين وجد في هذا النّظام إمكانيةأو سع للإفادة منه. وعبّر عن ذلك بما قاله لزميله إيريك بينا: إذا ابتكر أحدهم «متصفحاً» زلقاً ليجول في فضاء المعلومات الذي تكونبفعل حشد من الناس الذين يشاركون في نصوص وصور وأصوات على شبكة الويب فسوف يكون منلأ يسر استخدام الإنترنيت ذاتها وتصبح طريقة أفضل للحصول على المعلومات. وقد ابتكر هذا الثنائي، وكان كلاهما يعمل في مركز الكومبيوتر العملاق في الجامعة، برنامج موزاييك، وهو أول متصفح ويب ضخم؛ وتتجلّى أهميته في أنّه بات يتيحللنا س الحصول على كل المعلومات الرائعة من «صفحات» الويب اليدوي بالضغط على الفأرة، بدلاً من الاضطرار لاستخدام أوامر قديمة وتناول حساء مثير للحيرة من مختلف حروف الهجاء والكلمات المركبة. وقد اكتسب هذا البرنا مج فوراً صفة الظاهرة. وكان استخدام موزاييك يثير أشد الحماس بسبب المشاركة في تجربة ضخمة في مستقبل تبادل المعلومات. وسرعان ما أخرج فريق من المهتمين بجامعة إلينوي نسخاً من البرنامج تناسب كل منبر حسابي تقريباً. وأخذ ملايين النلس يتداولون هذه النسخ، وهبت آلافا لمواقع على الشبكة لاستغلال هذا الجمهور.

في عام 1994 كان لأندريسين أن يتناول فنجاناً آخر من القهوة، ويكون له أثر، وشاركه فيه هذه المرة، رجل أعمال له استثمارات في سيليكون فالي هو جيم كلارك. وكان هذا لمدير العام لشركة سيليكون جرافيكس، وقد غادر مكتبه ليحبث عن فكرة جديدة لشركة نا شئة، فوقع عند هذا الطالب الفتى على أحد أغنى المناجم في التاريخ. وكان كلارك الذي لم يكن محيطاً حتى ذلك الحين بفورة الشبكة، سريعاً إلىٰ إدراك الإمكانات التجاريةالكا منة فيها، فأمسك بأندريسين ذاته ومعظم فريق إلينوي ليطلق شركة موزاييك كميونيكا يشنس. (ولما اعترضت الجامعة على هذا الاسم استبدله كلارك بـ «نيتسكيب»

Netscape . وكان الغرض من هذهٔا لشركة، تطوير نسخة محسّنة من المتصفح يدعى الجوال Navigator، مع برمجية بـ«مخد مات» الشبكة تسمح بإجراء لصفقات والمعاملات التجارية على الشبكة. وكان ثمة مكوّن ينقص هذا التصميم، هو الأمن. فإذاكا نت الشركات تعتزم بيع منتجاتها وإجراء لصفقات التجارية على شبكة الإنترنيت فإن الزبائن سوف يطالبون بالتأكيد، بحماية سرّيّة مراسلاتهم. وهذا العمل المثالي للتشفير.

كان كلارك يعرف لحسن الحظ، شخصاً يعمل في هذا الحقل ـ جيم بيدزوس، فاتصل به؛ ولما انتهت المفاوضات بينهما، كانت نيتسكيب قد امتلكت ترخيصلًا ستخدام خوارزمية رسا والحصول على مساعدةا لشركة في تطوير معيار للأمن لشبكة الويب: قاعدة تعتمد على مبدأ المفتاح العام تُعرف بـ «طبقة الممرات الآمنة» Secure Socket Layer. وقامت نيتسكيب بدمج هذه في برمجياتها، وهي تكفل للملايين من الذين تتوقع الشركة أنّهمسو ف يستخدمونها التمتع تلقائياً بمزايا التشفير كما تصوره ميركلي وديفي وهيلمان وقام على تنفيذه رايفست وشامير وأدليمان. فيكفي أن يضغط المرء على الفأرة ليدخل مستخدم نيتسكيب حا لة التشفير، فتظهر على الشاشة رسا لة تنبئ بأنالمعلو مات المسجلة كلها با تتفي أ مان. وفي غضون ذلك تكون عمليات التشفير والتثبت من هوية المرسل بطريقة الرسا جارية على قدم وساق.

كان جيم بيدزوس صلباً كعادته في المساومة مع نيتسكيب، وتم لا تفاق على أن تنال شركة الآرإ س إيه مقابل الخوارزميات نسبة 1 بالمئة من الشركة الجديدة. وفي منتصف 1995، قدمت نيتسكيب أفضل عرض في تاريخ وول ستريت حتى اليوم بحيث جعلت حصة الآر إس إيه من الشركة الجديدة تزيد عن 20 مليون دولار. (وجد بيدزوس العرض جيداً لشركة كانت قبل وهلة توشك على الانهيار، حتى تلقت 100 ألف دولار سلفة من لوتس).

كانذ لك بعيد عملية الإدخال والمعالجة والإخراج IPO التي أكسبت

العيون بصيرة، حين بدأ أحد زعران الشّيفرة يدعى هال فيني بالتدقيق في حال الأمان الذي تتمتع به نيتسكيب. وكان فيني، وهو مبرمج يعمل في سانتا بربارة وله مساهمة في تطوير «منتهى السرّيّة» مهتماً بشكل خاص باستخدام الكريبتوجرافيا في التجارة الإلكترونية، وبات ملمّاً بـ «طبقة المطرت الآمنة». وقد طرحت نيتسكيب، نسختين من الجوال التزاماً منها بأنظمة التصدير: نسخة محلية ذات مفتاح من 128 بت لبرنامج آر سي ـ 4 لمشفر ونسخة من 40 بت معدّة للتصدير.

ولقد طرح فيني على نفسه تحدياً يتمثّل بتفكيك رسالة مشفّرة بواسطة ذلك المفتاح الأضعف. فوضع مشروع صفقة نيتسكيب ـ كما لو كان عميلاً من العملاء ـ ثم استخدم التشفير في نسخة التصدير. ويقول في شرح التجربة: «ما قمت به أساساً هو الاتصال بالنيتسكيب وإحدى صفحاتها المأمونة وشرعت في طباعة بيان انتقيته عشوائياً وطلبت فيه قمصاناً رياضية أو شيئاً من هذا القبيل». ثم التقط البيانات المشفّرة وضمنها في تجربة التحدي:

التاريخ: الاثنين 10 تموز/ يوليو 1995 16 ـ 13: 52 ـ 700

من: هال < hfinney@shell.portal.com

إلى: < Cypherpunks@toad.com

الموضوع: لنحاول تحطيم المفتاح SSL RC4

لما تبين أن تفكيك برنامج مايكروسوفت أكسيس فاشل فيمكن أن يكون البديل محاولة تفكيك الـ 40 بت آر سي ـ 4، المستخدم في نظام نيتسكيب SSL طبقة الممرات الآمنة للتشفير المُعد للتصدير...

من بريطانيا، قبلت مجموعة آدم باك التحدي. و مع أنّه كان يبدو أن خطة باك الأصلية، كانت توزيع مجال المفتاح بين عدة أشخاص، غير أنّه انتهى إلى قبول اقتراح مبمرج أو سترالي بالقيام بنصف بحث. أما بقية مجال المفتاح

فيتولاه متطوعون لكل واحد نصيب بجزء منه. ولقد نشب اضطراب بين الفتيين يومئذ مما أدّى إلىٰ تباطؤ العمل بضعة أيام.

أثناء فترة تباطؤ العمل هذه، أخذ داميين دوليجه يتساءل عن سبب هذا البطء. كان دوليجه عالم كومبيوتر في السابعة والعشرين من العمر، وقد نال شهادة الدكتوراه قبل بضعة شهور ويعمل باحثاً لدى إينريا INRIA، مخبر الحواسب التابع للحكومة الفرنسية. كان مكتبه يقع في أحد الأكواخ في ما كان ذات يوم قاعدة للحلف الأطلسي على بُعد بضعة أميال من فيرساي. وكان له عناية شخصية بالتشفير، إذ بلغه شيء من النفور من الأساليب التي تلجأ إليها الحكومة قمع قابلية المواطنين للتواصل فيما بين بعضهم البعض، واعتقد أنّه إذا استطاع أحدهم تفكيك إحدى منظومات التشفير ذات الأربعين 40 بت، التي أصبحت عرجاء بشكل مصطنع فسوف يكون ذلك ضربة بالقوة الغاشمة المهينة على المجتمع. كذلك ذهب به الظن إلىٰ أنه بعد النجاح في تفكيك الخوارزمية رسا 129، سيكون بالإمكان تنفيذ عمليّة التفكيك في غضون أسبوعين أو ثلاثة. لذلك أخذ يتساءل في خلده عن حقيقة ما حدث خلال الفترة ما بين التحدي الذي طرحه فيني وحل هذا التحدي.

كان لدوليجه القدرة على الوصول، بحكم عمله كباحث في مخبر الإينريا، إلىٰ محطة العمل في مكتبه الصغير، وشبكة الكومبيوتر كلها، بما فيها الكومبيوتر ماسبار الضخم، أيضاً.

وكان هذا الباحث قد درس مواصفات طبقة الممرات الآمنة وطلع ببرنامج صغير يسمح للكومبيوتر اختبار المفتاح المحتمل بسرعة، ثم قام بتكييف البرنامج على نحو يجعله قابلاً للعمل في مختلف الآلات المتوفرة في شبكة اينريا، وبعض الآلات لدى الجامعات القريبة، ومعهد البوليتكنيك، وكلية الدراسات العليا.

ومن ثم بدأ بتنفيذ هجماته المتلاحقة. فكان كلما انحرف أحد العاملين

في إينريا عن كومبيوتره أَو كومبيوترها ينبري برنامج دولجيه في غضون خمس دقائق، و يتناول ربما 10 آلاف مفتاح في ثانية. فكان يكفي المستخدم أن يلمس المفاتيح حتّى يستعيد سيطرته على الآلة. ولم يكن هناك من شكوى.

ولقد حسب دوليجه، أنفرصته ستكونأ فضل في العثور على المفتاح، إن بدأ من نهاية مدىا لمفتاح ورجوعاً إِلىٰ الأمام: «لقد اعتقدت أن زعران الشّيفرة يبدأون من البداية، فبدأت أنا من النهاية». فجهز شبكته للعمل في يوم الجمعة المصادف 4 آب/ أغسطس، وغادرمكتبه لقضاء عطلة نهاية الأسبوع. ولما عاد يوم الاثنين ليستأنف العملا كتشف خطأ في برنامجه. فعاد يجدد العمليّة من البداية. وكان أن أخذت عمليّة معالجة الأعداد تجري على أحسن ما يرام، منذ تلك النقطة، إِلاّ أن الأمر انتهى بدوليجه إِلىٰ عشر نسخ جديدة من البرمجيات، خلال الأيام القليلة لمعالجة ذلك الخطأ في الاتّصالات بين الآلتين. كان البرنامج يجري على ما يرام حين غادر دوليجه عمله يوم الجمعة 11 آب/ أغسطس وكلت ا لعطلةالأ سبوعية تمتد هذه المرة، بسبب مصادفتها مناسبة منتصف الصيف الذي تحتفل بفر نسا كلها، أربعة أيام فتنتهي في 15 آب/ أغسطس. ولكنّه حين تفقد كومبيوتره الخاص في البيت، قبل انتهاء ا لعطلة الانتصافية وجد برنامجه يقدم له رسالة كان ينتظرها.

قال: «وجدت أن الكومبيوتر قد عثر علىا لمفتاح». وإذن فقد تم تفكيك طبقة الممرات الآمنة!

وفي اليوم التالي قاد داميين دوليجه سيارته من منزله خارج باريس عائداً إِلىٰ عمله، واستعاد هناكا لمفتاح من محطة العمل، ثم التفت إِلىٰ تفكيك الرسالة على أكمل وجه. فلما تم له ذلك وجّه رسالة إِلىٰ زعران الشّيفرة، وكا نت تحمل العنوان التالي: «تحدي طبقة الممرات الآمنة: فُكك». وللبرهان على ذلك أرفق رسالته بالنص الواضح الصريحللر سالة المشفّرة. ولقد قدر أولئك الذين يعرفون الرسا 129 أهمية عنوان الشخصية الخيالية التي ابتدعها هال

فيني فيرر سالته المشفرة: السيد كوزميك كومكوات، شركة طبقة القوابس الآمنة المساهمة، يقيم في 1234 (شارع صقرالسمك ا لمتقزز).

وبالرغم من أن فكرة تفكيك شيفرة نيتسكيب، ليس فيه من الناحية الفنية ما يصدم المرء، إذ تفرض رياضيات التشفير، أن يتهاوى المفتاح الضعيف حين يتعرّض لهجوم مركّز، فإنّها استولت على مخيلة الصحافة الشعبية. وأصبح دوليجه هدفو سائل الإعلام. ولأن هذا الخرق جرى بعد أسبوع واحد من الفوز المؤزر الذي حظيت به نيتسكيب ولعله كان أعظم نجاح تحقّق في التاريخ في عملية إدخال وإخراج ومعالجة. فقد أبرز بعض الصحفيين هذا الخرق وكأنما يمس أمن المتصفح كله، وليس باعتباره مثالاً على أثر أنظمةا لتصدير التي تأخذ بها الحكومة في إضعاف البرمجيات على العموم. وقد لاحظت نيتسكيب فيرر سالة بثتها عبر موقعها في وقت لاحق من الأسبوع أن دوليجه إنما استطاع تفكيك رسالة واحدة وحسب، واستغرق في ذلك (MIPS 64 عاماً) أي توجيه 64 مليون أمر في الثانية من السنين، وقدرت تكاليف عمليّة التفكيك 10 آلاف دولار. ولكن دوليجه نفّذ العمليّة كما قال في أوقات لعطلة والراحة ودون أن يتكبّد أية نفقة. غير أن موقف نيتسكيب كان أرسخ حين لاحظت أن النسخة المباعة في الأسواق المحلية من برنامج المتصفح الجوال Navigator اعتمد على مفتاح أفضل يتكون من 128 بت؛ وقالت في رسالتها: «يجب أن يكون الكومبيوتر اللازم لتفكيك مثل هذه الرسالة، بتريليون تريليون ضعف قوة الكومبيوتر المستخدم في فكّ شيفرة الرسالة آر سي ـ 4 ـ 40».

وكا نت هذه النقطةعينها، هي جوهر الأمر عند زعران الشّيفرة: وهو أن برامج التفكيك المعدّة للتصدير ضعيفة دونما مبرّر.

ولكن زعران الشّيفرة لم يكونوا قد أنهوا الأمر ونيتسكيب. ففي بيركلي، وجدنا اثنين من طلبة الدراسات العليا يتحولان إلىٰ تحليل الشيفرة، وهما إيان جولدبرج وديف واجنر، وكلاهما في الثانية والعشرين من العمر، وقد وجد

هذان، ما يحملهما على التطفّل على النيتكيب، أي سفينة القيادة في أمن لإ نترنيت. وكان كلاهماقد قصر عن الهجمات بالقوة الغاشمة، كان جولدبرج قد انتقل حديثاً من موطنه كندا إلىٰ كاليفورنيا بينما كان واجنر قد قدم لتوه بعد نيله إجازته الجامعية من جامعة برنستون. وهكذا أخذ الاثنان يختبران شكلاً مختلفاً من الهجوم، وكان أقرب للتوصية الثانية التي أوردها روبرت موريس: ابحث عن النص الأصلي الصريح. فهل يحتمل أن يكون فريق الأمان في نيتكيب قد ارتكب خطأ بسيطاً، ولكنّهفا حش، في تنفيذ برنامجهم، مما يكشف للمتنصتين ما قد يبلغ ملا يين الصفقات التجارية التي تتم عبر الأَجهزة الإلكترونية؟ إن ذلك مستبعد. ولكن المرء، كما ألمح موريس، يظل جاهلاً إلىٰ أن يبحث من حوله حتّى ينجلي له الأمر.

وهاكم متى رأى واجنر السر. فقد وجد الرجل أن التعليمات لمولد الأعداد العشوائية، مدفونة في رموز النيتكيب وهذا جزء هام من أي نظام تشفير راقي. الجزء الحاسم في التشفير لتعمية الرسائل الذي يجعل النص المشفر خلواً من لإ شارات التي تنم عن نمط معين يرشد محلّل الشيفرة إلىٰ ثغرة في الرسالة. فمن المعلوم تماماً أنا فتقارا لعشوائية الحقّة ضعف يستطيع محلّل الشّيفرة استثماره متى وقع عليه. لذلك كان من الضرورة بمكان توفّر مولد أعداد عشوائية متين، بحيث يجعل دولاب روليت حرو ف الهجاء يدور على أفضل ما يكون الدوران. كذلك ثمة جزء هام في مولد الأعداد العشوائية يتجلّى في استخدام «بذرة» غير متوقعة، وهي عدد تبدأ به العمليّة لعشوائية. فلما كانت الكومبيوتر تجري مجراها ذاته كلما تحرّكت ـ وهي في ذلك عكس النرد ـ فإنّه من الضروري أن تبدأ ببذرة لا يملك الخصم المحتمل أنيحد س ماهيتها بأي حال. وغالباً ما تشتمل أساليب تنفيذ هذا استخدامإ حصائيات غريبة غير مألوفة من عالم الواقع ـ وضع الفأرة مثلاً، أو أي أمر لا يمكن لعدو معرفته.

أما نيتكيب فقد أهملت، كما تبين، هذه الحكمة. فما أن دقّق ديف واجنر النظر في الشّيفرة، حتّى برز له الخطأ. والسر في ذلك أن نيتكيب استمدت بذرة مولد الأعداد العشوائيَّة من ثلاثة عناصر: الوقت المدون في الرسالة وشكلين في تعريف المستخدم يعرف الأول باسم هوية العمليَّة وهوية الأم. وتلكم هي الكارثة. ذلك أنه يكفي الخصم أن يدير الكومبيوتر بضعة دورات ويشغل عدداً من خلايا الدماغ أقل من دورات الكومبيوتر ليعثر على القسم الأول من البذرة: فمن اليسير على المرء أن يعرف العدد المحدود من أوقات اليوم. وغالباً ما يكون من اليسير على المرء العثور على أرقام التعريف، في كلتا الحالتين، خاصة إذا كان ثمة من يشترك مع آخرين في المخدم ذاته، كما هو الحال غالباً في بيئة مثل الإنترنيت. يقول جولدبرج: إذا كان للمهاجم سجل للآلة التي لديك، غدا الأمر بسيطاً. ولدينا هنا في جامعة بيركلي آلاف المستخدمين. فإذا كان هناك من يستخدم النيتكيب، استطاع اكتشاف الهويتين». غير أنه بوسعك اكتشاف هاتين الهويتين ببساطة، وإن لم تتوفر لك هذه الميزة. وجدير بالذكر أن أرقام الهويتين المطلوبتين لا يزيد طولهما عن خمسة عشر بت، وهذا رقم يسهل مهاجمته بالقوة الغاشمة.

ولقد أمضى واجنر وجولدبرج العطلة الأسبوعية في وضع برنامج لاستغلال هذا الضعف، ولما كانت ليلة الأحد جلسا لامتحانه، واستطاعا اكتشاف المفتاح السري في أقل من دقيقة، بالتركيز على الثغرة الضخمة في برنامج النيتكيب. ووداعاً لأمن الشبكة، وبعث جولدبرج بالنتيجة إلى قائمة زعران الشّيفرة. وقال معلّقاً: لم نكن نتوقع أن تحظى هذه الواقعة بكثير من العناية من الصحافة. ويا لسذاجة الفتى. لقد كان بين قراء تلك الرسالة مخبر في صحيفة النيويورك تايمز، فقام هذا بنشر الخبر. فلما ظهر في صحيفة الوقائع أخذ الفضوليون والصحفيون يتقاطرون على هذين الطالبين، وهما لما ينالا شهادة التخرّج بعد. وكان من بين ما صرح به هذان الطالبان، تلك الملاحظة

التي أدلى بها جولدبرج، وتحمل على التفكير: «إننا شابان طيبان، و لكننا لا ندري إن كان هناك من الأشرار من وقع على هذه الثغرة مثلما وقعنا نحن عليها».

كانت هذه سقطة شنيعة، على العكس من عمليّة فك الشّيفرة الأولى على النيتكيب، حيث كان يمكن لهما القول أن رسالتهما المشفرة كانت على قدر عظيم من المنعة لولا القيود التي فرضتها الحكومة. ذلك أنك لم تكن بحاجة هذه المرة إلىٰ رصد شبكة مؤلفة من عدد كبير من المحطات، أولا صول إلىٰ كومبيوتر ضخم لتتمكّن من حل الشّيفرة. فهناك حالات معينة لا تحتاج فيها إلاّ لدقيقة واحدة من متعة معالجة الأرقام. قال مايك هومر، نائب رئيس نيتكيب لشؤون التسويق: «إن المهندسين لد ينا ارتكبوا خطأً في تنفيذ البرنامج».

و لقد أرخى هذا الخطأ ظلالاً من الشك، حول مبلغ الأ مان، الذي توفره شر كة برمجيات الإنترنيت الرائدة. وقد حمل هذا عالم الشيفرة بروس شتاينر على التساؤل: «إذا كانت نيتكيب قد ارتكبت هذا الخطأ، فقد تكون هناك أخطاء أخرى أيضاً». ولكن السؤال الملحّ الذي يحتاج إلىٰ إجابة هو إن لم تكن نيتكيب مأ مونة، فأ ين الأ مان إذن؟ والسبب في السؤال هو أن نيتكيب كانت تبذل قصارى جهدها لحماية مستخدِميها. وإذا كان يمكن اختراق برنامج الجوال بهذا القدر من اليسر، فأي أمل هناك إذن للآخرين بالفلاح؟

لكن لتلك الواقعة جانبها المشرق أيضاً: فبوسعك أن تذهب مذهب القول أن الأمور سارت على الوجه الأ فضل، لأن زعران الشّيفرة كشفوا ضعفاً في النّظام لو ضحاً فعمدت نيتكيب إلىٰ تلافيه فوراً. لكن الدرس الذي رسخ كان أشد قتامة إلىٰ حد ما. فمع انتشار الإنترنيت أخذ الجمهور يعتمد حقاً على الكومبيوتر المرتبطة ببعضها في عقد لصفقات التجارية وتخز ين المعلومات، بدءاً من شراء الكتب فشراء وبيع الأسهم إلىٰ تسديد الفواتير. وشرعت مصالح تجارية تخطط، لعرض السجلات التجارية على شاشات شبكات الكومبيوتر.

ولكن الأمان ظل، في أحسن الأحوال، مقلقلاً. وكان ثمة سبب عظيم واحد يزداد جلاء باطراد فيه تفسير هذا القصور، وهو العرقلة المستمرة من جانب حكومة الولايات المتّحدة. وفي حين حاولت الحكومة الترويج للمقراض ووديعة المفتاح كحل مفضل للمشكلة، ظلت الإنترنيت تحث الخطى ـ دون جهدمنظم لتوفير ما تحتاج إليه من أسباب الحماية.

في منتصف التسعينات وجد أولئك الذين كانوا يجهدون لبلوغ عصر جديد من حماية الشّيفرة عصر يوفر الأمانللإ نترنيت ووسائط الأتصالا ت الإلكترونية الأخرى أنفسهم تحت وابل متزايد منا لنيران. وبدا أن أولئك المسؤولين عن القوانين والمؤسسا ت الاجتماعية كانوا قادرين على فعل الكثير، لحمل المجددين في التشفير على إدراك أن لأفعالهم عواقب، وإن عجز المسؤولون هؤلاء عن قطع أسباب التقدم أمام الرياضيات والهندسة. وأصبح ا لسؤال عندئذ إلىٰ أي حد يمكن للحكومة، أن تمضي في تهديدها بهذه ا لعواقب.

بالنسبة لراي أوزي، في شركة لوتس، لم يكن تلقي مثل هذا الدرس في قدرة السلطة بالأمر اللازم، فقد كان الرجل ملتزمًا لعمل في إطار النظام القائم. (فضلاً عن ذلك كانت لوتس قد انضمت إلىهؤ سسة رسمياً، في عام 1993، حين قامت شركة الآي بي إم بشرائها، بمبلغ ثلاثةبلا يين دولار). وكان أوزي قد أصبح في السنوات التالية لتبنيه المبكر لخوارزمية رسا، شخصية ذات صوت مسموع في معارك التشفير، في شهاداته أمام الكونجرس والزيارات التي كان يقوم بها للشخصيات البارزة في الحكومة. ومع أنّه كان او ضحاً في انحيازه إلىٰ التشفير إلاّ أن ما كان يتحلى به من كيا سة واستعداد للأ خذ بالرأيا لمعارض بعين الاعتبار أكسباه احترام حتّى المتشددين في موضوع التصدير. وقد دأب الرجل، وهو غير قادر على انتظار

الحكومة لتحرير قوانينها، على البحث عن طُرق جديدة لتجاوز العقبات التي تضعها أنظمة التصدير وتعرقل التجارة.

بعيد تفكيك رسالة نيتكيب، أخذ زبائن لوتس نوتس يزدادون ضيقاً باستخدام برنامج التشفير بـ 40 بيت من آي بي إم المسموح بتصديره إلى الخارج. وكانوا يريدون معرفة السبب في بيع الزبائن الأمريكيين نسخة ذات مفاتيح مكونة من 64 بت، وهي بملايين المرات أصعب من النسخة المصدرة إليهم التي يمكن تفكيكها على يد حامل شهادة دكتوراه وقعت بيده على غير اتفاق هذه الرسالة في ضاحية من ضواحي باريس. (وفي تلك الأثناء كانت الشركات التي لم تشأ، مثل مايكروسوفت، أن تقدِّم المُنتَج ذاته بنكهتين، تقدم لزبائنها كافة برنامج التشفير الأضعف. وقد أدَّى هذا العقيم إلى خفض قيمة خط الإنتاج كله عند أولئك الذين ينشدون التشفير، فالتفت بعض هؤلاء الزبائن إلى الشركات الأجنبية، التي تستطيع بيعهم برنامج التشفير الأقوى بصورة قانونية).

في عام 1995 طلع أوزي بما بدا أنه تسوية مقبولة، على الأقل في المدى القصير: وكانت هذه تقوم على حيلة رياضية لتلبية متطلبات وكالة الأمن القومي. وتتضمن خطة أوزي، نسخة أزهد ثمناً من المقراض، على ما كان عليه من النفور منه، ومع ذلك فقد ظلَّت لوتس تبيع نسختين من النوتس، إنما تختلفان عن النسخ الأخرى من حيث أنهما ببرنامج تشفير من 64 بت. غير أن النسخة الدولية تحمل معها هدية صغيرة لوكالة الأمن القومي: مجال دخول الأمن القومي NSAF، ويتألف من 24 بت من البيانات المشفَّرة التي لا يملك تفكيكها سوى وكالة الأمن القومي وحدها. وكان هذا البرنامج مشفراً بالمفتاح العام للوكالة، بحيث لا يستطيع تفكيك ذلك المجال إلاَّ أهل «القلعة» حصراً. وجدير بالذكر أن الرسائل المشفَّرة وفق برنامج النوتس يتقلص، بعد استخدام وكالة الأمن القومي مفتاحها الخاص، لتفكيك برنامج مجال دخول الأمن

القومي ذي الـ 24 بت، من نص مشفَّر من 64 بت، إلىٰ نص مشفر آخر من 40 بت. وكان تفكيك الشّيفرة المتبقية تتطلب القدر من العمل ذاته الذي تتطلبه الرسائل المشفَّرة بمفاتيح بطول 40 بت المصدرة مع النّظام القديم. ولكن بما أن التشفير كان على وجه الإجمال أقوى من قدرات المهاجمين جميعاً، عدا وكالة الأَمن القومي ـ وكان مصدر القلق لدى معظم المستخدمين المهاجمين الآخرين، كالمخبرين وجوا سيسرا لصناعة ـ فقد اعتقد أوزي أن هذا الحل ربما كان مفيداً في المدى القصير.

ولقدتقد مت لوتس بطلب براءتين لابتكارها هذا، وعرفته باسم «نظام وطريقة شيفرة عامل التشغيل التفاضلي» في كانون الأول/ ديسمبر 1995 وأدمجته في النسخة الجديدة من برنامجها نوتس ـ الإصدار 4 Notes Release 4. وكان أول حديث أدلى به أوزي عنه علناً في كانون الثاني/ يناير 1996، في مؤتمر لشركة آر إس إيه داتا سيكيوريتي، في سان فرانسيسكو. وكان هذا المؤتمر أحد المناسبات التي يقيمها جيم بيدزوس لعرض الأفكار الجديدة في لتسويق. فقد دأبت إدارة لشركة منذ 1990 على جمع زبائن الشّيفرة التجارية في منطقة خليج سان فرانسيسكو، في إطار ندوات ومعرض صغير يستعرض فيه البائعون بضائعهم على مدى بضعة أيام. وكان هذا لمؤتمر قد بدأ كاجتماع يضم قلة من الحرة والحواة في فندقسو فيتل بالقرب من مكاتب الشركة في رد وود سيتي ثم تطور إلىٰ حشد من عدة آلاف وبات يعقد الآن في فندق ضخم بالقرب من ساحة يونيون سكوير. وقد حازت كلمة أوزي على اهتمام واسع كما أثار بين المستمعين قدراً من الضيق، و حمل البعض علىٰ لتساؤل، إن كان المصمّم المبتكر خلف برمجيا ت النوتس قد تخلّى عن الكفاح واستسلم.

لا، إنه لم يستسلم؛ بل كل ما في الأمر أنّه كان منشغلاً بمتابعة جدول أعمال، أكثرد قة مما يشغل الآخرين، وعبَّر عن ذلك بقوله: «لقد كنت أسعى

إلىٰ تحريك الأمور». وكان هدفه يومذاك، أن يضرب إسفيناً بين الإدارة ووكالة الأمن القومي. وقد ذهب بها لفكر يومذاك مذهب أنه متى تراجع آل جور عن فكرة سيطرة الحكومة علىترتيبا ت الإيداع فلن تجد وكالة الأمن القومي مسوغاً عظيماً لأفكار ما بعد المقراض. ذلك أنه إذا أخذ للنا س، بإيداعا لمفاتيح في مستودعات خا صة فسوف تضطر الـسلطات عند ئذ إلىٰ الحصول على أمر قضائي حتّى تـستطيع وضع يدها على هذه المفاتيح. وفي هذا ما يضر بأسلوب عمل الوكالة، فهل تعمل بالسر ويحظر عليها رصد ما يجري داخل البلاد. وبالتالي فإن الخطة التي اقترحهاأوزي تنطوي على شيء من الإغراء، من حيث أنها تسمح لها بأن تحقّق قصب السبق في عمليّة تحليل الشيفرة. (ذلك أنّها لن تحتاج في هذه الحالة إلىٰ أمر قضائي للحصول على مفتاح فك شيفرة من 24 بت). وإذن فقد كانت خطة أوزي بعيدة كل البُعد عن خذلان دعاة التشفير، بل هيا ستراتيجية تخريب لدفع وكالة الأمن القومي والإدارة إلىٰ الاختلاف حول طُرق معالجة متعارضة. وقد أمل أوزي بأن تفيلا لصناعة من حالة فوضى الآراء لتنفذ حلها الخاص.

ولكن أوزاي كتشف، قبل أنيهنئ نفسه لحصافته، أن الحكومة لم تكن لتفتقر إلىٰ وسائلها الخاصة للتعامل معأ مثال هذه الاستراتيجيات. ففي 30 كانون الأول/ ديـسمبر 1996 تلقى أوزي وشريكه المخترع تشارلز كاوفمان رسالتين وعلى الغلاف عبارة «أمر سرّي». وأفادت الرسالتان أن طلبيهما المتعلقين ببراءة الملكية الفكرية «يتضمنان موضوعاً قد يؤدي الكشف عنه دون تصريح، في رأي الجهة المعنية في وزارة الدفاع إلىٰ ضرر فادح ينال من الأمن القومي». (لوحظ فيا لفراغ المتروك لإشارة المسؤول الحكومي عن براءة الملكية الفكريةعلا مة X إلىٰ جانب كلمة «الجيش»). وقدحذّر ت الرسالة من أن الكشف عن موضوع الطلب دونما تصريح لأية جهة يجعل المخترعين، وشركة آي بي إم، عرضةللعقوبا ت التي تشمل الـسجن. وفي النهاية أعلم

الرجلان بأنّه يتوجب عليهما إتلاف النسخ موضوع الطلب، على النحو الذي يمنع الكشف عن محتويات الوثيقة أو الإفادة منها».

أدرك أوزي، فور تلقي الأمر يوم 7 كانون الثاني/ يناير 1996، أن الامتثال للأمر ينطوي على مشكلة. فهو قد سبق له أن خاض في تفاصيل المشروع في عدة مناسبات، كما تم توزيعه فعلاً على حوالى ستة ملايين شخص يستخدمون برنامج اللوتس نوتس، نصفهم خارج الولايات المتّحدة. فأسرع إلىٰ إخطار رؤ سائه في الشركة بما بلغه، وأخذ هؤلاء في التفكير بالعواقب المترتبة على اعتبار أحد أكثر برمجياتهم شعبية في العالم سراً مِن سرار الحكومة.

ولعل أفضل ما قام به أوزي أنه دفع بصديق لهللا تّصال بنائب مدير وكالة الأَمن القومي بيل كرويل، الذي ضحك كما ذكر، حين سمع بالخبر وقال للصديق أنهسو ف ينظر في الأمر. وفي 9 كانون الثاني/ يناير اتصل كرويل بأوزي، وقال له أن في لأمر خطأ سوف يصار إلىٰ إصلاحه. وبالفعل أُخبر محامو شركة آي بي إم حين اتصلوا بمكتب براءات الملكية الفكرية بأن الأمر السري قد طوي، ثم ورد كتاب بالفاكس بهذا المعنى يؤكد الكلام الشفهي الذي بلغهم أثناء المكالمة الهاتفية. وهكذا لم يعد راي أوزي وشريكه المخترع وآي بي إم معرضين للمقاضاة عن ستة ملايين مخالفة لقانون سرية براءات الاختراع. ولكن بعد أن تنفس الجميع الصعداء وجدوا الأمور ما تزال على حالها. فإذا كان هذا المآل الذي ينتهي إليه مزيعمل على خد مة زيا ئنه بروح وديعة المفتاح، فما هو مصير أولئك الذين يتصدون للحكومة صراحة؟

لقد كان جواب هذا السؤال عند جيم بيدزوس. ففي الوقت الذي اتخذ فيه أصرح موقف علني في معارضة الحكومة ـ فقد ذهب به الأمر إلىٰ حد توزيع ملصقات تحثّ الشعب على «إغراق المقراض»كا نت العلاقة بين شركته ووكا لة الأَمن القومي تتدهور باطراد. وبالرغم من أنّه لم يكن لديه أي دليل مادي على أن هاتفه كان يخضع للمراقبة فقد حسب بأنه تحت المراقبة.

ولعل أشنع المواجهات كانت ما حدث في نيسان/ أبريل 1994، أثناء اجتماع مع ثلاثة من المسؤولين عن قضايا التصدير في وكالة الأَمن القومي، وكان لبيدزوس معهم جميعاً صراع منذ سنوات. وكان من هؤلاء الثلاثة امرأتان له بهما قدر من الثقة، أما الثالث فكان رجلاً ينطوي على مقت لا ريب فيه لبيدزوس وشركته.

ولما وجد بيدزوس، فريق وكالة الأَمن القومي لا يطرح أية قضايا محددة لفتح باب التفاوض معهم، استغل المناسبة ليحاضر فيهم في موضوع المقراض، فقال أنه لن يجد من يقبل عليه، ووصفه بالنِّظام الحافل بالعيوب وإلخ. ولاحظ بيدزوس أن الرجل بين جماعة وكالة الأَمن القومي، بدأ يزداد ضيقاً بحديثه. ثم تكلم في النهاية، وخاطب بيدزوس قائلاً: إن صادفتك في ساحة وقوف السيارات فلن أتردد في دهس مؤخرتك حتَّى تستوي مع الأرض.

ويذكر بيدزوس أنه صعق لما سمع، لكنَّه قال في النهاية مخاطباً الرجل: «سوف أمنحك فرصة لسحب كلامك أو الاعتذار. ولكن هذا استمر في الضغط وصاح هائجاً: «إني جاد في ما قلت. لكنك لم تستوعب ما قلت، أمْ لعلك استوعبت الكلام؟».

هل كان بيدزوس يتلقى تحذيراً رسمياً، ما يعادل قبلة المافيا على الشفتين من السياج الثلاثي؟ هل يجب عليه أن يتجنّب ساحات وقوف السيارات؟ لقد خالجه شعور بأن الرجل كان ينفث عن غضبه وحسب، إلاَّ أنه لم يشأ أن يدع التهديد يمضي دون رد. فأخبر أحد الصحفيين بما كان، وإذ بالقصة تظهر في إحدى الصحف المحلية. ثم لم يمض إلاَّ وقت قصير حتَّى تلقى مكالمة من رئيس ذلك الموظف في وكالة الأَمن القومي يعتذر فيها عن تلك الحادثة. ولقد راود بيدزوس شعور بأن الوكالة تريد منه ترك العمل، وإن لم تكن حياته في خطر.

ولكن بيدزوس شعر بالارتياح مع ذلك، إذ لم يعد تحت وطأة التهديد

بالمقاضاة. فهذا المصير كان محفوظاً للرجل، الذي نغص عليه حياته ذات يوم، فيل زيمر مان. كان زيمرمان يحسب منذ نشر برنامجه «منتهى السرِّيَّة» أن مشكلته الكبرى تكمن في الخلاف مع شركة آر إس إيه بشأن حق الملكية الفكرية. لكن جيم بيدزو س لم يكن بالمقابل ليجد مشقة في مهاجمة زيمرمان علناً. كان حسبه أن يضغط زر جهاز الفاكس فيتلقى الصحفيون نسخة من تعهد زيمر مان المكتوب (بصيغة غا مضة) بإيقاف توزيع البرنامج، وهو تعهد يبدو أنه لم يلتزم بروحه. غير أنه لم يكن ليراود زيمرمان خاطر بأن يجد نفسه عرضة للتحقيق النائي. وهكذا حسب عندما جاءته امرأتان من دائرة الجمارك الأمريكية في شمال كاليفورنيا في 1993، أن سبب الزيارة دعوى من جيم بيدزو س. والحق أن هاتين المفتشتين تناولتا مو ضوع توزيع البرنامج وكيف كان يتم، إلاَّ أن معظم الأسئلة كانت تنصب على التشابه بين برنامج «منتهى السرِّيَّة» ومُنتَجات شركة آر إس إيه. وكان واضحاً للعيان أن المفتشتين كانتا تفتقران للخبرة في المسائل التكنولوجية. فكان على زيمرمان أن يشرح لهما الأفكار الأساسيَّة التي يقوم عليها التشفير وتوزيع البرمجيات. ولما غادرت المفتشتان المكتب كان الرجل مطمئناً إلىٰ أنالمو ضوع طوي، ولم يعد لديه إلاَّ القليل مما يشغل باله. وحدثته نفسه أن الحادثة كانت مضايقة له من بيدزوس، وقال يومئذ: «لا أعتقد أنهم هناك سيتخذون أي إجراء ضدي. لقد أثارت المفتشتان بعض الأسئلة حول [أَنظمة التصدير]، ولكني تمكنت من إنهاء هذا الموضوع».

وكان ذلك صحيحاً، إنما ليس تماماً. فقد كان يراودا لمدعي العام في الولايات المتّحدة وليم كين خشية من أن يكون قد جرى خرق أَنظمة التصدير. وكان لذلك الخوف ما يبرّره، إذ لم يكن قد مضى إلاَّ ساعات على نشر برنامج «منتهى السرِّيَّة» على الإنترنيت حتى كان هذا البرنامج القوي قد وجد طريقه إلىٰ خارج الولايات المتّحدة. وليس واضحاً ما إذا كانت واشنطن قدمارست ضغطاً إلاَّ أن الواقع هو أن كين أخبر زيمرمان بعد بضعة أسابيع من تلك الواقعة بأنَّه

سيخضع للتحقيق بتهمة تصدير ذخائر حربية إلى الخارج. (كذلك استهدف التحقيق كيلي جوين الذي عرف نفسه للصحفي جيم وارين الذي يعمل في مايكرو تايمز على أنّه جوني آبلسيد في «برنامج منتهى السرّيّة»).

ولقد ظل زيمرمان، يعاني طوال السنوات الثلاث التالية من جحيم قانوني، يحقق في أمره هيئة من المحلفين، إنما دون إدانة. ونصحه محاموه بالابتعاد عن الأضواء. غير أن الشهرة التي أصابها برنامج «منتهى السرّيّة» أكسبت فيل زيمرمان ميلاً للحديث والتعبير عن آرائه بصوت عالٍ. وفضلاً عن ذلك كان يرى أن فرصته الكبرى في طرح الموضوع علناً أمام الجمهور. وكان يجد أن الناس العاديين كانوا يثورون كلما حدّثهم عن برنامج «منتهى السرّيّة» والموضوعات التي تتصل بالتشفير، ويتصاعد غضبهم من احتمال قيام الحكومة بالحد من إمكانية التواصل في ما بينهم دون تدخّل من أحد بهذه الحرية والخصوصيّة. و لقد ظن ولسبب وجيه أنّه حتى الذين لا خبرة لهم بالتكنولوجيا سوف يضيقون بهذه الفظاعة الجديدة، حيث الأخ الكبير ذاته يعد غرفة في السجن لمن يقوم بتوزيع برمجيات توفر الخصوصية للمقاتلين من أجل الحرية والعشاق وأولئك يرون أنه لا شأن لأحد بأسرارهم. والأكثر من ذلك أن التهمة الموجهة إلى زيمرمان كانت ضعيفة لا تصمد عند الامتحان؛ فالرجل لم يكن مرسل البرنامج إلى الشبكة. والشخص الذي قام بذلك أخبر [الصحفي] جيم وارين، بأنّه كان شديد الحرص على اقتصار عمليّة التوزيع على المواقع الأمريكية وحسب. فهل كانت وزارة العدل تؤكد في واقع الأمر على أن القيود التي تنص عليها أنظمة لتصد ير تحظر على المواطنين الأمريكيين، توزيع مواد مباحة قانونياً على مواطنين أمريكيين آخرين؟

وآه من أنظمةا لتصدير. إنك كلما أطلت النظر فيها، وجدتها تبدو أشد غرابة من ذي قبل، ومن القضايا المثيرة مؤخرا قضية تتصل بكتاب «الكريبتوجرافيا التطبيقيّة» لمؤلّفه بروس شتاينر والصادر عام 1994. وكانا لكتاب

مرجعاً شاملاً لنظرية الشيفرة الرياضية، ويضم شروحاً لمنظومات التشفير الشائعة وكافة الخوارزميات التي قد يحتاج إليها كل مختص بالأمن أو زعران الشّيفرة. وقد عرفه كتاب The Millenium Whole Earth Cataloge بأنّه «الكتاب المقدس لهواة الشيفرة». والمفارقة في الأمر أنّه يمكن لأي شخص أن يصدر الكتاب برمته إلى مختلف أرجاء العالم، سوى أن القيود المفروضة في موضوع التشفير تحظر على ما يبدو تصدير محتوياته بشكل رقمي. هذا على الأقل ما اكتشفه فيل كان، أحد زعران الشّيفرة، حين طلب الإذن بتصدير الكتاب وفق الصيغة الرسمية CJ Commodities Jurisdiction مع القرص المرن الذي يرافق الكتاب ويضم نفس محتوياته. ولقد وافق المسؤولون على تصدير الكتاب ذاته إنما دون القرص المرن. وبدا الأمر عندئذ سخيفاً.

أخذ زيمرمان يتحدّث ويثير ضجيجاً من حوله. وكان كثيراً ما يذكر في أحاديثه أن الثوار في بورما على ما تشير التقارير يستخدمون برنامج «منتهى السرّيّة» للتستر على نشاطاتهم المعادية للحكومة؛ وقد ذكر في شهادة له في جلسة استماع أمام إحدى لجان الكونغرس سنة 1993 أنه تلقّى شكراً من وطني من لاتفيا وزعم: أن «برنامجك منتهى السرّيّة شائع ومستخدم من بحر البلطيق حتى الشرق الأقصى وكفيل بمساعدة الشعب الديمقراطي عند اللزوم». ولما اتهمته الدوائر الأمنية بأن برنامج «منتهى السرّيّة» يفيد منه المجرمون على وجه الخصوص، وقد استند هذا القول إلى واقعة في سكرامينتو، حين تعذّر على رجال الشرطة قراءة يوميات أحد مرضى الشذوذ الجنسي المشفّرة، وفق برنامج زيمر مان، أجاب أن للتكنولوجيا فوائد ومضار.

ولعل الواقعة التالية تبين مدى الشهرة التي أصابها زيمر مان؛ اصطحبه بعض رجال الأعمال ذات ليلة لقضاء سهرة في سان فرانسيسكو، حتى انتهى بهم المطاف في ناد بنورث بيتش يعرض برنامجاً تتعرّى فيه الراقصات. وقد

سألته إحدى الراقصات حين أصبحت بالقرب منه عن عمله. فأجابها: «إنني أعمل بالتشفير، وقد وضعت برنامجاً اسمه منتهى السرِّيَّة».

توقفت الراقصة عن هزّ وسطها، وسألته كالمذهولة: «أأنت فيل زيمرمان؟ إني أعرف «منتهى السرِّيَّة» وكل ما يتعلّق به جيداً».

حقاً إن المرءلا يصادف مهووسين بالشّيفرة، ويعملون في مجال الجنس، كل يوم. ولكن الحق أيضاً، أن روّاد برنامج منتهى لسرِّيَّة كانوا قد أخذوا يتجاوزون نطاق المجانين والمهووسين بالسرِّيَّة. وقد ذكرت صحيفة وول ستريت جورنال أنمحامين يستخدمون هذا البرنامج للحفاظ على سرِّيَّة المعلومات والكتّاب لحماية الأعمال التي هي قيد الإنجاز حفاظاً على حقوقهم الأدبية كمايستخد مهعالم فلك في تسجيل اكتشافاته.

وليكسب رجال الأعمال والفعاليات التجارية عمد زيمرمان إلىٰ منح شركة تدعى فياكريبت، حق إنتاج الشيفرة، ولما كانت الشركة المذكورة تدفع أجراً لشركة آر إس إيه لقاء حق استخدام مُنتَجها، فيمكنها إذن أن تبيع برنامج منتهى السرِّيَّة لزبائنها من رجال الأعمال دون أن تخشى المقاضاة. (اعتقاداً منها أن ليس في دفع أجرين لقاء استخدام البرامج ما يضير، بفضل تميز برنامج منتهى السرِّيَّة كمُنتَج رائع والإقبال الواسع الذي يحظى به من الرواد غير الظاهرين).

وبدءاً من 1994 صبح لنقطة التوزيع الرئيسة، للنسخة المجانية الأكثر شعبية حليف غير متوقع هو معهدما ساتشوسيتس للتكنولوجيا. وكان البعض في المعهد يعتقدون، ومن أبرزهمللبرو فسور هال إبلسون ومد ير الشبكة جيف شيللر، أنه ينبغي السماح للمعهد بتزويد الأمريكيين ببرامج مسموح باستخدامها قانونياً ـ وأن يتم ذلك عبر الإنترنيت التي كانت أسرع وسيلة لتوزيع البرمجيات. وهكذا قام المعهد بتخزين أحدث النسخ من برنامج «منتهى السرِّيَّة»، في مخدم الإنترنيت، وسمح باستنساخها لمن يشاء ـ بعد شهادتهم بأنّهم أمريكيون فعلاً.

إن الحكومة الأمريكية، لم تكن تفكر بنظام الوعود، وعهود الشرف حين وضعت قوانين التصدير. والحق أنا لإجراءات التي أخذ بها المعهد لحماية الصادرات كانتمن ا لهشا شة ما جعل عدداً من نسخ «منتهى السرِّيَّة» تلحظ خارج البلاد بعد يومين من عرض البرنامج. ومع ذلك فإن القيود المفروضة بما يخص الجنسية كانت كافية لتجعل معهد ماساتشوسيتس بمنأى عن المساءلة الرسمية، ناهيك عن التحقيق الجنائي. وليس مؤدى ذلك أنا لحكومة كانت موافقة من الناحية الرسمية على هذا الترتيب. ففي جلسة مشهودة من جلسات مؤتمر عقد سنة 1995 وقعت مواجهة بين ممثل معهد ماساتشوسيتس جيف شيللر ومحامي وكالة الأَمن القومي رونالد لي (حل محل ستيوارت بيكر، عام 1994). فقد رفض لي أن يحدد ولو بشكل واه ماا لممسموح به وما هو الكفيل بأن يلقي بك في السجن، بالرغم من الطلبات المتكررة بأن يدلي ببيان يفصح فيه عما إذا كانت القيود التي وضعها معهد ماساتشوسيتس كافية. وفي تلك الأثناء كانت دار النشر الخاصةبا لمعهد قد أصدرت كتاباً (هذه المُنتَجات الصناعية الشبيهة بالأشجار الميتة ما تزال حولنا) ولا يحتوي إلاَّ مئة صفحة من الرموز بلغة البرمجة سي C بحيث يمكن لبرنامج منتهى السرِّيَّة، الذي وضع على نحو تستطيع معه الكاشفات وبرمجيات التعرف إلىٰ الكلمات تحويل الكتاب المطبوع بسهولة إلىٰ برنامج تشفير قوي ينتج على نطاق واسع. وبدا الأمر أقرب إلىٰ الخيال أن يجيز القانون مثل هذا المخطط بينما هناك هيئة عليا من المحلفين ما زالوا ينظرون في إدانة فيل زيمرمان؛ غير أن هذه هي حالة الضعف التي كانت عليها سياسة تصدير برامج التشفير عام 1995.

ولقد واجه مجدد ثوري آخر في مجال الشيفرة تطفلاً من عالم الواقع الشر س، وكان هذا يولف هيلسينجيوس المبرمج الفنلندي الذي كان يدير أول مدور للبريد وبالتأكيد أشد المراكز شعبية في العالم. وكان المشروع الذي يقوم عليه سنة 1995، يدعى بينيت، وهو مثل ساطع على فوضى التشفير، إذ كان

ينزع شارات التعريف عن آلاف الرسائل كل أسبوع، ثم يعيدها مغفلة لتسير في طريقها بسلام. وأصبح المشغل معروفاً في أوساط معينة وممقوتاً من المتنبئين باليوم الآخر في الحكومة الذين حذروا بأن خدمات كهذه، آتية لا ريب بنهاية المجتمع المتحضر. لكن المتاعب لم تأت من الحكومة بل من جماعة خاصة، الكنيسة العلمية.

كان العلميون، قد ضاقوا بما يصدر من النقد عن أعضاء قدامى حاقدين من جماعات جرت على عادة التداول والنقاش على شبكة الإنترنيت. وكان هؤلاء المبشرون يحصلون أحياناً على وثائق كنيسة فيقومون بتوزيعها عبر الشبكة. وقد سعى بعض المسؤولين في الكنيسه العلمية إلى مقاضاة هؤلاء الأشخاص لخرقهم حقوق الكنيسة الأدبية وأسرار المهنة. ولما كانت عناوين النقاد قد نزعت عن مراسالاتهم عبر نظام تدوير البريد، وتبين أنه غالباً ما كانت بينيت هي الجهة المخدمة، فلم يكن من اليسير اكتشاف الشخص المسؤول.

ثم تبين أن هناك فعلاً طريقة لاكتشاف المرسل. فقد كانت بينيت تسير بخطين ـ على العكس من الكثير من مدوري البريد، من زعران الشّيفرة ـ فأتيح بذلك للناس، الرد مباشرة، على الرسائل التي لا تحمل عنوان المرسل. وقد اقتضى هذا النّظام، وجود وسيلة لتعقب أصحاب الرسائل عبر نظام «يولف». فوجه محامو الكنيسة أولاً رسالة يحذرونه فيها بأن المصلحة التي يقوم عليها إنما تقوم بخرق حقوقهم الأدبية. فرد «يولف» بلغة لبقة مهذبة بأنه انتهج لشبكته سياسة عدم التدخل في ما يمر بالكومبيوتر. أفليس لديهم مدورون لبريدهم؟ ورد محامو الكنيسة بالتهديد بمقاضاته قانونياً، إذا ما استمر في انتهاك حقوقهم الأدبية. فاستبعد هيلينجيوس، وهو في فنلندة، أن يقدم هؤلاء المحامون، الذين لا ملامح لهم، والمقيمون في كاليفورنيا، على اتخاذ مثل هذه الإجراءات. وفي تلك الأثناء سمع يولف هيلينجيوس رنين الهاتف. وكان المتكلم، ممثل للكنيسة العلمية، بشحمه ولحمه. في فنلندة.

سأله ممثل الكنيسة إن كان يقبل دعوته إلىٰ العشاء؟

فقاليو لف في دخيلته، أنه ليس في رفض وجبة طعام ما يرضي العقل. وكان الرجل يبدي في حديثه كل الود، وأخبره أنه رجل شرطة متقاعد، وما يبغيه منه أمران: التوقف عن توجيه الرسائل، وإعلامه بالطرف الذي يوجهها.

فردهيلـــينجيو س: «آسف! هذا أمر لاأ قدر عليه». ولكن العلميين لم يكونوا يعتمدون، على حسن نية يولف هيلسينجيوس للوصول إلىٰ الاسم. فتقد موا عندئذ بشكوى إلىٰ شرطة لوس أنجليس، يدَّعون فيها أن ملكيتهم المسروقة يجري شحنها عبر الإنترنيت ووجِّهوا اصبع الاتهام إلىٰ هيلسينجيوس بأنه يتستر عمداً على اللصوص. وهذه في فنلندة جريمة خطيرة يكفي توجيهها ليحصل المدعي على أمر بالتفتيش وإلقاء الحجز على المادة المسروقة.

وبعد أسبوع من ذلك الاعتذار، ورد طلب الشرطي المتقاعد، تلقى هيلسينجيوس مكالمة أخرى من شرطة هيلـــينكي. وأُعلم يومئذ بأن لديهم أمراً صادراً عن المحكمة يقضي بـ «مصادرة الكومبيوتر لتفتيشه». وهنا وجف قلب هيلسينجيوس وأدرك أن عليه إلاَّ الانصياع. (والمضحك المبكي في الأمر أن هذا البحث كان سيذهب أدراج الرياح لو أن هيلـــينجيوس لجأ إلىٰ برنامج التشفير لديه ليرمز البيانات عنده ويوفر الحماية لزبائنه. ولكنه لم يلجأ لتشفير محتويات القرص لأسباب تتعلَّق بقدرة [الكومبيوتر] ضخامة قاعدة البيانات، على حد قوله، حالت دون إجراء عملية التشفير).

ولما كان هيلسينجيوس يدرك أن العلميين، إنما يريدون منه أن يتخلَّى عن عميل واحد، فقد نحا، إلىٰ عدم المجازفة بالآلاف الآخرين. وكان من حسن حظه أن ستطاع الإفادة من العلاقة الطيبة القائمة بين لفنلند يين والشرطة، بأن عقد وإياهما تفاقاً لا يقتضي منه تسليم كل محتويات قاعدة البيانات. وعمد عندئذ، إلىٰ نسخ عنوان البريد الإلكتروني الخاص بالطرف المعني على القرص

ا لمرن، ووضعه على الطاولة بمتناول الشرطة. وقد علق على تلك الحادثة بقوله: «لم أكن سعيداً جداً بما حصل، إلاّ أنها كانت تسوية».

غير أنّه لم تكن تلك نهاية متاعب هيلسينجيوس، إذ كانت هناك مؤسّسة أخرى في عالم الواقع، تهيئ لمداهمة استعراضه التشفيري لفوضوي: الإعلام. فقد نشرت إحدى الصحفا لسويدية هذه الحادثة في ذات اليوم الذي سلم فيه القرص للشرطة وادعت أن تقصي أثر معظم الصور الإباحية للأطفال على الإنترنيت قادإلىٰ مخدم في فنلندة. وغني عن القول أن هذه إشارة إلىٰ بينيت. لكن «يولف» كان واثقاً من أن دائرته لم تقم بتوزيع مثل هذه المواد، لأنه كان قد أغلق «الثنائيات» (الصور الرقمية). ولقد شاعتا لقصة ولم يتجشم أحد عناء التحقق من صدق الخبر. فلما أخذ يلاحق مصدر المعلوما ت تبين له أن شبكة منلشبكا ت التي تقدم صوراً إباحية للأطفال كانت تزور الرأسية التي تتصدر الصور بحيث تبدو وكأن مصدرها موقعه بينما هي تبث من موقع في المملكة المتحدة. ومع ذلك فقد كان لتلك الأخبار المروجة أثرها المؤذي، وازداد الأثر سوءاً حين رددت صحيفة بريطانية هذا الادعاء، وأوردت هذه المرة اسم هيلسينجيوس بالذات باعتباره الوسيط الشرير، في برامج الأطفال الإباحية على الإنترنيت.

وفي غضون ذلك، ملتمر ت هو ى كنيسة العلم؛ واستدعي هيلسينجيوس للإ جابة أمام المحكمة، عن سبب عدم تسليم الأسماء الأخر ى. وكان في غضون ذلك قد اتخذ إجراءاته لحماية أمن 700أ لف عنوان على قائمة البريد الإلكتروني، وكانت هذه الأسماء ما تزال غير مشفّرة حتى تلك اللحظة، إنما مخفية، إذ كان الرجل قد نقل الكومبيوتر من بيته إلىٰ غرفة مستودع في مكان سري. ثم قام بتوكيل محامين لمتابعة قضيته، ويعلم الله أنه لم يكن يملك المال لإنفاقهفي مثل هذا السبيل. وقد دافع عن موقفه أمام المحكمة الفنلندية أن من يفيد من خدماته، له كل الحق في التمتع بالخصوصية والسرّيّة. ولقد جزع حين

قضى القاضي بأنه لا ينبغي إيلاء البريد الإلكتروني الحماية ذاتها التي يتمتع بها البريد العادي. وكان من أثر تلك الواقعة، أن تراجع عالم الآلة خطوة إلى الوراء، على الأقل في فنلندة.

كان السيل قد بلغ الزبى، عند يولف هيلينجيوس. فمال: كان القرار واضحاً: «لم يعد بوسعك أن تقوم بمخدم كالذي أقوم عليه في فنلندة. وهكذا كان إغلاق موقع شبكة بينيت يوم 30 آب/ أغسطس 1996. وكان الدرس المستفاد الذي لا مهرب منه هو أن التكنولوجيا وإن وفرت حرية التشفير فلا بد للناس الواقعيين من أن يعيشوا في عالم الواقع ـ حيث تتمتع الحكومات والمشرعون بالوسائل لملاحقتهم. إن لعالم الواقع، القدرة على تعقيد الأمور أشد تعقيد.

لقد كان بوسع ديڤيد تشوم أن يعرض عليك هذا الدرس، أيضاً.

كان مخترع النقود الرقمية المجهولة المصدر ـ وصاحب أهم البراءات في مجال النقود الإلكترونية ـ يواجه وقتاً عصيباً وهو يجهد لتظل شركته ديجيكاش عائمة. ومع أنه توفر له جمع رائع من المبرمجين والكريبتوجرافيين في مقر شركته بأمستردام فقد كان ثمة ضيق متزايد أخذ يشيع بين أعضاء فريق العمل. كذلك كان تشوم قد قصر عن إكمال التحالفات الهامة التي هو بحاجة إليها لتعميم أفكاره. ثم ازدادت المؤامرات داخل جماعته الصغيرة حدة حين زعم أحد طلابه القدامى ويدعى ستيفان براندس أنه ابتكر طريقة بديلة لطريقته في إنتاج نقود دون تحديد مصدرها وبدأ باستقصاء طرق لبيع هذه الأفكار. وقد أصر تشوم على أن عمل براندس يعتمد على بحوثه وطرائقه. (نال براندس على براءات اختراع نافذة). وكانت ديجيكاش، ما تزال تبحث عن الصفقة الكبرى.

كانت ديجيكاش، قد بدأت برنامجاً تجريبياً رائداً على شبكة الإنترنيت، يدعى النقود الإلكترونية E-Cash واستخدمت في ذلك ما يشبه النقود، نقود رقمية كلعبة المونوبولي. أما في الحقيقة، فكانت هذه تجربة لدراسة إمكانية

استخدام، نقود رقمية على الشبكة، شكل من النقود تحل ذات يوم، محل العملة الورقية والمعدنية. أما الآن فبوسع المستخدم أن ينال 100 «دولار آلي» بمجرد أن يستدعيها من الآلة. وكان ذلك كله يجري دونما معرف. كذلك كان يمكن إرسال هذه الأموال الرقمية بالبريد الإلكتروني إلى الأصدقاء أو «شراء» ما يلزم من أي تاجر يقبل الدولارات الرقمية على سبيل التجربة. ومع أن دائرة المعارف البريطانية قبلت بهذا الأسلوب في تسديد ثمن مطبوعاتها، فإن قلة من التجار قد قبلوا بالنقود الإلكترونية، وهؤلاء يدورون في مجال محدود جداً وفي نطاق عمليات محددة يعرض نسخاً مسروقة لمجموعة كوميدية لتحصل على أرباح الدولارات الآلية.

ولما أذاع تشوم نبأ عقد الصفقة، كان الطرف المالي مؤسَّسة في منطقة وسط غرب الولايات المتّحدة، لها اسم مألوف عند طلاب الأدب أكثر منه لدى الممولين الدوليين: ماركتوين بنك. وقد تم الاتفاق على تقديم نسخة من النقود الإلكترونية. حيث يمكن تحويل الوحدات النقدية الإلكترونية إلى عملة حقيقية مكفولة من مارك توين. فإذا نجحت التجربة فقد تهرع المؤسَّسات المالية الأضخم إلى تبني هذا الأسلوب. وهنا ربما وجد نقاد تشوم، ما يحملهم على الصمت، وكأنّ حد هؤلاء النقّاد قد وصف أفكار تشوم بالخيالية والطوباوية كالتقاء بحيرة والدن [التي خلّدها المفكر الأمريكي ثورو في كتابه الموسوم باسم البحيرة، والدن. هـ. م] والإنترنيت.

ولم يكن تشوم وحده الذي يعاني المصاعب في إرساء النقد المشفّر ليكون معياراً تتعامل به الإنترنيت. إذ أن الصفقات التجارية لم تكن تقلع بالسرعة الكافية، ومعايير الشبكة كانت ما تزال، بعد، في طور التبلور، مما جعل استخدام أي نوع من النقد المشفَّر صعباً. وكان منافسو تشوم لا يعيقهم الالتزام الأخلاقي بضرورة إخفاء منشأ النقود الرقمية. فقد كانوا يرون على العموم أن الناس لا يهتمون بطلب مثل هذا الالتزام. ولكن تلك الشركات كانت

قد قصرت، عن تحقيق ما يتوقع منها، وكان من بين تلك الشكا ت شركة سايبر كاش وشركة موند يكس الحديثتان والمدعومتان بالمال، اللتان سمحتا للزبائن تنزيل النقود على بطاقات ذكية بحجم بطاقات الائتمان (فكر بآلة حساب مصرفية على كومبيوترك الشخصي). ولكن أين هذه من خيبات الأمل التي أصابت تشوم. لقد كان تشوم صاحب براءات النقود الرقمية المغفلة، ولمّا علنت ديجيكاش إفلاسها في النهاية، في عام 1998، كان تشوم ذاته الذي خسر تلك البراءات.

وبالرغم من المشكلات، والمضايقات التي خبرها أصحاب الثورة، في عالم التشفير في منتصف التسعينات فإن رسالتهم الكبرى كانت تمضي قدماً إلى الأمام. وبصرف النظر عن المناوشا ت والنكسات التي اعترضتهم فإن الحكومة هي التي كانت تفر أمام زحف هؤلاء الثوريين. فبعد تراجع آل جور الأول عن تعهده بتعديل خطة المقراض في كتاب إلى عضو الكونغرس كانتويل، عرضت الحكومة التوصل إلى تسوية مع أرباب الصناعة ثم عقد ت عدة اجتماعات في مقر المؤسسة القومية للمعايير والتكنولوجيا بماريلاند للتوصل إلى اتفاق. وكانت الآمال عظيمة بالتوصل إلى خطة ما تسمح بتحرير قواعد التصدير وترك موضوع وديعة المفتاح ليكون موضوع خيار حقاً. ولقد بدا بعض ما صدر عن الحكومة منطقياً تماماً. ولكن لما أزاح المسؤولون في الإدارة الستر عن الأنظمة النهائية تبين أن الشيطان يكمن في التفاصيل. وخلاصة القول أن القيود المفروضة على الصادرات سوف تستمر كما كانت دائماً، أما القوانين الخاصة بالمقراض فسوف يخفف منها جزئياً (كأن يكون للمستخدمين اختيار الوكالات لإيداع مفاتيحهم). ولقد فازت الخطة بلمها ا لمستعار المقراض 2 بجدارة.

ولقد تلا المقراض 2 بالضرورة المقراض 3، عام 1996. وكان لهذه الخطة غرض جديد، وتقوم على التلويح للشركات المتعاونة بجزرة تنالها إذا وعدت بأن تقوم بوضع الوديعة في مُنتَجاتها مستقبلاً، ويسمح لها بتصدير شيفرة بقوة معيار تشفير البيانات، بدون إيداع فوراً. والأمر المريح الواضح هو إعفاء

شيفرة قوية إلى حد ما من قيود التصدير لتأخذ لصناعة مجالها. ولكن الحكومة عمدت بدلاً من ذلك، إلى طرح بدل للسيا سة المتبعة ذاتها، هي غير لسيا سة المطلوبة.

وكان ثمة مشكلة لم تنقطع، تلح على الحكومة، هي نظرة البلدان الأجنبية بعين الريبة، إلى تصميم أمريكي يحتوي على مدخل للمفاتيح. وهنا أر سل «سفير للشيفرة» إلى الخارج لإقناع المجتمع الدولي بأن حلاً شاملاً كهذا الذي يحمله معه سيأتي بالفائدة للجميع. ولكن لما كان الحل لا يقدم في التطبيق مساواة بين كافة الدول فيلو صول إلى المفاتيح بات من المحتم أن تنتهي مهمة السفير إلى الفشل. وقد رأى بعض أعضاء الحكومة في هذا المثلب الضربة القاتلةلسيا سة كلها.

وفي تلك الأثناء أخذ الكونغرس بدراسة حل تشريعي للمشكلة، مدفوعاً بالشكاوي من الخسائر، التي تنزلها لصناعة الأمريكية، أمام الشركات الأجنبية التي تبيع برنامج الشيفرة. ففي عام 1996 قدما لسيناتور ونراد بيرنز، عن ولاية مونتانا، مشروع قانون «الأمن والحرية من خلال التشفير» ينص على رفع القيود عن برامج، تقدم شيفرة من مستوى «مقبول عموماً». (يفترض بأن هذا لفقرة تشمل معيار تشفير البيانات وخوارزميق سا التي تستخدم في الولايات المتّحدة. كذ لك تناولت مسودة القانون لمخاوف من أن تعمد الحكومة إلى اعتبار تكنولوجيا لمقراض أسلوب التشفير الوحيد المعتمد: نص مشروع القانون على منع نظام وديعة ا لمفتاح. ولقد سر بيرنز للسمعة الجديدة التي اكتسبها باعتباره فارساً مدافعاً عن حرية التكنولوجيا الحديثة، وهو ابن الغرب الذي يرتاح لركوب ظهرا لحصان أكثر من الجلوس أمام شاشة الكومبيوتر. غير أن مشروع القانون ذاته بقي حبيس ملفات اللجنة بينما ظل المشرّعون تحت تأثير جلسات المذاكرة المعدّة أحسنإ عداد من رجال وكالة الأَمن القومي وهم يحذرون من تهديد الأَمن القومي. وقد عبر عن هذا الوضع، السيناتور باتريك ليهي، وكان

من أوائل المؤيدين للقانون المقترح، بشكواه، من أنّه في الوقت الذي «يتفهم فيه بعض [المشرعين] هنا الموضوع تماماً، إلاّ أن هناك آخرين يخوضون في الأمر وكأننا [في الأوضاع التي كانت سائدة قبل عشر سنوات، عن صناعة [تتطور بسرعة، حيث] تعتبر عشرة أيام كالأبدية».

لو كان هدف الحكومة مجرد المماطلة، كل يوم يمضي، وجدار السد قائم هو بمثابة نصر لنا، لحق اعتبار النهج الذي سارت عليه نجاحاً. ولكن هذه السياسة كانت تنطوي على مخاطر، كما برهنت الهجمات التي شنّها زعران الشّيفرة على البرامج المخصّصة للتصدير، وأظهر اعتراض المكالمات عبر الهاتف الخليوي، بما في ذلك التي تجريها الزعامة الجمهورية في الكونغرس ومجلس الشيوخ، بأجلى صورة. فالبلاد تفتقر لنظام أمن إلكتروني قوي، وهو ضعف ازداد خطورة مع ازدياد انتشار الإنترنيت بصورة أعمق، وتداخل الشبكة في نسيج الحياة الأمريكية.

كان هذا على الأقل أحد الاستنتاجات الرئيسة التي خلصت إليها دراسة أعدها مجلس البحوث القومي. وكانت تلك المنظمة، وهي ذراع البحث في الكونغرس، قد قامت بفحص شامل لسياسة الولايات المتّحدة والمتصلة بالشّيفرة والتشفير، مستعينة بجهار من الخبراء من كافة الأطراف المعنية بالموضوع، وضمت وزراء سابقين ومسؤولين من وكالة الأَمن القومي والنقاد من الفعاليات الاقتصادية والجامعات، مثل راي أوزي ومارتي هيلمان. وجاء تقرير اللجنة، وكان بعنوان «دور الكريبتوجرافيا في تأمين مجتمع المعلومات»، شديد الانتقاد، على نحو مفاجئ، لسياسة الحكومة ونصح بالدأب على حرية ممارسة التشفير في الداخل، وتخفيف القيود على الصادرات وقبل كل شيء وضع «آلية لإشاعة الأَمن المعلوماتي في القطاع الخاص». وبعبارة أخرى، مزيداً من التشفير.

ولعل أكثر الملاحظات أهميةً، التي وردت في الدراسة، كانت نتيجة

لجلسات المذاكرةا لسرِّيَّة، التي حضرها أعضاؤها (حرم ثلاثة من أصل ستة عشر عضواً، من الموافقة الأمنية فلم يحضروا الجلسات). ومع أن أولئك الأعضاء امتنعوا عن كشف ما سمعوه في جلسات المذاكرة فقد كان بوسعهم تقدير أهمية تلك المعلومات السرِّيَّة في تحديد السياسة على المستوى القومي وهذا ما ورد في تقريرهم. الجواب: لم تكن بالأهمية العظيمة. فذكر التقرير أنَّه ليس لتلك «التفاصيل السرِّيَّة... صلة ذات شأن بالقضايا الأوسع من الأسباب التي تجعل السياسة تتخذ هذا الشكل وهذا الحال اللذين هي عليهما اليوم ولا بالصورة العامّة التي ستكون عليها التكنولوجيا ولا المنحى الذي يحكم تطور السياسة مستقبلاً». وحسبنا من هذا ما بلغنا من تفصيل القول: «لو كنتم تعلمون ما نعلم».

ولقد أصاب بعض القوم في الإدارة حرج من هذه النتيجة. (بل قد ساد أوساط مجلس الأَمن القومي، شيء من الضيق، لأنه يمكن اختصار عنوان الدراسة بالإنكليزية Cryptography's Role in Securing Information Society، بإعادة تشكيله من الحروف الأولى CRISIS، أيأز مة). وكانوا قد سلموا بأن جلسات المذاكرةلسرِّيَّة كا نت دقيقة شاملة، ولكنَّهم كانوا على قناعة من أن استيعاب المرء الموضوع على الوجه الصحيح عليه أن يحيا في عالم المخابرات ويتنفس هواءها. حقاً أن مارتي هيلمان أَو راي أوزي كان يدرك نظرياً أن مراقبة خطأ حد المحتالين أَو اعتراض مكالمة إرهابي بلها تف الخليوي أمر هام. ولكن الرئيس ونائب الرئيس يتلقيان كل صباح مجلدات ضخمة حسنة الشكل تر صد مختلف نقاطا لضغط الحساسة في العالم، كل شيء من شيفرة التقارير الدبلوماسية إلىٰ رصد مكالمات رجال المافيا الروسية عبر الهاتف في سبارته. وجماعة كلينتون كانوا يعلمون جيداً أن التشفير إن شاع وعمّ فسو ف يضيع منهم جزء عظيم من هذه المجلدات.

ولكن هذه النقطة الدقيقة لم تبلغ الجمهور الواسع، بل وفاتت العديد من

أعضاء الكونجرس، الذين كلفوا اللجنة بإجراء هذه الدراسة. وبدا تقرير مجلس البحوث القومي بدلاً من ذلك أشبه بدعوة إلى السلاح، للإطاحة بالقيود السخيفة، المفروضة على الشّيفرة والبدء بتدعيم أنظمتنا الخاصة. وبعد فالجني كما قال التقرير قد خرج من القمقم. وبهدوء أخذ بعض أقوى المدافعين عن إخضاع الشيفرة لسيطرة الحكومة يقرّون بهذا الرأي، أيضاً.

ولقد فُتحت بعدئذ جبهة أخرى في حرب الشّيفرة. فلأول مرة أخذت أنظمة التصدير، تواجه تحدياً جاداً في القضاء. وكان مدير وكالة الأمن القومي بوبي رابي إنمان قد اطمأن إلى نجاحه برد رأي محام بوزارة العدل سنة 1978 بأن أنظمة التصدير تشكّل خرقاً للتعديل الأول للدستور [الذي يكفل للمواطنين كل الحرية دون عائق أو تدخل. هـ. م]. غير أن هذا الموضوع ظل بمنأى عن النقاش، ولم يسبق أن تعرض له قاض من قبل. وكان العديد من الخبراء القانونيين قد رأوا أن الموضوع لو طُرح أمام المحكمة فإن القرار سيكون لصالح جماعة الشّيفرة. والحق أنه حين نظرت المحكمة قبل حين في دعوى أقامها أحد زعران الشّيفرة، فيل كارن، ضد قرار بمنع تصدير القرص المرن الذي يحتوي كتاب «الكريبتوجرافيا التطبيقية» قد أثار جدلاً مستعراً. فقد جاء قرار القاضي مبالغاً بالتشدّد. فقد رفض القاضي الفيدرالي المساواة بين المعلومات المتضمنة في كتاب مطبوع والمعلومات ذاتها بصيغة رقمية، ورد الدعوى، ثم أدلى برأي مفحم على الطلب الذي تقدم به كارن، هو بالضرورة اتهام له بشنّ هجوم غير أخلاقي على الأمن القومي. ولكن ذلك كان عرضاً ثانوياً لقضية أهم: قضية دانييل بيرنستين.

كان بيرنستين، طالباً يعد لنيل شهادة الدكتوراه من جامعة بيركلي، وبدأ اهتمامه بالشّيفرة والأمن سنة 1987 حين تمكّن أحدهم من التسلّل إلى كومبيوتره ومعرفة حساباته، فرغب منذ ذلك اليوم بدراسة خوارزميات الشّيفرة في إطار دراسته الجامعية وليس ثمة دلالة على تغير الأزمان أكثر من أن مناهج الدراسة

التي تركز على دراسة الكريبتوجرافيا، أصبحت اليوم أمراً شائعاً. وجدير بالتنويه أن الأنظمة الجامعية تحظر، من الناحية الفنية، على أي شخص أن يضع شيفرة مبتكرة في مكان يمكن أن يقع عليه أجنبي. وهذا بالضبط ما كان بيرنستين يريده.

كان مشروع بيرنستين يستلهم، صدفة، برنامجاً وضعه رالف ميركل عام 1989 يوم كان يعمل في زيروكس بارك، هو عبارة عن دالة تجميع ودعى سنيفرو. كانت الإضافة التي قدمها بيرنستين إلىٰ برنامج سنيفرو في إطار دراساته العليا، سنة 1990، في جامعة نيويورك كشف افتقار الشيفرات المعدّة للتصدير للمنطق. وكان يعلم أن برامج التشفير تخضع لقيود معينة، بينما الألعاب التي تتضمن دالةتجميع مثل برنامج ميركل مباحة (وهي لا تقوم بتعمية المعلومات لمجرد التعمية وحدها). وهكذا وضع بيرنستين برنامجاً يحول برنامج سنيفرو إلىٰ برنامج يؤدي وظائف التشفير وتفكيك الشّيفرة (انظر إلىٰ سنيفرو باعتباره سلاحاً أوتوماتيكياً محظوراً تم شحنه وتمريره عبر الجمارك بدون زناد والبرنامج الجديد هو العدة لتركيب الجزء المفقود). وقد شرح ابتكاره في ما بعد بقوله: «إنه قادر على معالجة أي دالة تجميع برمجية ويجعل منه أداة تشفير جيدة». وكان أن أطلق على ما ابتكره وهو رزمة التشفير هذه سم «خنخنة» Snuffle، ثم أرفقه ببحث يشرح العمل الذي قام به. ولكن الرجل كان قلقاً من أمر نشر برنامجه، خشية أن يثير بإبرازه هذه الناحية، ضيق الحكومة». وهكذا وضع البرنامج على الرف.

لكن بيرنستين أعاد النظر في الأمر، وهو في بيركلي، سنة 1992. فلم لا يقوم بنشر برنامجه؟ وما الضير في ذلك وهو ليس إلاّ تمريناً أكاديمياً، لا سلعة تجارية تعرض للبيع. ولما كان التشفير الفعلي يعتمد على خوارزمية مطبوعة ـ وهو لم يقدم خوارزمية تشفير أصلية من ابتكاره ـ فإنه لا يطرح تهديداً للجمهورية، فلمَ يكون نشره مشكلة؟ وكان المكان الواضح لنشره مجموعة

منا قشة الشّيفرة Sci. crypt discussion group . ولكنه قرّر أن يتخذ قبل ذ لك: إجراء احترازياً أخيراً، ليتأكد من أنه لا ينتهك بعمله القوانين. وكان أن سأل أ حد الأشخاص في الحكومة، إذ كان ذ لك مسموحاً به؟

و لقد كان من شأن هذه الخطوة الصغيرة أن تبعد البرنامج عن الإنترنيت طوال ما تبقى من القرن ا لعشرين.

كانت المشكلة الأولى التي واجهت بيرنستين هي تحديد الدائرة الحكومية المختصة، بمعالجة طلبه. وبعد سلسلةطو يلة من الأسئلة انتهى أخيراً إلىٰ ما يطلق عليه اسم مكتب ر قابة تجارة المواد العسكرية. وقام عندئذ بتوجيه كتاب إلىٰ هذه الدائرة في حز يران/ يو نيو 1992. وكان أن تلقى الرد الذي أثار غضبه والذي يحمل توقيع مديرذ لك المكتب الغامض، وليم بي روبنسون، ويؤكد أن توزيع البرنامج دون ترخيص يجعل بيرنستين عرضة للمساءلة القانونية.

قال بيرنستين في خلده، حسن، سوف أ قوم بالإجراءات الشكلية للحصول على حق التصرّف بالسلع. و لكنه أمل أولاً بأن يقوم مكتب رقابة تجارة المواد العسكرية بتوضيح حقوقه وما هي السُبل التي يمكنه اللجوء إليها في حال عدم موافقته على قرار من طرف الحكومة. وانتظر الرجل حتى آذار/ مارس 1993 حتى وجد من يتحدث إليه. وأ خيراً استطاع حمل تشارلز راي، المساعد الخاص لوليم بي روبنسون، على مكالمته. (قام بيرنستين بتسجيل المكالمات، بإذن رسمي). فأخبره راي أنه، بصورة أساسية، لا وجود لأي حقوق له. فلو وضع البرنامج على الشبكة بدون ترخيص، ثم قام عدو للولايات المتّحدة بنسخه في قاعدة للإرهاب في أفغانستان أو شقة في باريس فقد يكون مآل بيرنستين السجن ليكون بيته الثاني. ثم أخبر راي أن «ليس هناك ا ستثناءات في هذا الموضوع. فإذا كنت تملك ما يعتبر معلومات فنية وفق لوائح الذخيرة. . . فلن يكون لك ملجأ سواء كنت من رجال لصحافة أم الجامعة. . .

فإنك تظل عرضة للمحاكمة». وسأله بيرنستين: «ولكن ماذا عن التعديل الأول».

وكان تفسير تشارلز راي لدستور الولايات المتّحدة، أن «تلك الحرية تحمل معها مسئولية الانصياع للقوانين والأنظمة السارية».

وبعد شهر أمكن لبيرنستين الوصول إلى رئيس راي، وليم روبنسون الذي أكّد له ضرورة الحصول على إجازة رسمية لتصدير السلع CJ قبل القيام بتوزيع برنامجه. وقام بإجراء عدة لقاءات مع المسؤولين وكانت المحادثات معهم أكثر تثبيطاً للعزائم. وعلم أن ليس إيداع البرنامج وتوزيعه على الشبكة محظوراً وحسب، بل إن بيرنستين يصبح عرضة للمحاكمة. إذا ما وضع نسخة من بحثه في مكتبة عامة أيضاً. وبطبيعة الحال أصبحت وكالة الأَمن القومي طرفاً في الموضوع، شأنها دائماً، حين يتعلق الأمر بقضايا تتعلّق بتصدير أَنظمة شيفرة جديدة. وفي النهاية تمكن بيرنستين من إجراء بعض المحادثات مع ممثلين لوكالة الأَمن القومي، بعدما بلغه أن هناك وراء السياج الثلاثي من يعتبر برنامج «الخنخنة» Sunffle أداة «استراتيجية». وقد استنتج من ذلك أن البرنامج لا يسهل تفكيكه. ثم «أبدوا مساعدتهم لإعادة كتابة البرنامج حتى تنتزع منه مقوماته الاستراتيجية». ولكن بيرنستين اعتبر عملاً كهذا ضاراً.

وإذن عليه أن يخوض هذا السجال. ففي أيلول/ سبتمبر 1992 قدم خمسة طلبات، منفصلة للسماح بالتصدير. ثم قام بتجزئة المشكلة إلى خمس نسخ مختلفة ـ وهي تتراوح بين وصف للنظام بالإنكليزية، وعرض لصيغ رياضية ـ «لمعرفة ما هو مسموح به وما هو ممنوع». وهل يمكن للحكومة اعتبار كل جزء «مادة عسكرية»؟ كان بيرنستين ما يزال يعتقد أن الضباب سينقشع عن عيني أحد البيروقراطيين فيدرك أخيراً أن برنامج «خنخنة» مجرد بحث أكاديمي قام به طالب يحضر لدراساته العليا، وليس سلاحاً. ولكن الحكومة ردّت على تساؤلاته، في تشرين أول/ أكتوبر 1993، بقولها أجل، إن كل صيغة

رياضية أتى بها هي سلاح «يخضع للقوانين والأنظمة التي تأخذ بها وزارة الخارجية».

الحق أن بيرنستين لم يدخل العمليّة دخول مثير للشغب، ولكنه وجد نفسه الآن ثائراً مُستفزاً. وراح يتابع القضية بصبر وتأنّ وعقل منهّج على نحو كان له الأثر المدمر لدفاع الحكومة الأمريكية لاحقاً عن أنظمة التصدير كما طبقت على برنامجه. فقدم ستتنافاً عن استمارة إجازة التصدير CJ الأولى. فلما مضت الشهور ولم يبلغه ردّ الحكومة رأى أن ينشد المساعدة.

كان نصيره في هذه القضية شخص يدعى جون جيلمور، وهو رجل اعتاد خوض المعارك فيا لمحاكم ضد الحكومة. وكان هذا المشاغب المخضرم بين زعرانا لشّيفرة قد جمع لديه خزانة كاملة من الوثائق والعرائض التي تتصل بحرية تدفق المعلومات، وكا نت في الأصل قيد السرّيّة ثم أفرج عنها بأوامر قضائية. نصح جيلمور بيرنستين بالاستعانة بمحامية تدعى سيندي كون وقد قبلت هذه المحامية بالمرافعة في القضية للصالح العام. (قامت مؤسّسة الآفاق الإلكترونية EFF بتغطية تكاليفا لدعوى وتنسيق العمل مع محام مساعد). وفي عام 1995 تقدم بيرنستين ومؤسّسة الآفاق الإلكترونية بشكوى ضد وزارة الخارجية مدعين بأنقوانين ا لتصدير مخالفةلد ستور. وكان في مركز القضية الادعاء بأن نص البرنامج الأساسي في جهاز الكومبيوتر عند بيرنستين هو شكل من النطق والحديث والحكومة بمنعها نشره، إنما تنكر على بيرنستين حق التعبير.

وها قد أصبح الرأي الذي صدر في 1978، والقائل أن الأنظمة قد تتجاوز التعديل الأول أخيراً أمام الامتحان. ولكن قلة من الناس وحسب كانوا يعتقدون بأن القاضي ربما عارض رأي الإدعاء الذي لا بد وأن تطلع به الحكومة، والقول بأن لقوانين ا لتصدير أهمية حاسمة للأمن القومي، ولا بد وأن يؤدي القضاء عليها إلى ظهور الفرسان الأربعة في سفر الرؤيا في صورتهم لمعا صرة:

تجار المخدرات المختطفون وتجار صور الأطفال الفاضحة، والأفلام الفضائحية والإرهابيون.

ولقد عرضت القضية، أمام القاضية مارلين باتيل في محكمة منطقة شمال كاليفورنيا.. ولم تكن تصرفاتها الأولى تدعو للارتياح في نظر الادعاء، إذ أمرت بختم الأدلة، نظراً لأن قوانين التصدير تحظر توزيعها. ولكن القاضية باتيل أظهرت مع متابعة الدعوى تعاطفاً قوياً مع دعاوى بيرنستين. ولعل الحكومة لاحظت هذا التعاطف فلجأت إلىٰ عدة تكتيكات لتنتزع الدعوى من محكمتها. وقد ناقضت الحكومة نفسها في استمارتين من أصل الاستمارات الخمس التي قدمت، فاعترفت بأن تلك الآراء الرياضية كانت مجرد «بيانات فنية». ثم عمدت إلىٰ الطعن بصلاحية محكمة القاضية باتيل النظر في قضايا تتصل بقوانين التصدير. وطلبت عندئذ برد الدعوى على هذا الأساس. ولكن القاضية باتيل قرّرت يوم 27 نيسان/ أبريل 1996: استمرار النظر في القضية. وكان المسوغ الذي اعتمدته كافياً لإثارة القشعريرة في بدن واضع الأنظمة: فقد رأت القاضية مارلين باتيل أن بعض القيود المفروضة على تصدير برامج التشفير، على الأقل، مخالفة للدستور. ثم قبلت فوق هذا، بادعاء فريق بيرنستين أن نص البرنامج الأصلي يمكن اعتباره شكلاً من الحديث. وكان هذا يعني سريان القواعد الأشد صرامة التي نصّ عليها التعديل الأول للدستور. والمتعلق بتقييد الحرية ويتصل بطلب الإذن المسبق إنما ينطبق على هذا البرنامج. وبالنسبة إلىٰ موضوع الدعوى التي تنظر فيها باتيل فالأمر لا يتعلّق بالمحافظة على سلاح داخل الحدود؛ بل إن الموضوع هو منع غير شرعي لحرية التعبير وهذا مخالف للدستور وكان أن أكّدت باتيل في ذلك الصيف قرارها الأولي.

استأنفت الحكومة قرار المحكمة أمام محكمة الدائرة التاسعة الأعلى. وكان بيرنستين قد نال في تلك الأثناء شهادة الدكتوراه، وانتقل إلىٰ شيكاجو

للتدريس في جامعتها. وهناك، رغب في تدريس منهاج، يتضمن الكريبتوجرافيا، ولكنه بسبب من استمرار الدعوى كان بحاجة لموافقة الحكومة على تدريس هذه المادة. فتطلب الأمر قراراً قضائياً آخر قبل أن يسمح له أخيراً بتوزيع المواد المتعلقة بعمله ـ على طلابه حصراً. وهكذا جرى تدريس ذلك المنهاج دون أن يترتب على ذلك ضرر ملحوظ للأمة.

ومع ذلك فقد استمرت القضية، أمام المحكمة بين أخذ ورد. ثم تقرَّر عقد جلسة للمناظرة الشفهية أمام مجلس مؤلف من ثلاثة قضاة، في شهر كانون الأول/ ديسمبر 1997. وشاءت الحكمة السائدة يومذاك، أن تلغي محكمة الاستئناف ما اعتُبر قراراً غير متبصّر من قاضٍ يجلس على كرسي المحكمة، في نهاية المطاف، في سان فرانسيسكو التي يشيع فيها السخف. ولكن القضاة راحوا، في قاعة المحكمة المزدحمة بالحضور، يوجهون أسئلتهم بلهجة قاسية إلى محامي الحكومة الذي غلبت عليه سلاطة اللسان والإزعاج. وبدا القضاة يومئذ أكثر إعجاباً بمحامية بيرنستين سيندي كون، وكانت امرأة ضئيلة الجسم في أوائل الثلاثينات من عمرها، تقدم حججها بقوة بالرغم مما كان يعتور صوتها من تردد بين الحين والآخر. وكان ثمة نقطة مفاجئة أوردتها المحامية، وهي أن الحكومة حينما قامت بمنع عملية النشر على شبكة الإنترنيت لم تنتبه إلى قرارا تخذته المحكمة العليا مؤخراً و يعلق قانوناً يعرف بقانون آداب الاتصالات Communication Decency Act، إذ رأت المحكمة أن الشبكة منارة للديمقراطية ولها الحق بأعلى مستوى من الحماية التي نص عليها التعديل الأول. كذلك ألحّت كون على القضاة النظر إلى المضامين التي ينطوي عليها، قطع أسباب الحياة عن التشفير؛ وتساءلت إن كان يليق بالحكومة أن تمنع الأدوات التي قد يحتاجها مواطنيها لضمان خصوصياتهم.

ظل القضاة الثلاثة ينظرون في القضية مدة تزيد عن عام، ولم يصدروا قرارهم حتى أيار/ مايو 1999. وكان ذلك لدانييل بيرنستين قراراً يستحق الصبر.

فقد عبَّر القضاة، بأغلبية اثنين مقابل واحد، عن رأي واسع، لا يثبت قرار باتيل وحسب، وإنما زاد بالاحتفال بالكريبتوجرافيا باعتبارها من مقومات الديمقراطية، وعنصراً حيوياً في تكوينها فلا ينبغي أن يكون التشفير مجرد سر من أسرار الدولة، على ما جاء في القرار، وإنما حامياً لخصوصيات الناس أيضاً. وقد نم هذا القول عن أن القاضيين أدركا بطريقة من الطُّرق جوهر التشفير، دون أن يكونا قد تلقيا ثقافة علمية في هذا الموضوع. فكتبت القاضية بيتي فليتشر أن «محاولة الحكومة السيطرة على التشفير قد لا تقتصر آثارها على النيل من حقوق الكريبتوجرافيين التي كفلها التعديل الأول وحسب، بل ستنال من الحقوق الدستورية التي يتمتع بها كل منا، نحن الذين قد تصيبهم نعمة التشفير».

أقالت نعمة التشفير؟ لقد كانت القاضية فليتشر أحد زعران الشيفرة متخفياً في زي قاض!

كان بيرنستين في شيكاجو يشرف على امتحان في مادة رياضيات التفاضل، في عصر ذلك اليوم الذي صدر فيه قرار المحكمة، ولم يعلم أنه أصاب الحكومة بضربة إلاَّ بعد ذلك الوقت حين نظر في رسائل البريد الإلكتروني.

استأنفت الحكومة، طبعاً، الحكم الذي أصدرته المحكمة ـ ولكن أنظمة التصدير التي كانت تدافع عنها بدت أقرب إلى التداعي. لقد صمد السد في وجه التشفير طوال سنوات بشكل يدعو للإعجاب. ولكن السد أخذ الآن ينهار.

كانت هذه لعبة النهاية للحكومة.

والغريب أن وكالة الأمن القومي، لم تعد تبدو العقبة الرئيسة في عملية التوصل إلى حل، وبوسع المرء أن يتبين عند السياج الثلاثي، قبولاً واستسلاماً بحقيقة التشفير الجديدة. بل إن كلينت بروكس ذاته لم يعد في الخطوط الأمامية، ولكن في النهاية قبلت المؤسَّسة التي قام على خدمتها بفكرته عن التغير. ولعل قادتها وجدوا أنَّه من الأفضل أن يوجهوا جهودهم للاستعداد لما

هو قادم، بدلاً من محاولة الوقوف في وجه التقدم. ولعل أساطين الشيفرة في وكالة الأَمن القومي رأوا بعد إمعان الفكر أن كابوس شيوع التشفير في كل مكان أمر يستطيعون التعامل معه إن توفر لهم المزيد من الأموال. وكما ألح روبرت موريس في كلمته أمام مؤتمر كريبتو 95، وتفكيك زعران الشّيفرة [لبعض البرامج] تشير إلىٰ أن، هذه البرامج البرّاقة، والتي «لا يمكن تفكيكها» التي ابتكرها القطاع الخاص هي في الحقيقة ليست بالعصية إلىٰ هذا الحد، وكانت وكالة الأَمن القومي على اقتناع بقدرتها على الحصول على النص الواضح للر سالة المشفَّرة متى شاءت. وهناك شاهد على ذلك هو العمليّة التي موّلتها وأشرفت عليها مؤسّسة الآفاق الإلكترونية: حيث قام فريق من المهندسين بقيا دة جون جيلمور وبول كوتشر بصنع آلة تفيك معيار تشفير البيانات بكلفة 210 آلاف دولار (كان معيار تشفير البيانات ما يزال يعتبر ذخيرة حربية خيرة يحظر تصديرها إلىٰ الخارج في الظروف العادية). وفي العرض الذي قُدم في مؤتمر كريبتو 1998، تمكّن الجهاز من إنتاج النص الواضح لرسالة مشفَّرة بمعيار تشفير البيانات في أقل من 24 ساعة. وغني عن البيان أنه إذا أمكن إنتاج هذه الآلات على نطاق واسع، فإن كلفة الحصول على مثل هذه المفاتيح تصبح زهيدة. وللمرء أن يفترض، بأن في أقبية وكالة الأَمن القومي الكثير من هذه الوحدات.

على كل حال، كان مكتب التحقيقات الفيدرالي، وخاصةمد يره لويس فريه، هو الجهة التي ظلّت تحثّ على الأخذ بالخط ا لمتشدد إلىٰ حد الاستمرار في الإصرار على أن يتمتع المكتب بحرية الوصول إلىٰ النص الواضح ولو كلف الأمر تنظيم التشفير داخل حدود الولايات المتّحدة. واستطاع فريه في النهاية أن يحرر نسخة من مشروع قانون الهاتفية الرقمية، لإجبار أهل صناعة الاتّصالات على ما يفترض لتصميم منتجاتهم على نحو يسمح بمراقبتها ودياً. (غير أن معارضي هذا التصور في الكونجرس أفشلوا مسعى دعاته بالامتناع عن تخصيص

مئاتملا يين الدولارت ا لمطلوبة لتنفيذه). ومع ذلك، فقد ظل فريه يخشى أن يؤدي التشفير إلىٰ موت رصد الاتّصالات. ولقد دأب منذ عام 1994 على المطالبة علناً بأن يفتح الكونجرس عهداً جديداً من الحظر سمته منعا لتشفير ا لفعّال دون مفتاح مودع، إذا لم يتمكن عملاؤه من الحصول على النص الصريح من عمليات الرصد. فقال: إن الهدف الذي نسعى إليه هو معرفة تلك الحوارات التي تجري عبرو سائل الاتّصال سواء تمت بواسطة مشابك التمساح أم بالواحد والصفر [رقمياً] إني أريد الحصول على هذه المعلومات، مهما تكن، ومهما يكن الطرف فيها». لكن فر يه، كان قد فقد حظوته لدى إدارة كلينتون فلم يأخذ المسؤولون فيها بملاحظاته، و ضربوا عنها صفحاً.

ولا يقصد من هذا القول، أن الإدارة قد تخلّت عن آمالها بالقضاء على موجة الشّيفرة. بل إن كل ما في الأمر هو أن رؤاها المعادية للتشفير، كا نت تتضاءل وتزداد تضاؤلاً مع كل واقعة جديدة. وكان المشايعون في البيت الأَبيض يؤكدون أن هذه التبدلات أملتها روح آل جورسوامداده للتعاون مع المستثمرين في عالم التشفير وإيجاد التوازن المناسب بين الشّيفرة وراصديها. لكن جماعة كلينتون إنما كانوا يسيرون باتجاه واحد ليس له آخر إلىٰ الوراء. و قد أقرّبذ لك مايك نيلسون بقوله: «كان المركب تحت القصف»؛ وليس من علا مة تدل على أن السياسة تواجه ورطة كبرى أبلغ من أن الكلمات المستخدمة في وصفها تلقى أشد التنديد بحيث أنّها تحتاج للتلطيف والتشذيب لتكون مستساغة، حتى أن كلمة وديعة بالإنكليزية Escrow غدت سنة 1979 كلمة نابية، بالرغم من أنّلا ف الهواتف المزودة بالمقراض كانت قد بيعت في الأسواق في ذ لك الحين، ومفاتيحها تجمع الغبار الرقمي في الأماكن المحددة للإيداع. وقد بلغنا الآن مرحلة أصبح الهدف المعلن، يسملى ستعادة ا لمفتاح. وإن تلك ا لسياسة التي بدأت بضوابط المقراض الصارمة ـ خوارزميات سرّيّة في عتاد منيع، وخزائن وديعة، وتجهيزات للودائع تسيطر عليها الحكومة ـ قد جرى

تعديلها لتصبح مخططاً يعتمد على برمجيات، بحيث يستطيع المستخدمون اختيار تجهيزات الإيداع الخاصة بهم. وكانت هناك تسوية أخرى؛ فقد تم إشهار خوارزمية سكيجاك (الوثاب) بعدما كانت في الماضي سراً محروساً بعناية. وقال أحد المسؤولين في الإدارة فيما بعد، في تفسيره لما حصل: «إننا لسنا أغبياء. لقد أصغينا إلى السوق ومشينا». لكن السوق ـ والمقصود به الناس الحقيقيون الذين يسعون لشراء وبيع واستخدام برامج التشفير ـ لم يكن يريد شيئاً من برنامج الوديعة.

وفي غضون ذلك، كان الكونجرس يتلمس في نفسه الثقة، ليتابع مقتضيات السوق، بدلاً من أن يقع ضحية السيناريوهات الرهيبة التي تقدمها الإدارة منذرة بيوم القيامة الوشيك. ولعل العامل الأهم في هذا النزوع كان ظهور جهد ضاغط حسن التنظيم يمثل صناعة الكومبيوتر. فمنذ انقضاض النائبة ماريا كانتويل الانتحاري على قوانين التصدير ازدادت معرفة جمهور التكنولوجيا المعقَّدة، واكتسبوا الكثير من الدراية بقدرات كتيبة الأحذية البيضاء [الإدارة الأمريكية هـ. م] وما يمكن أن تلحقه بهم. فقد جعل المحاربون ضد الأنظمة، أمثال بروس هاينمان من اتحاد أصحاب البرمجيات من التشفير قضيتهم وجعلوا منها قضية حياة. وكانت التحالفات التي أقاموها مع جماعات الحقوق المدنية مثل مركز معلومات السرِّيَّة الإلكترونية، ومؤسَّسة الآفاق الإلكترونية، ومركز الديمقراطية والتكنولوجيا، توفر لهم الآن قاعدة شعبية من الناس العاديين. وكان أن التقت قوى الضغط مع المسؤولين ذوي الكلمة النافذة في الإدارة وأكثروا اللقاءات حتى كان يكمل أحدهم كلمة الآخر قبل أن تكتمل الجملة. وتمكنوا بالدهاء من معرفة المشرعين الذين يؤيدون مشاريع القوانين المتعلقة بالتشفير، ليس ليتجاوزوهم إلى سواهم، وإنما لزيادة الضغط لإشاعة جو من الانفراج الشديد لصالح التشفير. وكان من أبرز من كسبتهم قوى الضغط النائب الجمهوري المحافظ عن ولاية فيرجينيا، روبرت جودلات، وديمقراطية من

دعاة الاقتصاد الجديد من وادي السيليكون، زوي لوفجرن. وكان جودلات بالأخص، متقداً شديد الحماس لهذا الموضوع، عبقرية ولدت حديثاً في الكتابة بالشّيفرة كأنما رسمت الإبرة خطوطها بدقة. قال هاينمان: «كان أولما فعلنا هو أن ندعه يمضي بعض الوقت مع مسؤولي وكالة الأَمن القومي ليسمع وجهة نظر الطرف الآخر». وبعد أن اكتسب المناعة بفضل جلسات المذاكرة والاحتكاك المباشر والاطلاع على المعلومات السرِّيَّة، عرض له الوجه الآخر من الواقع، وهو التشفير أَو الكتابة المعماة باتا مطروحين في الخارج، والصناعة تواجه خسارة بلايين الدولارات وإلخ. وما أن اعتاد عضوا لكونجرس رؤية الغريب [عن وسط الحكومة هـ. م] حتى بات يظهر في أغلب الأحيان، مع كبار أهل صناعة الإنترنيت ومن المؤسف أنَّه صار هدفاً للنقد وسهامه.

ولقد أخذ جودلات ولوفجرن، يوضحان لزملائهما، بمساعدة جماعة حديثة العهد من أرباب الصناعة أطلقت على نفسها اسم «الأمريكيون من أجل سرِّيَّة الكومبيوتر» (كان هؤلاء «الأمريكيون» يتألَّفون من ثلاث عشرة شركة منها الآر إس إيه، والآي بي إم، ونوفيل، والصن، و مايكروسوفت)، ما قد ينطوي عليه تأييد نظام تشفير قوي من فوائد سياسيَّة. وفي مجلس الشيوخ وقف فارس غير متوقع هو كونراد بيرنز عن ولاية مونتانا ليتصدَّى للحكو مة، بمؤازرة المتبخّر في الخصوصية والسرِّيَّة باتريك ليهي والسيناتور ممثل مايكروسوفت باتي موراي، عن ولاية واشنطن.

وفي تلك الأثناء أخذ شكل مختلف كل الاختلاف عن المذاكرات المعهودة بالشيوع في قاعات لا ستماع. فبدلاً من الأحاديث المستهلكة عن استمرار نجاحنا في تفكيك الشيفرة، أخذ ا لشهود يحذرون من وقوع كوارث محتملة نتيجة عبث الغرباء بأنظمتنا وهي قابلة للنيل منها، جزئياً، لأن أكثر دولة في العالم تقد ماً قصرت عن اعتماد شيفرة قوية لحماية هذه الأَنظمة. وكان يبدو أن كل تخريب يصيب موقع الشبكة وكل سرقة لأَرقام بطاقة اعتماد على الشبكة

كان يدعم تلك المخاوف؛ وأخيراً أصبحت النتائج التي توصّل إليها المجلس القومي للبحوث تكتب صدى. بل لقد نال موقع مكتب التحقيقات الفيدرالي على الشبكة نصيبه من الضرب! كذلك أصاب موقع مقام الكونجرس تشويش فجأة مع احتمال وقوع هجوم رقمي يماثل الهجوم الذي وقع على بيرل هاربر، حيث يتعاون المتسربون إلى الشبكة والإرهابيون وأمم معادية ويتمكنون من شل حركة مجتمعنا بإغلاق المراكز التي تعمل في بلادنا مثل شبكة الكهرباء أو منظوما ت الأسلحة التي يحكمها الكومبيوتر. وإن لم يكن هناك رصاصة سحرية تعوض عن دفاعاتنا فالصحيح كذلك أن لدينا أداة قوية نحمي بها نفسنا، هي شيفرة قوية، أي ما كانت الإدارة تسعى إلى منعه!

في عام 1999، كان الكونجرس، الذي اكتسب الآن جرأة وجسارة، قد أخذ بالتجمع وحشد التأييد لمشروع القانون «الأمن والحرية بالتشفير» SAFE، الذي مضى على تقديمه ثلاث سنوات ويهدف إلى التخفيف من أنظمة ا لتصدير. والواقع أن الغالبية العظمى من أعضاء المجلس التشريعي ـ 258 عضواً كا نت قد وقّعت على مسودة القانون بوصفهم مؤيدين له. ولم تكن لأ خبار لآ تية من مجلس الشيوخ أحسن حالاً من منظور الإدارة. وكان القائد الذي تولى النضال والكفاح من أجل الوصول إلى تخفيف الرقابة على الصادرا ت، هو جورج ماك كين، وكان أسيراً في فييتنام، ولا تشوب مصداقيته في هذه الأمور شائبة. أما مشروع القانون الذي قدمه ماك كين والسيناتور بوب كيري فيحز يران/ يونيو 1997 فقد اتسم بحظر قيام «سلطات توثيقية» من أية حكومة في المستقبل، (والسلطات التوثيقية هذه هيؤ سّسا ت تتولّى توزيع المفاتيح العامة والتعريف بها، وهي مكون ضروري في البنية التحتية للتشفير الكامل) بتقديملخد ما ت لأولئك الذين يمتنعون عن إيداع مفاتيحهم. وفي ذلك ما يتيح للمواطنين الخيار بين استخدام الخطط من نوعية المقراض أو حرمانهم من المشاركة في الجماعة الإلكترونية. ولكن ماك كين عاد في عام 1999 فأمعن

النظر في الموضوع(وربما في أثرها على ترشيحه المنتظر لمنصب الرئاسة). وفي انقلاب مذهل، تحول ماك كين إلىٰ السيد كريبتو، وبا ت يجا هر بتأييد مشروع الأمن والحرية بالتشفير.

فهل كان الوقت قد حان، لترميالحكو مة باستماراتا لتصدير في الهواء وتصيح «ليحيا النص المشفر»؟ هذا ما يبدو. فمع أن الحكومة لم تكن لتؤمن بأن الكونجرس سوف يقر مشروعاً يطلب تحر ير الصادرات كان النِّظام أشد تعقيداً من أن يمد المرء يده إليه، والمجازفة بتعريض الأَمن القومي بالغة الحرج، وعلى كل حال هناك دائماً الفيتو الرئا سي الموعود ويمكن اللجوء إليه كان البيت الأَبيض في ضيق وقلق من أن تبقي الأصوات في اللجان الفرعية الموضوع حياً. وإذا شئنا الدقة قلنا أن جماعة كلينتون كانت قد أخذت تقلبا لتداعيات المحتملة لكارثة قومية تنجم عن فقدان التشفير وهو أمر تقع اللائمة فيه عليهم. فعلاً إن السماح بتصد ير برامج تشفيرية أمر ينطوي على خطورة، كانوا يقولون فقد يموت نا س لهذا السبب. . . ولكن الناس من جهة أخرى قد يموتون إذا ما هاجم شخص بنية رقمية تحتية! لكن المسألة كما عرضها أحد صانعي السياسة في البيت الأَبيض هي كيف يموت هؤلاء: هل تريد لهم أن يهبط عليهم الموت من السماء بصاروخ من الأرض إلىٰ الجو، أم بنسف أبواب سد جراند كولي؟» فإذا اختصرت المسألة بستة مرطر ف مقابل اثني عشر على الطرف الآخر، فأي معنى يكون عندئذ، لمعركة صعبةمر يرة لا خير يُرجى من ورائها؟

في أ يلول/ سبتمبر 1999، أعلن آل جور، وكان يتهيأ هو ذاته للترشيح إلىٰ ا لبيت الأَبيض، أن هناك عدداً من القرارات سوف تصدر في كانون الأول/ ديسمبر وتسمح بتصدير منتجات تشفيرية موجهة للمستهلك مهما يكن طول مفاتيحها. وكان هذا تحولاً كبيراً إلىٰ حد لم يستطع معه عضوالكونجر س كورت ويلدون، عن ولاية بنسلفيانيا، وكان قد ساعدالحكو مة، في رد مشروع قانون «الأمن والحرية عن طريق التشفير»، أن يتمالك نفسه، فصاح:

«كيف بوسعكم أن تعملوا بهذه السياسة؟ لقد دأبتم على القول لنا طوال سنوات، بأن من شأن طرح شيفرة قوية، أن تعرض الأمن للخطر، وتمنح المجرمين قوة وسلطة. وها أنتم تقولون لنا الآن، أنكم أصبحتم تأخذون برأي آخر؟».

«لقد انتهى الأمر! بهذه العبارة، لخّص ستيوارت بيكر رأيه، وكان قد عاد بعد مغادرته وكالة الأمن القومي في عام 1994 إلى مكتب المحاماة الذي يملكه ليختص بقوانين آلات التحكم التلقائي. وكان هناك من الناس من يعتقد أن الأمر كله مجرد تكتيك أخر للعرقلة تلجأ إليه الحكومة؛ وفي اللحظة الأخيرة يكشف واضعوا الأنظمة النقاب عن خطة بحروف أنيقة لا تحتوي إلاّ على القدر اليسير من التغيير. وكان الأمر في تصورهم أشبه بلوسي تختطف الكرة من اللاعب تشارلي براون وهو يتهيأ لركلها، كذلك سوف تحول وكالة الأمن القومي ومكتب التحقيقات الفيدرالي دون امتلاك القدرة على تصدير مفاتيح فعّالة. ولكن بات من الواضح الآن أن حيز المناورة بات يضيق باطراد، قبل أن يسدّد تشارلي ركلته النهائية والقاضية.

والحق أن الحكومة وفت بوعودها هذه المرة. فكان مشروع الأنظمة الأول يبدو كأنما يحتوي على قدر كبير من المحظورات والنواهي ينبغي الالتزام بها قبل منح برنامج تشفير قوي استثناء «تلقائياً»، لكن المسودة الثانية انطوت على تفهم أفضل بفضل المعارضة اللبقة إنما الحازمة أيضاً من طرف جماعة جودلات ـ لوفجرن او لصناعة. حقاً أن القانون لم يكن مثالياً، إلاّ أنه كان واضحاً بما يكفي لطمأنة حتّى المهووس إلى أن هذه المُنتَجات في طريقها إلى التصدير إلى الخارج. ولم يعد طول المفتاح إن كان معيارياً من 56 بت، أو حتّى 64 أو 80، أو 128، يعتبر سلاحاً قاتلاً.

لقد صار التشفير رسمياً مباحاً: صار التشفير العام صديقاً لنا.

بعد أيام قلائل من دخول الألفية الجديدة، تحين الذكرى العاشرة

للاجتماعا لسنوي، الذي تقيمه شركة آر إس إيه، لموضوع الكريبتوجرافيا، وباتا لحضور يشغلون كافة الفنادق الفخمة في سان فرانسيسكو، أما مكان المؤتمر في هذه السنة فهو مركز المؤتمرات في سان خوسيه. لقد غدا اليوم، سوقاً ضخمة لبرامج الشيفرة وتقنياتها وله برنامج للندوات التي تدور على خمسة مسارات وعدد الحضور يربو عنالأ لف.

وقد دأب منظمو المؤتمرات أن يتناول أحد الخطابات الرئيسة التطور أَو سواءفي ا لكريبتوجرافيا في المجال السياسي. وكان المؤتمر يجري وكأنما هو أشبه بمسرح الكابوكي (الياباني)، أبطاله ممثلون مفجوعون من عالم التجارة أَو الجامعات أَو عالم الحريات المدنية يشكون من عسف الحكومة. وقد تجد في المؤتمر مندوب عن الإِدارة سيء الفأل مساعد للمدعي العام، محام من وكالة الأَمن القومي، مستشار في سياسة التكنولوجيا يتأرجح على ساقيه، وتسمع هذا أَو ذاك يحاضر في جمع قاس عن التوازن الذي يعجز عنه الوصف بيرا لسرِّيَّة والأمنا لقومي، ولعله يثير في مستمعيه أسباب الثورة بقول أساء اختيار موقعه مثل «لو كنتم تعلمون ما أعلم» في رد على أسئلة لا بد أن تكون مشحونة بالنقمة. ولكن الأمور كانت تختلف عما عهدها رواد المؤتمرفي ا لسنوات السابقة. فقد وجد الحضور جيم بيدزوس يتقدم من منصةلمحا ضر وبيده زجاجة يقدم الشمبانيا لأعضاءا لندوة من وزارة العدل، ووكالة الأَمن القومي، وهو يقولانتهى ا لقتال وفاز جماعتنا.

وكان بيدزوس قد انتهى من التفرغ للعمل يو مئذ، ومرد بعض السبب إِلىٰ انتقال ملكية الآر إس إيه داتا سيكيورتي إِلىٰ شركة في الساحل الشرقي تعمل في مجال أمن الحواسب تدعى سيكيوريتي ديناميكس. (وكانت الشركة المالكة الجديدة قد قرَّرت قبل عدة أسابيع من كانون الثاني/ يناير تغيير اسم الشركة فأصبحت آر إس إيه سيكيورتي، وكانت [redacted] الصفقة حوالى 300 مليون دولار، وبلغ نصيب بيدزوس منها 40 مليون دولار. وهناك من يذهب إِلىٰ أن هذا هو

الرقم المعلن، أما في الحقيقة فلربما كان أعلى من ذلك، أو قد تكون شركة آر إس إيه استطاعت انتزاع حصتها البالغة بليون دولار بعد أن نجحت في برنامج الإدخال والمعالجة والإخراج على الإنترنيت لولا فضّ شركة ببليك كي بارتنرز على النحو المشين، حين اشتعلت الدعاوى بين آر إس إيه داتا سيكيوريتي وشريكتها سايلينك. فقد ضاق القوم في سايلينك بالشراكة القائمة وأزعجهم أن يحول الاتفاق الأساس دونهم واستثمار تكنولوجيا الخوارزمية «رسا» في مُنتَجاتهم؛ بل ولقد ذهبوا إلى حد الاعتراض، على براءة ملكية معهد ماساتشوستس للتجديدات التي أتى بها رايفست ورفيقاه. (وهذه دعوى غريبة نظراً لأن سايلينك كانت تنال حصة من عائدات تلك البراءة، عن طريق ببليك كي بارتنرز). وفي غضون ذلك أزعج بيدزوس وزميليه أن تكون سايلينك قد طورت مُنتَجاً أساسه الخوارزمية «رسا» لصالح مصرف التصفية العالمي سويفت SWIFT. ولقد تمّت تسوية هذه الدعاوى في النهاية في أواخر عام 1996 بمعونة قاض فيدرالي. وكان أن ادعى كلا الطرفين الفوز في هذه التسوية المعقدة (لاحظ بيدزوس أنه لم يبرز في الدعوى أدلة تثبت أن شركة آر إس إيه خالفت قواعد السلوك السليم في تصرفاتها)، إلاّ أن الدعوى استنفذت الكثير من الطاقة من الطرفين ـ فيما كانت براءات الملكية الفكرية، تقترب من تاريخ الانتهاء).

ولقد ظن بيدزوس بعيد بيع الشركة، أنه سيكون أسعد حالاً إن تقلصت علاقته بها. وكان قد انتقل للإقامة يومذاك في قصر بناحية مارين كاونتي، واشترى مجموعة من سيارات بي أم دبليو الأنيقة ويتدرّب على عزف الجيتار الأصيل، ويقود أسطوله الصغير من الطائرات وأخذ بشراء الأسهم حتّى أصبحت تملأ حقيبة بكاملها. ولقد أفاد من استثماراته حتّى بات من أصحاب الملايين، كانت قيمة حصته الشخصية في شركة فيري ساين للشهادات الرقمية وحدها (وهو أحد مؤسسيها) تزيد على ما حصّل من بيع شركة الآر إس إيه (تزيد قيمتها اليوم عن 100 مليون دولار). أما عمله الآن فهو ما يشبه السفير

الرقم المعلن، أما في الحقيقة فلربما كان أعلى من ذلك، أو قد تكون شركة آر إس إيه استطاعت انتزاع حصتها البالغة بليون دولار بعد أن نجحت في برنامج الإدخال والمعالجة والإخراج على الإنترنيت لولا فضّ شركة ببليك كي بارتنرز على النحو المشين، حين اشتعلت الدعاوى بين آر إس إيه داتا سيكيوريتي وشريكتها سايلينك. فقد ضاق القوم في سايلينك بالشراكة القائمة وأزعجهم أن يحول الاتفاق الأساس دونهم واستثمار تكنولوجيا الخوارزمية «رسا» في مُنتَجاتهم؛ بل ولقد ذهبوا إلى حد الاعتراض، على براءة ملكية معهد ماساتشوستس للتجديدات التي أتى بها رايفست ورفيقاه. (وهذه دعوى غريبة نظراً لأن سايلينك كانت تنال حصة من عائدات تلك البراءة، عن طريق ببليك كي بارتنرز). وفي غضون ذلك أزعج بيدزوس وزميليه أن تكون سايلينك قد طورت مُنتَجاً أساسه الخوارزمية «رسا» لصالح مصرف التصفية العالمي سويفت SWIFT. ولقد تمّت تسوية هذه الدعاوى في النهاية في أواخر عام 1996 بمعونة قاض فيدرالي. وكان أن ادعى كلا الطرفين الفوز في هذه التسوية المعقدة (لاحظ بيدزوس أنه لم يبرز في الدعوى أدلة تثبت أن شركة آر إس إيه خالفت قواعد السلوك السليم في تصرفاتها)، إلاّ أنا لدعوى استنفذت الكثير من الطاقة من الطرفين ـ فيما كانت براءات الملكية الفكرية، تقترب من تاريخ الانتهاء).

ولقد ظن بيدزوس بعيد بيع الشركة، أنه سيكون أسعد حالاً إن تقلصت علاقته بها. وكان قد انتقل للإقامة يومذاك في قصر بناحية مارين كاونتي، واشترى مجموعة من سيارات بي أم دبليو الأنيقة ويتدرّب على عزف الجيتار الأصيل، ويقود أسطوله الصغير من الطائرات وأخذ بشراء الأسهم حتّى أصبحت تملأ حقيبة بكاملها. ولقد أفاد من استثماراته حتّى بات من أصحاب الملايين، كانت قيمة حصته الشخصية في شركة فيري ساين للشهادات الرقمية وحدها (وهو أحد مؤسسيها) تزيد على ما حصّل من بيع شركة الآر إس إيه (تزيد قيمتها اليوم عن 100 مليون دولار). أما عمله الآن فهو ما يشبه السفير

إضعاف البت!) آر سي ـ 4 ـ بعد خمسة عشرعاماً من احتكاكه الأول بوكالة الأمن القومي. ثم، بالمناسبة، إجازة تصدير لمعيار معالجة البيانات العادي القديم، أيضاً.

وهناك، بعد، ديفيد تشوم المسكين الذي حُرم من الظهور تحت الأضواء. ولو كان حضر، فلربما رأى الكثير من الأمور التي تستهويه. فقد كانت الإشارات تزداد إلى حلول للشيفرة كالتي يقدمها تشوم كترياق لبث المعلومات الشخصية، وهو أمر غير مرغوب. فكان هناك شركة كندية تبرز منتجاتها في المعرض المرافق للمؤتمر، وتعرف باسم المعرفة الصفرية Zero Knowledge؛ وقد ستطاعت هذه الشركة متصاص الملايين لاستثماراتها، في مشروعها «المُعمّي» Anonmizer، وهو عبارة عن موقع على الشبكة يسمح للناس بالتجول في الشبكة دون أن يخلفوا آثار أقدام رقمية وراءهم.

ومع أن يولف هيلسينجر، لم يغادر فنلندة لحضور المؤتمر فقد ظلت آراؤه تنتشر. ففي الاجتماع الشهري لزعران الشّيفرة والذي عُقد في عطلة نهاية الأسبوع السابق للمؤتمر دار النقاش المعهود في هذه الاجتماعات وكان موضوعه ظهور جيل جديد من مخدمي البريد، ويعرفون بالماكسيماسترز»، ويستخدمون تقنية محسّنة تيسلر ستخدام الرسائل المشفرة المغفلة عبر الإنترنيت إنما بالغة الصعوبة يشق عل الحكومة قراءتها كل المشقّة.

غير أن فيل زمر مان استطاع، على كل حال حضور المؤتمر. كا نت الحكومة قد أسقطت دعواها في 11 كانون الثاني/ يناير 1996 ضده والمستهدف الآخر كيلي جوين. فأقامت زوجة يمر مان حفلة بمناسبة «إفلات فيل» في مركز السلام في جبل روكي. ولم يمض طويل وقت حتّى قرّر يمر مان الانتقال إلى وادي سيليكون لينشئ شركة باسم منتهى السرّيّة Pretty Good Privacy, Inc لإنتاج البرمجيات التجارية. (كانت شركة الآر إس إيه قد ادعت على الشركة الجديدة ومقاضاتها لانتهاكها حقوق الطبع، وتمّت تسوية الدعوى في النهاية، وكان على

شركة بي جي بي دفع العائدات المترددة والمعتادة عن قواعد إرسال ا لمفتاح العام). بيد أن الشركة لم يقيض لها الاستمرار طويلاً. والحق أن زيمرمان وهو الذي لا يستطيع، كما يقر بنفسه، ضبط دفتر الشيكات، سلم عمليات شركته لرجال أعمال، لتقويم وضع شركته، فأفلحوا في تدقيق حساباتها البالغة ملايين الدولارات. ثم توسعت أعمال الشركةا لجديدة وضمت إليها شركات أخرى وشرعت تشاركئا. جنحة تخطف الأنظار ببهائها في المعارض، وأخذت بخطة طموح لتتحول إلىٰ خدمة سرية كاملة عملاقة. وكان أن جرى بيع الشركة وقد شارفت الإفلاس إلىٰ شركة أمن حواسب شخصية راسخة تدعى نيتورك أسوشييتس، وظل زيمرمان يعمل في الشركة باعتباره رئيس برنامج بي جي بي، بيد أن مساهمته لم تكن في مجال تطوير برمجيات بقدر ما تكمن في مكانته رمزاً حياً للكريبتوجرافيا القوية. وبهذا الدور الرمزي حضر زيمرمان مؤتمر رسا 2000، في حفل أقامته نيتوورك أسوشييتس في الليلة الثانية من تلك المناسبة، حين وقف وأمامهو حة مفاتيحا لكومبيوتر وقام باستعراض كبير بتنفيذ نقل ملف بواسطة نقر الفأرة انتقلت معه نسخة من برنامج «منتهى السرّيّة» إلىٰ الخارج. وكانت الحكومة، قد أرادت أن تر مي به قبل سنوات قلائل في السجن للعمل عينه.

و لقد عقدت عدة جلسات في مراحل أخرى من لمؤ تمر ركزت الجهود التي ترعاها المؤسّسة القومية للمعايير والتكنولوجيالا ختيار خليفة لمعيار تشفير البيانات. فعلى العكس من عمليّة اختيار معيار تشفير البيانات الذي تم وراء الأبواب المغلقة، للحفاظ على سرّيّة مبادئ التصميم، كان طرح معيار تشفير البيانات المتقدم في إطار مسابقة يعلن اسم الفائز فيها في عام 2001.و هنا لا تقتصر العلانية على الخوارزميات وحدها بل وتسري على مقومات التصميم ذاته، وكل ما تطلبه مؤسّسة القومية للمعايير والتكنولوجيا هو أن يكونا لمعيار الجديد أقوى من سابقه معيار تشفير البيانات، على ألاّ يقل طول المفتاح عن

128 بيت. وكان من الصعوبة بمكان أن يُطلب فرض قيود شديدة على تصد ير الخوارزميات، نظراً لأن أكثر من نصف الخوارز ميات المشاركة في ا لمسابقة كانت من وضع كتّاب شيفرة يقيمون خارج الولايات المتّحدة.

كان قد مضى أكثر من عشر ين عاماً منذ أن طلع هويت ديفي باكتشافه، والحق أن الأمر استغرق من الوقت ما جعل سلسلة براءات الملكية الفكرية بما في ذ لك المفتاح العام وخوارزمية ر سا تقترب في غضون شهور قلائل من بداية القرن الجديد من الانتهاء، ومع ذلك فقد وجدنا العصر الذي راود حلمه بدأ يطل أخيراً. ففي الكلمة الهامة التي ألقاها أحد نوّاب رئيس مايكروسوفت، بعد كلمة بيدزوس، أعلن صاحبها أن النّظام الجديد، ويندوز 2000 وهو نظام لا ريب أنأ شكالاً منه، سوف تجد طريقها إلىٰ كل كومبيوتر خاص تقريباً في القرن الجديد سوف يكون مزوداً بنظام تشفير من 128 بيت، ومعه ترخيص بالتصد ير من الحكومة. وكان الكومبيوتر آبل، قد شرع يحمل نظام تشفير قوي في نظام تشغيله الجديد.

وكان نظام التشفير، قد أصبحأ ساسياً في كل متصفح في شبكة ويب، بما يتيح النقل الآمن لأرقام بطاقات الائتمان والمعلومات المالية. والمقدر أن تبلغ قيمة الأموال المتداولة بهذه الطريقة، في العام 2000، ما يزيد عن 80 بليون دولار ـ ويقدّر أن يرتفع الرقم في النهاية إلىٰ التريليونات، ونكون نحن جميعاً تقريباً في حماية خوارزميالر سا. وجد ير بالذكر أنه سوف يصدر في و قت لاحق قانون يختص بالتوقيع الرقمي لقومي لتفسح الطريق أخيراً لتجاوز العقبات التي سبّبها تباطؤ الإدارة، في ا تخاذ قراراتها سنة 1992 و لسوف يقوم الرئيس كليتون بالتوقيع على القانون إلكترونياً.

إن التكنولوجيا التي كانت محرَّمة ذات يوم، أصبحت الآن الدواء الشافي الجديد. كانا لتصور قد ذهب إلىٰ أن التشفير، هو الحل لمشكلة نسخ الموسيقى والأفلام وتهريبها إلىٰ الأسواق. فضلاً عن ذ لك كان التشفير المادة

السرّيّة للأحاديث ولمناقشات المحمية التي تدور جماعة من الجماعات وتجري في «شبكات خاصة تقريباً»، وهذا اتجاه تجاري هام يسمح بعقد المؤتمرات عبر الشبكة، دون أن يخترقها متلصصاً أو راصداً من الخارج. كذلك سوف يوفّر التشفير السرّيّة لسجلات المرضى، فلا يمكن الاطلاع عليها إلاّ بامتلاك المفاتيح السرّيّة لمغاليق لملفات. ومن المتوقع، بعد، أن تصبح برامج التشفير عنصراً أساسياً في الجيل التالي من الإنترنيت، حيث سيكون لنا أن نتواصل مع كومبيوتر غير شخصي وأدوات تتراوح بين الكومبيوتر الشخصي والهواتف إلى أدوات لمطبخ. ولسوف يكون كل ما يحيط بنا سلكياً ولاسلكياً، والتشفير، شبكة الأمان التي تضمن لنا السرّيّة.

وإذا شئنا الدقّة، لقلنا أن الأثر الثوري لكل هذا، سوف يتسرّب ويشيع خلسة بعيداً عن الأرصاد. فمئات الملايين الذين يستخدمون المستعرضات على الشبكة وأنظمة التشغيل لم يكونوا يدرون بهويت ديفي والآخرين، بل إنهم غدوا قادرين على إعجاز ثريسميوس السراني الذي عاش في القرون الوسطى وإدهاش فيجينيه الساحر صاحب المفتاح الذاتي، وحمل هورست فايشتل مبتكر لوسيفر على الابتسام، حتّى بينما تقوم الآلات بعمليات التبديل وتفكيك وتركيب الشيفرة وإنجاز لصفقات التجارية بهدوء وسكينة. وإذن، لمَ كان هذا لاحقاً ولم ينجز كما توقع ديفي في وقت أقرب؟ والجواب أن السبب في ذلك أن الإنترنيت هو، الذي أتاح لهذا الإنجاز أن يحصل.

وإذن، هناك سبب وجيه للاحتفال في مؤتمر آر إس إيه 2000. ولكن أولئك الذين يتساءلون عن السبب في سرعة التحول كانوا سيجدون الجواب لو جيز قبل عام من ذلك التاريخ، السبب ذاته والمكان ذاته والأشخاص ذاتهم، في مؤتمر آر إس إيه 1999. ولقد افتتحت تلك المناسبة بتصاعد أصوات جوقة كتاب مؤمني أوكلاند، حين ظهروا وملأوا المسرح وهم يرتدون جلابيبهم الزرقاء ويصدحون بأصواتهم على أنغام نسخة حديثة من الأنشودة الدينية: «ما

زلت انتظر ما أبحث عنه». كانت كلمات الأغنية، موضوعة قد حوِّرت، لتبرز النضال الطويل من أجل شيفرة قوية تشيع بين الجمهور. حينما ظهر جيم بيدزوس ذاته على المسرح وهو في ذات الرداء قال في شهادته التي كان يتلوها بلهجة الواعظ أن السحب في انحسار وقوس قزح لا بد أن يظهر قريباً. وبشر بأنّه إن لم تعم فوضى التشفير فسوف تشيع الشّيفرة. فقد كان يدرك أن أحلامه المتصلة بالمفتاح العام طوال تلك الأعوام كانت أشبه بدفع صخرة إلىٰ أعلى الجبل. ولكنا لمشكلة لم تكن في الحكومة أو أنظمة التصدير ذاتها. لقد كانت شيفرة المفتاح العام معجزة رياضية، إلاّ أنّها نزلت علينا قبل الأوان. كانت يومذاك، قبل خمس وعشرين سنة، حلاً لمشكلة لم تظهر بعد تماماً.

كان ذلك أمر مضى وانقضى. وليس هذا هو الحال، في وقت نجد فيه كومبيوتراً، فوق طاولة مكتب ومتصلاً بالإنترنيت. ولا حينما يكون في كل حضن تقريباً أحد هذه الأشياء أيضاً. لا ولا حين بدأت الهواتف ترتبط بالشبكة العالمية، مع أجهزة التلفزيون بل وحتّى منصات ألعاب الفيديو. وليس قطعاً حين تستخدم أدوات اتّصالات الشبكة غير المرتبطة في نقل المعلومات بين الناس، بل وحتّى بطاقتهم الائتمانية وخاصة بطاقاتهم الائتمانية.

نظر جيم بيدزوس إلىٰ مستمعيه وتعالى صوته الصدّاح معلناً: «قد وجدنا المشكلة للحل... وهي التجارة الإلكترونية!».

الخاتمة: السر المكشوف

عوداً إلىٰ الوراء، إلىٰ عام 1969. كان هويتفيلد ديفي قد بدأ للتو يولي لكريبتوجرافيا تفكيراً عميقاً. ولم يكن مارتي هيلمان، بعد، يعمل في جامعة ستا نفورد. ورالف ميركل ما زال في المرحلة الثانوية. وعالم الرموز ذات ا لمستوى العالي ما زال ملكاً لوكالات الاستخبارات وتحت إدارتها. وقد ظل الأمر كذلك، حتّى ابتكر ديفي وهيلمان وميركل المفتاح العام. واكتشف رايفست وشامير وأدليمان تطبيقاته. وكانت أفكارهم المعجزة للعقل والتي أنهت ا حتكار الأشباح لهذا المجال، لا تزال في المستقبل البعيد.

لم يكن جيمس إلليز، من النوع الذي يسمي نفسه شبحاً. صحيح أنه عمل لصالح القيادة العامة للاتّصالات GCHQ، ا لصنو البريطاني لوكالة الأمن القومي. لكنّه يفضل أن يصف وكالته، وابنة عمها وكالة لأ من القومي كذلك، بـ «المجتمعا لمغلق». لقد كان عضواً من جماعة تحفزهم الوطنية، والكبرياء، والحاجة البسيطة للمرتب لإعالة الأسرة. فإذا قدّر للمرء أن يحقّق إنجازاً رائعاً، فإن الاعتراف بيتم سراً، ضمن حدود المجتمع السري. وما أصاب جيمس إلليز من الألمعية والألق هو مثال بارز على هذا القول. فإلليز كان هو المخترع الحقيقي لكريبتوجرافيا المفتاح العام. وظل هذا الأمر مجهولاً لا يعلم به أحد واقعياً طوال قرابة الثلاثين عاماً.

لم يكن زملاء إلليز ليضعونه في عداد من يحتمل أن يأتوا بفتح يمكن أن يغير من قوانين مجالهم من العلم. وكان ينظر إليه على أنَّه قادر على الخروج بأفكار جيدة لكنَّه في أعماقه رجلاً حالماً. بل اعتقد بعضهم أنه على حافة الجنون. وقد وُلد في أستراليا وحين أصبح يتيماً ربَّاه جداه في شرق لندن. وفي الخمسينات وبعد تخرجه من إمبيريال كولدج، انضم إلىٰ القيادة العامة للاتِّصالات، في بلدة كوتسولدس في تشلتنهام. وكان إلليز يدرك أنه كان يدخل عالماً يُمنع فيه الاتِّصال مع العالم الخارجي بشأن عمله، الآن وإلىٰ الأبد. كان العمل هنا يعني أن يعمل المرء من أجل بلده؛ وعليه أن يضع أحلام الطموحات الشخصية والاعتراف العلني جانباً. وقد كتب إلليز قائلاً: «إن الأهمية القصوى للكريبتوجرافيا تتحقَّق بتقليص حجم المعلومات المتاحة للأعداء المحتملين إلىٰ أدنى حد. وإن المختصين في شؤون الكريبتوجرافيا المحترفين يعملون عادة في مجتمعات مغلقة لتأمين تفاعل مهني كاف لتحقيق مستوى رفيع من العمل والحفاظ على السرِّيَّة في الوقت ذاته».

قد يبدو في هذا شيء من العجرفة، لكن مهمة إلليز في الحقيقة لم تكن لتضعه وسط عالم المؤامرات الدولية. ويقول مالكولم ويليامسون، الذي سيكون له نصيب في هذه القصة بوصفه زميل المستقبل: «أعتقد أنه في بعض النواحي قد تمت تنحيته نوعاً ما. وعلى الأقل، كان انطباعي أنه لم يكن يعمل في أمور بالغة الخطورة ولم يعين فعلاً ليتولَّى المسؤولية في مشاريع كبيرة أَو شيء من هذا القبيل».

أما نيك باترسون الذي انضم إلىٰ القيادة العامة للاتِّصالات في أواخر الستينات، فيقول: «كان أقرب ما يكون إلىٰ أنموذج الرجل الإنكليزي غريب الأطوار: لطيف، غير منظم، يمشي متثاقلاً. وقد جرى بعض المدراء على التقليل من شأنه واعتبروه مجنوناً، لكنَّه كان رجلاً، لا ينضب معينه من الأفكار. والتي كان نصفها سخيفاً لكن ربما كان نصفها الآخر مذهلاً».

وبالرغم من أن معظم الناس كانوا لا يرون فيه إلاّ الرجل الغريب الذي اعتاد أن يعد قوته باستخدام النيسكافيه الممزوجة مع السكر والتي يضعها في مرطبان خاص به، لأنه كان يعتقد أن إضافة السكر بعد تذويب القهوة في الماء يجعلها أقل جودة. والعقبة الأخرى التي حالت دون الاعتراف بمواهبه، تمثّلت في عدم قدرته على التعبير عن بعض رؤاه بشكل واضح. ويقول أحد زملائه: «كان أسوأ محاضر تقني صادفني على الإطلاق. وكان المستمعون يعتبرون أحاديثه محنة تامة. وعادة ما كان يبدأ حديثه بالاعتذار، بأنه طلب إليه تقديم عرض، لأمر لا يعرف عنه شيئاً، بعدئذ يمضي لمدة عشرين دقيقة في اتجاه غريب. ولكن عندئذ ـ وهذا هو السبب في حضور الناس لأحاديثه ـ ودون جعجعة يطرح شيئاً مذهلاً.

كان إلليز مستاء بعض الشيء، لأن واحدة من أهم أفكاره أهملت فضاعت هباء. ذلك أن هيامه الشديد طوال حياته بتصاميم الراديو جعله يبتكر نوعاً خاصاً من الدارات السمعية التي تؤمن استقبالاً أفضل للموجات الصوتية. وحصل بالفعل على براءة اختراع لهذه الفكرة، وعرضت شركة أن تجرب وضعها في أجهزة الراديو التي تنتجها. لكن يبدو أن مهندسي الشركة، تنفيذاً لأوامر بتوفير المال عن طريق تقليص عدد المكونات قد أفسدوا تصميمه. وكانت النتيجة، أن استقبال الراديو لم يكن بالأمر الخارق الذي توقعه. فكان لهذه المهزلة أشد الوقع في نفسه وما انفكت تثير فيه أشد الألم.

في عام 1969، وكان إلليز في الأربعينات من عمره، ويعمل في قسم من الوكالة يدعى مجموعة أمن الاتّصالات الإلكترونية، في منصب ربما كان الأنسب له: مجموعة من الباحثين ربما بلغ عددهم الستة يعملون على مشاريع طويلة الأمد. وكان قد عاد للإنضمام إلى هذه المجموعة بوصفه كبير العلماء بعدما عمل لفترة في مكتب البريد، ومن المحتمل أنّه كان يساعد في مسائل أمنية. ووجد نفسه الآن يعمل على مشكلة اعتقد معظم الناس أنها عصية على الحل.

في الستينات، كانت المؤسّسة الاستخباراتية، قد بدأت للتو في التفكير ملياً في الثورة في الكومبيوتر، والتقنيات اللاسلكية، وما تلا ذلك من حاجة ملحة، لتأمين الحمايةلاتّصالات الحكومة التي كانت تجري عبر هذه الأقنية. لكنبينما غدت الأجهزة التي تقوم بالتشفير أرخص ثمناً، فإن جزءاً واحداً من العمليَّة لم يطرأ عليه تغيير جذري منذ الحرب العالمية الثانية. وكانت هذه وسائل توزيع وامتلاك المفاتيح الكريبتوجرافية. وكانت القيود الضرورية لحماية هذه المفاتيح بمثابة عنق الزجاجة: فكل شخصين يريدان الاتّصال سراً، كان لا بد لهما من توليد مفتاح سري جديد من أجل هذه المحادثة بالذات. وكان الآلاف من الناس في تلك الحلقة السرِّيَّة؛ وذلك يعني حرفياً ملايين المفاتيح للتحرّك بأمان وحماية. وكانت المشكلة هي نفس المشكلة التي ستزعج هويت ديفي بعد حين: تلك التعقيدات المزعجة جداً، والأخطار الأمنية الناجمة عن إدارة هذا العدد الهائل من المفاتيح.

كانت مشكلة صعبة، والطبع لم يتوقع أحد من جيمس إلليز أن يأتي بحل لها. فبعد كل شيء، كان ثمة قواعد معينة في الكريبتوجرافيا، تبدو راسخة رسوخ قوانين الفيزياء. وأيقانون مؤكد، أكثر من ذلك الذي يقول بوجوب عدم وضع المفاتيح السرِّيَّة المستخدمة في تشفيرلاتّصالات، في موضع يمكن للدخلاء اعتراضها؟ لكنإ لليز، وفقاً لزميل آخر يدعى كليفورد كوكس: «كان منذلك النوع من الرجال الذين مهما تكن المشكلة التي تعطيها لهم يبدأون بتحديلفرضيات الأساسيَّة، وغالباً ما يثيرون أسئلة تشير إلىٰ بطلانالفرضيات التي كنت تعمل عليها ـ فرضيات ربما كانت تمنعك من بلوغ الحلول». وفي محاولة حل مشكلة إدارة المفاتيح، تجد أن الكريبتوجرافيين بأجمعهم تقريباً يستبعدون أي حل يتضمن إرسال رسائل آمنة عندما لا يكون أسلوب التشفير معروفاً للمتلقي المحتمل فحسب، بل كذلك كل إرسال يفترض به أن يكون متاحاً للمتطفل كما هو للمتلقي المعني بالرسالة، بما في ذلك بث مادة المفتاح.

حتّى إلليز، شكك بإمكانية ذلك. وكتب لاحقاً: «كان واضحاً للجميع وأنا منهم، أن الاتّصال الآمن مستحيل دون مفتاح سري، أو معرفة سرّيّة أخرى ما، أو على الأقل طريقة ما يكون المتلقي فيها، في وضع يختلف عن وضع المعترض. وبعد، إذا كان المتلقي والمعترض في وضعين متماثلين، فكيف يمكن أن يكون أحدهما قادراً على تلقي ما لا يستطيع الآخر أن يتلقاه؟ وهكذا لم يكن هناك حافز للبحث في أمر من الواضح أنه مستحيل».

إلاّ أن الحافز، سرعان ما سيتولد لدى إلليز. فقد كان ثمة ورقة بحث مغفلة التوقيع دُفنت منذ زمن بعيد في جبل من المواد السرّيّة المكدسة داخل حدود عالم الظلام. كانت الورقة تصف مشروعاً لشركة بل للهاتف في الأيام الأخيرة للحرب العالمية الثانية، وسرعان ما صنف بين الأعمال السرّيّة المحظورة ثم أصبح في عالم النسيان. وكان هذا جزءاً مما يسمى المشروع سي 43 C 43، وهو تجربة بدائية لكنها مبتكرة في التشفير التماثلي للصوت. ولشرح هذا نفترض أنّك أردت إرسال رسالة عبر خط الهاتف ويراودك شك بأن شخصاً ما يسترق السمع. فكيف تستطيع إبقاء الرسالة آمنة؟ لقد افترض العالم المغفل الاسم في شركة بل أن على المرء الذي يريد تلقي الرسالة أن يضيف ببساطة ضجيجاً إلى الخط. فعندما يتم إرسال الرسالة فتختلط مع الضجيج بحيث أن مسترق السمع لن يسمع سوى كلاماً غير مفهوم. لكن المتلقي الذي يعلم على وجه الدقة كيف تولد هذا الضجيج، قد يستطيع أن يطرح هذا الضجيج من الإرسال ويحصل في النهاية، على الرسالة الأصلية غير المشفّرة.

كان مشروع سي 43 عديم الجدوى، لأسباب تتصل بالكريبتوجرافيا الحديثة، منها أن النموذج كان تناظرياً بينما الناس الآن يستخدمون الاتصالات الرقمية. إلاّ أن إلليز وجد هذا النّظام مثيراً: لأن المرسل لن يقلق من وجود عدو محتمل يسترق السمع، حتّى ولو كان الخصم يعرف كيف يعمل النظام. وقد أدرك إلليز أن الذي جعل ذلك ممكناً، أنه بخلاف الكريبتوجرافيا التقليدية،

جعل المتلقي في الواقع مشتركاً في عملية التشفير. وكتب إلليز: «كان الاتّصال المأمون ممكناً، على الأقل من لنا حيةا لنظرية، إذا اشترك المتلقي في التشفير».

هل يمكن لنظام كهذا أن يعمل مع كريبتوجرافيا رقمية واقعية؟ قرّر إلليز أن جوهر الأمر هومسألة هرطقة: هل بالإمكان فعلاً، إرسال رسالة مأمونة مشفّرة رقمياً، دون تبادل مسبق للمفاتيح. ووفقاً لروايته، أن ذلك السؤال قد عرض له في فراشه ذات ليلة. وما هي إلاّ دقائق معدودة، حتّى حصل على الجواب:

نعم.

فبينما كان جالساً هناك، في الظلام في غرفةنو مه في تشيلتنهام، حصل على البرهان على القضية. وكان الاسم الذي أطلقه على المسألة يجسّد التناقض: التشفير غير السري.

كا نت خطة إلليز تتمركز حولمجمو عة من ثلاثة تحولات رياضية. يستخدم المتلقي ـ ولتكن أليس ـ اثنان منها لإمر سل (أهلاً ببوب مرة ثانية) سيستخدم الثالث. وفريق ثالث غير مرحّب به، ولتكن إيف. هي المعترض المحتمل والتي لديها كذلك القدرة على الوصول إلىٰ هذه التوابع (الدوال)، لأنّها في هذا السيناريومعلوما ت علنية/ عامة. تبدأ العمليّة بعمل حاسم، أوصى به لإلليز مشروع سي 43: يشترك المتلقي المحتملللر سالة في عمليّة التشفير. تبدأ أليس بتوليد عدد كبير تم اختياره عشوائياً، وهذا في الواقع، مفتاح سري لا يحمله أحد سواها. ثم تقوم كذلك عن طريق تنفيذ تابع رياضي معين، لتحويل المفتاح إلىٰ عدد مختلف. ثم تقوم بإرسال هذا العدد الجديد إلىٰ بو ب.

إن هذا العدد الجديد هو النظير لما سيطلق عليه ديفي وهيلمان فيما بعد، المفتاح العام. ولما كانت الدالة (التابع) تتميز بخاصية هامة أنه لا يمكن حسابها

بطريقة عكسية، لذلك حتّى الذين لديهم هذا العدد الثاني غير السري، ويعلمون أي تابع أنتجه، لا يستطيعون القيام بحساب عكسي لاكتشاف العدد السري الأول. فهذا سيبقى معروفاً لدى المتلقي أليس وحدها.

والآن ولما كان لدى بوب هذا العدد غير السري، فإنه يستخدمه مع تابع آخر، لتشفير الرسالة التي يريد إرسالها لأليس. ثم يرسل الرسالة المشفَّرة لأليس. فكيف تعيد أليس الرسالة إلىٰ شكلها الأصلي كنص واضح بسيط؟ مع التابع الرياضي الثالث، تستخدم مفتاحها الأصلي السري بشكل أساسي لنزع التشفير عن الرسالة. ويمكن الآن لأليس، أن تقرأ الرسالة. في حين أن إيف لا تستطيع أن تقوم بشيء سوى أن تصرّ بأسنانها غيظاً.

في الواقع، أن المفتاح غير السري، يعمل مثل ضجيج الخط في مشروع سي 43: فبالرغم من أن أي متنصّت يمكنه سماع الضجيج على الخط، فإن المتلقي وحده يعرف كيف تم توليد الضجيج (هذه المعلومة هي المعادل للمفتاح السري)، وهكذا فالمتلقي وحده يمكنه عزل الضوضاء (أو في هذه الحال أداء الدالة/ التابع المناسب) لإعادة الرسالة المشفَّرة إلىٰ شكلها الأصلي الواضح. وحينما اكتشف إلليز خطة جعلت مبادئ المشروع سي 43 تتلاءم مع العصر الرقمي، فإنّه قد غيَّر بالضرورة قواعد الكريبتوجرافيا. ولما كانت هذه المفاتيح غير السرِّيَّة لا تحتاج لحماية، فمن الممكن الحصول على اتِّصالات آمنة دون تدابير مسبقة. وكان هذا يعني أن الموظفين الذين يعملون في ذلك المجال لن يكونوا بحاجة لأن يزودوا مسبقاً بمفاتيح متماثلة، مفاتيح يجب عندئذ الحرص على حمايتها. لقد غدا الآن ممكناً التفكير باتِّصالات محمية على نطاق أكثر اتساعاً.

لم تكن المهمة الموكلة لإلليز، خلق ثورة في الكريبتوجرافيا، لكن عليه الآن التعامل مع احتمال أنّه قد قام بهذه الثورة فعلاً. ومن المؤكد أن أساس هذه النظرية ذاتها ـ العنصر غير السري فيها ـ كان مناقضاً جداً في ظاهره لأعراف

الكريبتوجرافيا، لدرجة أن ضرب نظرية إلليز كانا. لنسبة للبعض في القيادة العامة للاتّصالات بمثابةتأييد للنظام الطبيعي.

على أية حال، كان لا بد للفكرة من أن تُمحَّص. وفي شهر تموز/ يوليو 1969، تم إرسال مسودة بحث إللیز إلىٰ شون وايلي وهو كبير المختصين بالرياضيات في القيادة العامة للاتّصالات لدراساتها، فمن المؤكد أن مجموعة الرياضيين، أو ربما رئيسهم نفسه، لا بد أن يجدوا خطأ قاتلاً في هذا النّظام. و قد استغرق إعلان النتائج أشهراً عدة، لكن قبل عيد الميلاد من تلك السنة، كتب وايلي خلاصة نتائجه: «للأسف، لا أستطيع أن أجد أي خطأ فيه».

لكن عالم الرياضيات، أشار إلىٰ أنإ للیز قد جاء ببرهان فقط، على أن مثل هذاا لنّظام يمكن أن يوجد ولم يأتبا لنّظام نفسه. وما كان مفقوداً هو لو سائل لضمان أن ثمة طريقة آمنة لتوليد مفتاح غير سري (مكشوف) من المفتاح الخاص الأصلي، ذلك أنّك كنت بحاجة لأن تتأكّد من أن أمثال إيف في العالم، الذين بعد كل شيء سيكون بإمكانهم الوصول إلىٰ المفتاح المكشوف، لكن لن يستطيعوا عكس تلك العمليّة الأولى وكشف المفتاح السري. وكان إللیزقد حدس مجموعة من جداول البحث التي ستقوم بعدة حسابات للتشفير وفكّ التشفير، لكنّه لم يأت بالتوابع (الدوال) المحددة ذاتها. وإلىٰ أن تم اكتشافها ـ فإن الشك بإمكانية هذا قد انتشر بسرعة ـ ولم يكن يُنظر إلىٰ التشفير غير السري إلاّ باعتباره شذوذاً نظرياً طريفاً، ولا شيء سوى ذلك.

يقول كليفورد كوكس: «كانت النتيجة أن سمعنا، إن هذا رائع بالفعل، إنه عمل عبقري، في منتهى الذكاء، ولكن كيف نستطيع الإفادة منه؟».

عندما دون إللیز مشروعه في كانون الثاني/ يناير عام 1970، لم يقم بتغليف هذه المشكلة وتزويقها ظاهرياً. لكن المعرفة بمضامين فكرته لم تكن تعوزه. ذلك أن عنوان البحث الذي نشر داخلياً ـ كان سرياً بالطبع ـ «إمكانية التشفير غير السري الآمن» وقد كتب في الخاتمة «من الضروري التمييز بدقة بين

الواقعة والرأي، أي بين ما تم إثباته بالفعل وذلك الذي يرجح أن يبدو كذلك. والقيام بهذا أمر صعب خاصة في هذه الحالة ذلك أننا أثبتنا أمراً، يبدو لمعظم الناس أنه بطبيعته مستحيل». وفي الحقيقة، أن المفهوم ليس مستحيلاً لأنه أثبت «بدقة متناهية» أن مشروعه كان «مقبولاً نظرياً».

كان ثمة خطوة واحدة لا بدّ منها لإنتاج وسائل ثورية للتشفير، وهي إيجاد الدوال (التوابع) الرياضيّة المناسبة. ولم يكن هذا بالأمر السهل. ذلك أن إلليز منذ أن بدأ بحثه كان قلقاً بشأن مهاراته الرياضية التي لم تكن ترقى للمهمة. (فقد تدرب ليكون مهندس). وبالرغم من المزايا الواضحة التي يمكن للنظام غير السري أن يقدمها، إلاّ أن القيادة العامة للاتّصالات لم تعتقد أنه من المجدي رفده بمزيد من الأدمغة لمساعدته في البحث. ومع ذلك، وفي أوقات مختلفة وعلى مدى عدة سنوات تالية، كان بعض الكريبتوجرافيين لدى مجموعة أمن الاتّصالات الإلكترونية يطّلعون على البحث ويعملون على إيجاد بعض الحلول الممكنة. وفي عام 1971 اهتم رئيس العلماء المعين حديثاً بالمشكلة وعيّن بعض الأشخاص ليحاولوا إيجاد حل لها. لكن البحث في التوابع الغامضة أفاد هؤلاء بأن تكون لديهم بالنتيجة فهم لمميزات مثل هذه الأمور، إلاّ أن محاولاتهم لم تجد نفعاً ولم توصلهم إلى حل للمعضلة. وهذا أدّى إلى رجحان كفّة الذين يصرون على أن المفهوم برمته أمر مستحيل.

ليس معروفاً إلى أي درجة، كانت وكالة الأمن القومي قد ساهمت في العملية، إذا كنت قد [redacted]كت على الإطلاق، منذ أن تعاون الرؤساء السابقين في أيام بليتشلي، قامت القيادة العامة للاتّصالات بإطلاع ما يسمونهم أبناء العم الأمريكيين على ما لديها من أسرار. لكن ليس هناك أي دليل على أن وكالة الأمن القومي قد بذلت جهوداً في مجال التشفير غير السري في تلك المرحلة. وتشير الوثائق التي نشرتها القيادة العامة للاتّصالات إلى أن العمل في هذا المجال كان مقتصراً على عدد من الكريبتوجرافيين العاملين لدى مجموعة أمن

الاتّصالات الإلكترونية، الذين كان لديهم حرية الوصول إلى المشروع، وكان لهم اهتمام للخوض فيه. ولما كان بلوغ الحل يبدو أقل احتمالاً، فإن أعداد هؤلاء أخذت تتناقص.

وهنا بدأ دور كليفورد كوكس في القصة. ففي عام 1973، كان كوكس موظفاً حديث العهد في مجموعة أمن الاتّصالات الإلكترونية. وهو ابن لأبوين من الطبقة الوسطى ـ كان والده محاسباً ـ وكان كوكس على قدر من الذكاء مكّنه من اجتياز امتحانات مدرسة مانشستر الثانوية، وهي مدرسة تنافسية مستقلّة، ذات مكانة علمية راسخة. ثم التحق بكلية كينجز كوليج في كمبريدج، ليحصل على إجازة في الرياضيات. وتابع دراساته العليا لمدة سنة في أكسفورد، باحثاً في نظرية الأعداد. ويقول: «لم أكن أحرز تقدماً فعلياً». إذن فأين يعمل؟ وبالرغم من أنّه لم يكن يعرف كثيراً عن القيادة العامة للاتّصالات، ولا فكر جدياً في الكريبتوجرافيا على أنّها مجال عمله، إلاّ أنه كان يعلم أن الوكالة السرّيّة كانت بحاجة إلى مختصين بالرياضيات. كذلك كان واحداً من أصدقاء الطفولة ويدعى ما لكولم ويليامسون يعمل لدى القيادة العامة للاتّصالات. (عندما حقّقت الحكومة في طلب كوكس أبدى المحقّقون اهتماماً خاصاً بهذا الأمر، ربما خشية أن يكون في هذه المصادفة ما يريب) وهكذا دخل كوكس المجتمع المغلق، في أيلول/ سبتمبر عام 1973، وهو في الثانية والعشرين من عمره.

إن احتمال عدم نشر الأبحاث بصورة علنية ليطلع عليها من يشاء لم تزعج كوكس، إذ يقول: «لقد كنت سعيداً لهذا». فلن يكون هناك أي ضغط للتنافس مع عباقرة الهيئات الأكاديمية. ذلك أن افتقار أبحاثه عندما كان طالباً للنتائج قد قاده للاعتقاد بأن مساهمته ستنصب بصورة أكبر على الجهود العملية التي سيكرسها لحكومته.

بعد أن يتم توظيف الناس في القيادة العامة للاتّصالات، كان يعين لهم

مرشد خاص يتولى، حسبما يقول كوكس: «تعليمك، ويرشدك إلىٰ ما تحتاج إلىٰ معرفته». وكان معلمه يدعى نيك باترسون، وهو مختص بالرياضيات من كمبردج أيضاً. وكان أعجوبة في لعبة الشطرنج في مسقط رأسه آيرلندة، ولم يكن ليكبر كوكس سوى ببضع سنوات. وكان يتوقع له النجاح على الدوام. وفي عصر أحد الأيام أثناء تناول الشاي، وبعد حوالي شهرين من التحاق كوكس بعمله. أشار باترسون إلىٰ فكرة إللينز. ولم يقدمها للشاب على أنها تحد، لتطبيق نوع جديد من الكريبتوجرافيا، ولكن على اعتبارها أقرب ما تكون إلىٰ الأحجية. ويقول كوكس الذي يعتقد أن عدم اطلاعه على بحث إللينز كان ميزة: «لقد شرحها لي نيك بصورة رياضية جداً، من حيث الحاجة إلىٰ دالة (تابع) لا تعكس وتتمتع بخاصية التشفير وفك التشفير». وهذا ما جعله يعالج المشكلة دون أفكار مسبقة. ولما كان قد أجرى أبحاثه في السنة السابقة، في نظرية الأعداد ـ مستخدماً الأعداد الأولية الكبيرة والمضاعفات ـ فمن المنطقي أن يستخدم تلك المعرفة لتطبيق نظرية إللينز، وكان الأمر كما كان يأمل».

وأضاف قائلاً: «أعتقد أنه كان مفيداً، أنني لم أكن مشغولاً بأي شيء، ذلك المساء». فقد عاد في تلك الليلة إلىٰ الغرفة المتواضعة التي استأجرها في تشيلتنهام وتناول طعام العشاء الذي أعدته صاحبة البيت حيث ينزل عندها بين أفراد أسرتها، ثم جلس يفكّر. وبسبب السرّيّة التي تفرضها القيادة العامة للاتّصالات في جميع الأمور المتصلة بعمله، كانت هناك حدود لا يملك تجاوزها. فلم يكن يسمح له بإحضار أي شيء إلىٰ بيته من مكان عمله. وإذا كان يفكر ملياً في مشكلة تتصل بعمله أثناء وجوده في غرفته المستأجرة، لم يكن مسموحاً له أن يكتب أي شيء، ولاحتّى ملاحظات على أوراق المسودة. فكان عقله الشيء الوحيد الذي يحمله معه. وقال: «لحسن الحظ، بدا أن الفكرة الأولى تعمل جيداً».

كانت الفكرة الأولى أكثر من مجرد جيدة ـ كانت رائعة. وقال كوكس:

«إذا كنت تريد تابعاً لا يمكن عكسه، فيبدو من الطبيعي لي، أن أفكر في مفهوم ضرب أعداد كبيرة جداً ببعضها البعض». واعتقد كوكس أن «المفتاح» السري سيكون في تطبيق عددين أوليين كبيرين، تولدهما المتلقية أليس فوراً، ويكون حاصل ضربهما هو المفتاح غير السري، وهو العدد الذي يعطى للمرسل لبوب. (يمكن لبوب أن يجده في دليل موزع على العموم). ثم اكتشف كوكس صيغة رياضية بسيطة تمكن بوب من أن يستخدما لعدد غير السري ليشفِّر الرسالة بطريقة لا يمكن لأحد أن يفك تشفيرها سوى الشخص الذي يعرف الأعداد الأولية الأصلية.

كانت الصيغة من الناحية الفعلية هي الصيغة ذاتها لما نطلق عليه الآن خوارزمية رسا. لقد أنتج كليفورد كوكس في ليلة واحدة، ما أعاد اكتشافه بعد ثلاث سنوات ثلاثة سرعان ما أصبحوا رياضيين مشهورين في معهد ما سا تشوسيتس للتكنولوجيا واستغرق ذلك الإنجاز منهم أربعة أشهر من المحاولة والخطأ.

يتذكر كليفورد، أن أول إنجاز لمفتاح عام في العالم قد تم على الأرجح حوالي الساعة السابعة أو الثامنة. وقال لنفسه حينذاك «إن هذا مثير للغاية». ثم اخلد إلىٰ النوم، بعد أن نظم الفكرة في عقله. ويقول: «عدت إلىٰ العمل في اليوم التالي وهناك دوّنت ما توصّلت إليه».

وضع البحث القصير على مكتب نيك باترسون وانتظر رد فعل معلمه. ويروي باترسون قائلاً: «لقد أصابني نوع من الجنون». ويعترف بأنّه انتابه يومذاك الاهتياج الذي يعرف به الآيرلنديون واندفع مخترقاً الرواق ليصل إلىٰ مكتب أخصائيي أمن الاتّصالات الذي يبعد أربعين ياردة عن مكتبه، وفتح الباب على مصراعيه، وراح يصرخ قائلاً: «إن هذا أعظم كتشاف كريبتوجرافي في هذا القرن». وذلك وسط ذهول الموظفين البيروقراطيين الرجعيين المنزرعين وراء مكاتبهم.

لكن هذا، على أية حال، كان رأي الأقلية. وحتّى كوكس شعر في ذلك الوقت، أن الأمر كان أقرب إلىٰ حل ذكي لأحجية رياضية من أن يكون نقطة تحوّل بالفعل. ولما بدأ الأمر يشيع في مجموعة أمن الاتّصالات أن أحدهم قد وجد طريقة لتطبيق فكرة جيمس إليز الغريبة، فإن أحداً بالطبع لم يعامل الأمر على أنه مثل عودة المسيح أو أي شيء من هذا القبيل. ويذكر كوكس: «كان لنا س يقولون ها، ها هاكم طريقة، ونعم العمل».

يبدو أنه ما من أحد يذكر، لحظة سمع جيمس إليز، عن الاكتشاف الذي قام به كوكس. يقول باترسون مخمناً: «أعتقد أن ذلك حدث في ذلك الصباح. لقد كان سعيداً جداً». لكن إليز كان حذراً كذلك متخوفاً، ربما من أن القيادة العامة للاتّصالات لن تأخذ الفكرة بالجدية التي تستحقها. وإن كوكس نفسه لا يذكر أول لقاء له مع إليز، الذي قدّر له أن يتعرّف عليه جيداً في الأشهر التالية.

حصل كوكس، على إذن لكتابة ورقة بحث عن فكرته، وذكر ذلك لصديقه ما لكولم ويليامسون، (بالرغم من أن ويليامسون كان يسكن في نفس البيت الذي يسكن فيه كوكس، فإن المحادثة كان لا بد أن تحدث في مكان العمل. إذ كان تبادل الآراء في موضوعات تتعلّق بالعمل يحظر أن تتم خارج جدران القيادة العامة للاتّصالات). وكان هذا خطوة إلىٰ الأمام نوعاً ما، لأنه كان من غير المألوف أن يقوم موظف جديد بتوزيع ورقة بحث بهذه السرعة بعد وصوله. وقد أثار الإعلان انتباه يليا مسون، فأصغى جيداً لشرح كوكس للمشكلة وكيف توصل إلىٰ حلّها.

كان ويليامسون قد عرف كوكس منذ أن كان في الثانية عشرة من عمره. فهو الآخر كان طالباً في مدرسة مانشستر الثانوية، وينتمي شأنه شأن صاحبه إلىٰ أسرة من الطبقة الوسطى؛ إذ كان والده بائعاً لدى شركة نسيج. ولما كان كل من كوكس وويليامسون متفوقاً في الرياضيات، فقد قامت بينهما منافسة لطيفة، وإن لم تكن معلنة. كذلك فإن ويليامسون التحق بجامعة كمبردج حيث د س

لكن هذا، على أية حال، كان رأي الأقلية. وحتّى كوكس شعر في ذلك
ت، أن الأمر كان أقرب إلىٰ حل ذكي لأحجية رياضية من أن يكون نقطة
ل بالفعل. ولما بدأ الأمر يشيع في مجموعة أمن الاتّصالات أن أحدهم قد
طريقة لتطبيق فكرة جيمس إليز الغريبة، فإن أحداً بالطبع لم يعامل الأمر
أنه مثل عودة المسيح أو أي شيء من هذا القبيل. ويذكر كوكس: «كان
ل يقولون ها، ها هاكم طريقة، ونعم العمل».

يبدو أنه ما من أحد يذكر، لحظة سمع جيمس إ. إليز، عن الاكتشاف
قام به كوكس. يقول باترسون مخمناً: «أعتقد أن ذلك حدث في ذلك
اح. لقد كان سعيداً جداً». لكن إليز كان حذراً كذلك متخوفاً، ربما من
قيادة العامة للاتّصالات لن تأخذ الفكرة بالجدية التي تستحقها. وإن كوكس
ه لا يذكر أول لقاء له مع إليز، الذي قدّر له أن يتعرّف عليه جيداً في
هر التالية.

حصل كوكس، على إذن لكتابة ورقة بحث عن فكرته، وذكر ذلك
قه ما لكولم ويليامسون، (بالرغم من أن ويليامسون كان يسكن في نفس
ت الذي يسكن فيه كوكس، فإن المحادثة كان لا بد أن تحدث في مكان
ل. إذ كان تبادل الآراء في موضوعات تتعلّق بالعمل يحظر أن تتم خارج
ان القيادة العامة للاتّصالات). وكان هذا خطوة إلىٰ الأمام نوعاً ما، لأنه
من غير المألوف أن يقوم موظف جديد بتوزيع ورقة بحث بهذه السرعة بعد
وله. وقد أثار الإعلان انتباه يليامسون، فأصغى جيداً لشرح كوكس
كلة وكيف توصل إلىٰ حلّها.

كان ويليامسون قدعر ف كوكس منذ أن كان في الثانية عشرة من عمره.
الآخر كان طالباً في مدرسة مانشستر الثانوية، وينتمي شأنه شأن صاحبه إلىٰ
من الطبقة الوسطى؛ إذ كان والده بائعاً لدى شركة نسيج. ولما كان كل
كوكس وويليامسون متفوقاً في الرياضيات، فقد قامت بينهما منافسة لطيفة،
لم تكن معلنة. كذلك فإن ويليامسون التحق بجامعة كمبردج حيث و س

مجموعة معقدة من التبادلات، التي يقوم فيها كل فريق بانتقاء عدد عشوائي، ويجري عليه حساباً باستدخام صيغة يصعب عكسها، وأخيراً يصل كل فريق إلىٰ مفتاح مشترك. ومن الناحية القانونية كان ويليامسون ممنوعاً من تدوين ذلك على الورق أثناء وجوده في منزله. طبعاً كانت الفكرة تصبح ملكاً للدولة، حالما تخرج من رأسه، ولم يكن ذلك ليزعجه. وفي ذلك يقول: عندما تكون قد توصلت إلىٰ مفهوم صحيح، فلا يمكن أن تنساه. وكل شيء يتتابع منطقياً». مع ذلك وكما يذكر صديقه كوكس ساخراً، في صباح اليوم التالي، كان أول ما سجلته ذاكرة كوكس أن ويليا مسون قد وصل باكراً إلىٰ العمل.

وكان أول شخص أخبره عن اكتشافه ـ كما يقول ويليامسون ـ هوإ لليز ط ته، الذي كانت معرفته به في ذلك الوقت ضئيلة. ولا يتذكر الكثير عن المحادثة، لكنّه يتذكر في الأسابيع التالية: «لقد جعلني جيمس أرى الأمر أكثر و ضوحاً. مع ذ لك فإن عدم كتابة ويليامسون للعمل الذي قام به إلاّ بعد شهرين، إنما كان مؤشراً لعدم الأهمية النسبية للمشروع من وجهة نظر القيادة العامفلا تّصالا ت. (وقد أنهى مذكرته في شهر كانون الثاني/ يناير 1974؛ في حين أن عمل كوكس، يرجع إلىٰ شهر تشرين الثاني/ نوفمبر 1973)، وبعد و قت قصير، ومزيد من المحادثات مع كلينتون خرج بفكرة أخرى نظمت المفهوم الأصلي. وكانت هذه تقريباًالصيغة ا لدقيقة ذاتها لما سوف يعر ف لاحقاً باسم ديفي ـ هيلمان لتبادل المفتاح. أما فيما يتعلّق بويليامسون، فبالرغم من أن البحث كان إلىٰ حد كبير نتيجة لورقة البحث الأولى، فمن الواضح أنه شعر بأنه ليس في عجلة من أمره لتوزيع بحثه ضمن الدائرة. ويقول: كان أسهل بقليل. . وبالفعل لم يبد أن ذلك يمثّل خطوة كبيرة».

والآن، أصبح لدى القيادة العامفلا تّصالا ت وسيلتان، لا وسيلة واحدة وحسب، لتطبيق بدعة إللليز. ولكن كما كانت تنتاب الوكالة الريبة من خطةإ لليز الأساسية، فقد التزمت الحذرا لشديد من هذين المشروعين. ويقول كوكس: «إن أول شيء أردنا التأكّد منهأنه كان مأ مونا».

والغريب في الأمر، أن العامل الوحيد الذي كان ضد التشفير غير السري هو روعة مشروع كوكس والتطبيق الثاني لويليامسون. يقول ويليامسون: «إنه مغر وجميل، إلاَّ أن الأناقة لم تكن ما نبحث عنه سابقاً في أنظمة التشفير. فهناك قاعدة أساسية تقول أن المشكلات المرتبة والأنيقة، لها حلول مرتبة وأنيقة، أما المشكلات الفوضوية فليس لها حلول مرتبة وأنيقة. والآن، معظم تصاميم الشيفرة فوضوية بشكل أساسي؛ إنها ليست مرتبة ولا أنيقة أو رياضية. لذا نحن مرتاحون إلىٰ حد كبير إلىٰ أن الناس لن يكونوا قادرين على حلّها، ذلك أنَّك حتَّى ولو استطعت التسلّل إليها، فلن تقع فجأة على برغي سحري صغير بحيث إذا قمت بحله وجدت كل شيء ينهار. لكن في هذه الأمور المرافقة للمفتاح العام، فمما لا ريب فيه أنه من الممكن أن يوجد برغي سحري. ويمكن لطالب مجاز بالرياضيات أن يتسبَّب فعلاً بوقوع كارثة».

كانت القيادة العامة للاتِّصالات، قلقة جداً بخصوص هذه المسألة، لدرجة أنَّها لم تكتف بالنظر في هذين المشروعين داخلياً دون أن تجد أخطاء متأصلة فيهما، بل خطت كذلك خطوة غير عادية بأن لجأت إلىٰ بروفسور شهير من خارج المؤسَّسة يدعى آر. إف. تشيرتشهاوس وقدمت له العمليات الرياضية التي تقوم عليها فكرة كوكس وسألته إن كانت مأمونة. وخلص تشيرتشهاوس إلىٰ نتيجة مفادها أنه طالما لم يكتشف أحد طريقة سريعة لتحليل الأعداد الكبيرة إلىٰ عواملها ـ وهو شيء لم يستطع أي رياضي الاقتراب منه ـ فإن المشروع مأمون.

في النهاية وجدت القيادة العامة أن طريقة ويليامسون، هي المفضلة بين الطريقتين، لأن التوابع الخاصة بها كانت أسهل في التعامل معها من الأعداد الهائلة التي أتت مع مشروع كوكس الذي يقوم على أساس الضرب. ومع ذلك، اعتبر النِّظام غير عملي. ويشرح لنا كوكس ذلك بقوله: «كانت الآلات التي ستستعمل باهظة الثمن وبطيئة جداً. وتحتاج إلىٰ عدة دقائق لتوليد [مفتاح].

ونظرنا في الظروف التي ستجد فيها فائدة الحصول على آلة، تستغرق وقتاً طويلاً لإنتاج [المفاتيح] وسرعان ما اعتقدنا أن التطبيقات كانت محدودة جداً، لتكون جديرة بالتعويم».

أما في داخل القيادة العامة للاتّصالات فإن الحكمة السائدة تغيرت من «مستحيل» إلىٰ «غير عملي». بالإضافة إلىٰ أن الكثيرين ما زالوا متخوفين من الجانب «غير السري» للمنهج. وذهب التفكير يومئذ إلىٰ كون هذا النوع الثوري الجديد من الكريبتوجرافيا ينطوي على نقاط ضعف دقيقة يصعب اكتشافها، نقاط ضعف يمكن للعدو استخدامها لاختراق النّظام.

حتّى مالكولم ويليامسون اعتقد أنا لمغامرة برمتها، كانت محفوفة بالمخاطر. وعندما كتب أخيراً النسخة المنقحة من المشروع الذي وضعه للمفاتيح، ذكر أن هذه التحفظات كانت السبب، وراء التأخر [في لكتابة] مدة سنتين. إذ كتب: «إنني أجد نفسي في وضع حرج. فبعد أن كتبت [بحثي الأول]، أصبح يساورني الشك في مسألة نظرية التشفير غير السري برمتها. والمشكلة أنه ليس لدي دليل على أن الطريقة... مأمونة حقيقة». ثم ينتقل لاحقاً إلىٰ الشكوى «أشعر بأنّه لا بدّ من وجود عيب ما في أمن الطريقة. لكنني لا أستطيع أن أجد أي خطأ فيها، وسأكون ممتناً، إذا كان بمقدور أي شخص آخر العثور عليه».

وكان ذلك أمراً لم يقم به أحد. لكن القيادة العامة للاتّصالات تو صلت بصمت في ذلك الحين إلىٰ قرار، مفاده أن تطبيق نظام المفتاح العام للتشفير لا يستحق الجهد الذي سيبذل من أجله.

في عام 1976، كان ديفي وهيلمان قد عرضا، طبعاً، ماتو صلا إليه، أولاً في كانون الثاني/ يناير، (بعد أن وزعا مسودات غير رسمية قبل ذلك التاريخ)، ثم قدما النسخة المعدلة [illegible]شرين الثاني/ نوفمبر تحت عنوان «اتجاهات جديدة في الكريبتوجرافيا». وتلاه بعد ذلك البحث المتعلّق [بخوارزمية] رسا

عام 1977. وقد حصل أصحابها على الشهرة، إن لم يكن على الثراء فوراً. لكن بسبب لأخلا قيات والقانون، لم يكن بمقدور العلماء في القيادة العامة للاتّصالات أن ينبسوا ببنت شفة، و ظلوا صامتين عن الحقيقة.

واستناداً إلىٰ كوكس، أن جيمس إ للیز، لما قرأ البحث الأول، الذي رسم الخطوط العريضة للفكرة دون اقتراح أي تطبيق لها، قال: «إنهم الآن حيث كنت عام 1969». وبالطبع فإن البحث الثاني لفريق عمل جامعة ستانفورد قد اقترح وسيلة للتطبيق، وهي مطابقة للحل الذي وضعه مالكولم ويليامسون. (ليس من الواضح ما إذا كانت أبحاث ديفي ـ هيلمان قد قادته إلىٰ كتابة ما اعتبره «خطوة صغيرة» ثانية في تطبيق البحث الأول، لكن بحثه يرجع إلىٰ آب/ أغسطس 1976، بعد أشهر من البحث الأول المنشور لديفي وهيلمان). أما كوكس فكان قد ترك القيادة العامة للاتّصالات مؤقتاً للقيام مهمة محددة في وزارة الدفاع، وكانت أول مرة يعلم فيها بالاكتشاف الأمريكي حين قرأ مقال مارتين جاردنر في منتصف عام 1977، ذلك المقال الذي و صف خوارزمية سا التي كان قد اكتشفها قبلها ثلا ث سنوا ت. فقال: «لقد فوجئت».

من المؤكد أن الكريبتوجرافيين البريطانيين، كانوا في ذلك الوقت يتابعون نظراءهم، الذين يعملون خارج عالم الأشباح. ومن الواضح أنّهم شعروا بالفزع عندما علموا، في وقت لاحق من عام 1977، أن جامعتي ستانفورد ومعهد ما سا تشوسيتس للتكنولوجيا، كانا يعتزمان الحصول على التوالي، على براءتي اختراع خوارزميات ديفي ـ هيلمان ورسا، ا للتان تم ابتكارهما أساساً لدى مجموعة أمن الاتّصالات الإلكترونية. وهذا ما أثار غضب ويليا مسون بشكل خاص.

ويقول: «حاولت أن أحمل ا لقيادة للعا مة للاتّصالات على منع براءة الاختراع الأمريكية. وكان بمقدورنا القيام بذلك، لكن الأشخاص في المراكز العليا لم يكونوا يريدون ذلك في الواقع. وأن براءات الاختراع قضية معقدة». وكان هناك، على وجه الخصوص، مسألة ما إذا كان بالإمكان الحصول على

براءة اختراع، وفقا لقانون البريطاني لأمر كانبالأ ساس عبارة عن خوارزمية رياضية، وكانت هنالك بالطبع مسائل أمنية أيضاً، إذ لم يكن مما يناسب القيادة العامة أن تدع غرباء يعلمون ما الذي يفكر فيه رجالها. كذلك يقول كوكس: «كانت النصيحة التي تلقيناها لا تزعجوا أنفسكم بهذا الموضوع». أما ويليامسون الذي لا يزال يعتقد أن رؤساءه قد جانبوا الصواب في هذه القضية، فيتذكر رئيس العلماء الذي أتى إليه أخيراً وقال: «لا، إننا لن نعمل على إيقاف براءة الاختراع».

والتزم عالم الظلال بالبقاء هادئاً.

وهكذا، فإن جبن وعزلة ما أطلق عليه إليز، ا سم «المجتمع المغلق» قد أدى إلىٰ فشل إبداعي: وبالرغم من نطلا قتها الجديدة فقد تخلت [القيادة العامة] كلياً عن فكرةا لمفتاح العام وسلمتها إلىٰ الغرباء الذين ستخدموها لا ليبنوا مجتمعاً بديلاً فحسب، بل كذلك ليبنوا صناعة كاملة (كان أول منتج عرف بأنله ستخدم تقنية المفتاح العام خرج من وكالة الأَمن القومي أَو القيادة لعا مة للاتِّصالات هو الهاتف المأمون إس تي يو ـ 3 STU-III الذي أنتج عام 1987، بعد زمن طويل من نشر بحث ديفي وهيلمان. وكانت آر إس إيه داتا سيكيوريتي في ذلك الوقت في طريقها إلىٰ طرح حلول سهلة للتشفير).

بالإِضافة إلىٰ ذلك، فإن رجال الحكومة بإعراضهم عن فكرة كريبتوجرافيا لمفتاح العام ووضعها جانباً، قد عجزوا عن رؤية بعض الجوانب الأهم في اكتشافهم. وكان من أهم تلك الجوانب الفكرة القائلة بأن أهمية كريبتوجرافيا المفتاح العام تكمن في قدرتها على إثبات هوية مرسلرا سالة (التوقيع الرقمي) بالإِضافة إلىٰ ما تتمتع به من خواص تشفيرية. والأكثر من ذلك، أن الوكالتين برفضهما التشفير غير السري بسبب بطئه الذي يجعله غير عملي، قد فوَّتتا ما اتضح أنه حل بسيط للمشكلة: استخدام خوارزميات غير سرِّيَّة مقترنة مع أَنظمة تقليدية للمفتاح المتماثل. وحالما نشر ديفي وهيلمان بحثهما، فإن العقول

المبدعة في القطاع الخاص لم تستغرق وقتاً طويلاً لتستنتج أن في هذه الأَنظمة «الهجينة» يكمن مستقبل تقنيات السرِّيَّة.

كانت هذه واحدة فقط، من الابتكارات المبنية على المفتاح العام التي نشأت عن حرية النقاش التي شاعت في جو من الانفتاح. ففي هذا الجو طرحت أفكار مثل النقد الرقمي (المغفل أَو القابل للتعقب)، والشراكة السرِّيَّة، والشهادات الرقمية، خاتم التوقيت الرقمي، والاتِّصالات الإلكترونية، والقمار عن بُعد... وأي عدد من التنويعات لمد هشة التي يجريها الأكاديميون والعلماء والتجّار وزعران الشيفرة. ونتيجة لهذه الجهود، غدا المفتاح العام موجوداً في كل زمانو مكان، على كل نسخة من برامج نيتسكيب ولوتس نوتس وجزء لا يتجزأ من ويندوز وماكينتوش، وحتماً في محفظة كل شخص، ولا فضل في ذلك للمجتمع المغلق، إنما الفضل كله يعود إلىٰ المجتمعا لمفتوح.

هل كان على القيادة لعا مة للاتِّصالات، وشركائها العمل بجد أكثر لجعل هذه الأفكار قابلة للتطبيق؟ هل كان من الممكن أن يأتوا ببعض من هذه الابتكارات؟ ربما، لكن بينما من السهل إلقاء اللوم على المجتمع الاستخباراتي لعدم تطبيق أفكارهم الأصلية، هناك جانب آخر للقصَّة.

بالنظر إليها من وجهة نظر الأَمن القومي، كان توخي الحذر أمراً منطقياً. ذلك أن تطبيق نظام جديد كلياً في القطاع الخاص، واستخدام أي نوع من التشفير لضمان المعلومات يُعدّ إبداعاً بحد ذاته. لكن القيام بمثل هذا في ما يتصل بأسرار الحكومة، وهي أَنظمة يعتمد عليها توفير الحماية في مواقف خطيرة تتصل بحياة الناس أَو موتهم، إنما يطرح نوعاً آخر من المخاطرة. يقول ويليا مسون: «على الحكومة أن تلتزم بأشد الحذر. فالأمان في بعض هذه الأمور، أشد أهمية بكثير من النقل، التحويلات المصرفية، أَو الاتِّصالات عبر الإنترنيت، أَو كيف سيبدو التصميم الجديد لسيارة فورد. لو أنني على قمة

الهرم في ذلك الوقت، هل كنت أجرؤ على تطبيقه؟ ما هو احتمال أن يجد أحدهم البرغي السحري الذي يفكّ كل شيء؟».

كذلك لا يقدّم ويليامسون أي اعتذار، لقصور مجتمع الاستخبارات عن اكتشاف أي ابتكار عظيم، من تلك الابتكارات التي تمخضت عن المفهوم الأصلي لنظام المفتاح المجزأ. وتذهب الحجة إلىٰ أن القيادة العامة للاتّصالات كانت بشكل أساسي وكالة للتجسّس والأمن، ولم يكن لديها اهتمام في تطوير ذلك النوع من التقنية التي ستوفر منافع للشعب عموماً (حتّى ولو كان الشعب هو الذي يدفع رواتبهم). ويقول ويليامسون: «هناك أساس جوهري للأشياء التي على الحكومة القيام بها، أما الأمور الأخرى فربما من الأفضل أن يقوم بها القطاع الخاص». وكان السبب الوحيد لاستمرار الوكالة في العمل على هذه التقنيات هو أن تتبين ما إذا كان بإمكانها، تحسين نوع النشاطات التي تؤديها القيادة العامة للاتّصالات أصلاً.

لكن بإعراض القيادة العامة للاتّصالات، عن استغلال التشفير غير السري، كان الاحتمال قائماً بأن رجال الاستخبارات يفوتون الفرصة الهامة للاستفادة منه. وفي عام 1982، وبعد سنوات كثيرة من حصول القيادة العامة للاتّصالات على جميع المعلومات التي تحتاجها لتطبيق نظام المفتاح العام، واجهت الوكالة البريطانية واحدة من أسوأ الفضائح التي ألمّت بها، عندما باع موظف يدعى جيفري برايم معلومات خطيرة إلىٰ الروس. وفي تلك الفترة الزمنية الطويلة، عانت وكالة الأمن القومي كذلك من عدة إخفاقات أمنية كبيرة في قضايا شائنة تورطت فيها عائلة والكر، وكريستوفر وأندرولي. واشتملت هذه على نقل مواد هامة لا تُقدَّر بثمن وهذا ما كان ليحصل في نظام يعتمد المفتاح العام. لذلك لم يكن أمراً مفاجئاً حقاً أن تتعرّض الوكالتان لفضيحة على هذا النحو. فبعد كل شيء، فإن الصعوبة في حماية المفاتيح [التقليديّة] كانت

مشكلة معروفة تماماً. وفي الحقيقة، تلك كانت هي المشكلة التي شرع جيمس إلليز في حلّها.

لذلك لماذا لم تتحرّك الوكالتان على نحو حاسم كتشاف بدائل لأنظمتها مبنية على التشفير غير السري؟ في التقديرات النهائية كان التشفير غير السرّي انحرافاً كبيراً عن القاعدة، وينطوي على المجازفة ـ وهما ميزتان عند المتنصت، ومدعاة للفزع عند البيروقراطي. ويقول مالكولم ويليامسون: «عليك أن تتذكّر، أن هذه هيئة حكومية. أعني أن هذا [التشفير غير السرّي]، أمر جديد ومختلف. « فلنضرب عنه صفحاً، لنتجاهله. ولندفعه إلىٰ ما تحت السجادة».

هل شعرا لعلماء، لدى القيادة العامة للاتّصالات بأنّهم قد خدعوا لدى رؤيتهم الآخرين يحصلون علىا لتقدير على أمر كانوا هم الذين اكتشفوه أصلاً؟ إنهم يدعون بأنّهم لا يشعرون بذلك، ويعتقدون أنّهم يتحدّثون كذلك نيابة عن جيمس إ للليز في هذه النقطة. يقول كوكس الذي يشعر بارتياح تام لهذا الوضع: «لقد حصل إللليز على اعتراف داخلي. وذلك أمر تقبله [حين عمل في القيادة العامة للاتّصالات]. الاعتراف داخل الوسط هو كل ما تناله».

كذلك يرفض ويليامسون فكرة أن صمتهم كان النهاية الفجّة، لصفقة فاوستية أبرمت عندما دخلوا عالم الظلال. و يرى العكس، إذ يعتبر أن المتضررين هم الكريبتوجرافيين الذين لا يعملون لصالحا لحكومة. ويقول: «إني أتساءل أحياناً لماذا يعمل الناس في الخارج بالكريبتوجرافيا. وما هي أسبابهم؟ من الواضح، أن لدى الحكومات أسباباً وجيهة لذلك، إنها تريد أن تكفل الأمنلا تّصالاتها، وهي تريد الاطلاع علىا تّصالات الدول الأخرى. وهذه وظائفها مة. من الذي يريد الجلوس في الجامعة ويقوم بمثل هذه الأمور؟ إنها نوعاً ما مثل كونك بنّاء سفن وتصرّ على العيش في آيوا». [ولاية داخلية بعيدة عن البحر. هـ. م.] (ويليا مسون نفسه، بعد سنوات من العمل في القطاع الخاص، هو الآن مواطن أمريكي ـ وقد عاد إلىٰ عالم الظلال، إذ يعمل

لدى مؤسّسة أبحاث لا تتوخى الربح تقوم بأعمال دفاعية سرّيّة).

لكن يبدو أن جيمس إ للیز كان قد فكّر في مستقبل أيامه. ويقول نيك باترسون: «كان عمله الوظيفي لا يؤدي إلىٰ أي هدف، وأحسب أنّه كان محبطاً وأخذ يتأمّل عمله كما تأمّل خيبة أمله في اختراعه السابق في مجال الراديو». في عام 1985 كتب بحثاً خصيصاً ليطلع الجمهور على حقيقة من اخترع فعلاً كريبتوجرافيا المفتاح العام. وفي الفقرات الافتتاحية، شرح أنّه مع أن للسرّيّة أهميةحا سمة جداً في عمله، إلاّ أن هناك ظروف يمكن فيها تنحيتها جانباً «في سبيل الدقة التاريخية، بعد أن ظهر جلياً أنه ما من مكاسب أخرى يمكن الحصول عليها من ديمومة السرّيّة». ولهذا يتابع قائلاً: «أضحى من المناسب الآن رواية القصة».

من الواضح، أنّه كان يأمل في تثبيت دعاواه. ينتهي البحث بالتأكيد، لأي شخص بليد الذهن قد تفوته الفكرة، أنه «بعد فترة من القيام بالعمل الأساسي» قام ديفي وهيلمان بماا سماه، إعادةا كتشاف تقنيات التشفير غير السري. لكن إذا كان إلليز قد أمل بأن تجد روايته طريقها إلىٰ خارج المجتمع المغلق بسرعة، فإنه سيتعرّض لخيبة أمل مريرة. فقد مرّ سنوات وسنوات وظلّت محاولته لو ضع الأمور في نصابها طي الكتمان. إذ شعر رؤساؤه أن الوقت لم يحن بعد لإ حقاق الحق. ولم يكن لو قت قد حان، بعد خمس سنوات من كتابتها أو عشر سنوا ت.

إذن لماذا سمحوا أخيراً للأوراق أن ترى النور في كانون الأول/ ديسمبر 1997، بعد اثنتي عشرة سنة من كتابة إلليز لتاريخ التشفير وقرابة عشرين سنة من العصفا لدماغي الذي كان سيهز الكريبتوجرافيا ذاتها؟ يقول كليف كوكس أن الدافع لذلك كان خطبة من المفترض أن يلقيها قرابة ذلكالو قت، تتحدّث عن موضوعات تشبه ما سيطلق عليه دوماً سمخوارزمية ر سا. لكن ما لكولم

ويليامسون، كان أشد صراحة في هذا الموضوع، إذ يقول: أن أوراق البحث كانت جاهزة إلاّ أنه لا يمكن نشرها «حتّى يتقاعد الشخص المعني».

يبدو أن ذلك التقاعد قد حدث، قبل 23 كانون الأول/ ديسمبر 1997، عندما نشرت القيادة العامة للاتّصالات الأوراق الأصلية لكل من إلليز وكوكس وويليامسون على موقع الويب التابع لها، بالإضافة إلىٰ «تاريخ التشفير غير السري» الذي كتبه إلليز عام 1985. لكن النشر أتى متأخراً بالنسبة لإلليز. فلم يكد يمضي شهر على معرفة لعالم بإنجازه العظيم، حتّى كان جيمس هـ. إلليز قد مات.

لكن لم يكن ذلك، قبل أن يلتقي بنظيره في «المجتمع المفتوح». كان هويت ديفي لسنوات كثيرة، يتساءل عن الإشاعات التي تقول بأن كريبتوجرافيا المفتاح العام تم اكتشافها فعلاً على يد الأشباح. وفي أواخر السبعينات، كان لدى مدير وكالة الأَمن القومي بوبي إنمان وجهة نظر عندما أعلم الكريبتوجرافي جس سيمونز، الذي كان يكتب مادة الكريبتوجرافيا لصالح الموسوعة البريطانية، أنه كان من ابتكار وكالة الأَمن القومي. وفي إحدى المرات ألح ديفي على نائب مدير وكالة الأَمن القومي هوارد رورنبلوم للحديث في هذا الموضوع، ودهش حين لم يحله روزنبلوم إلىٰ شخص داخل السياج الثلاثي وإنما إلىٰ مهندس في القيادة العامة للاتّصالات البريطانية لم يسبق له أن سمع به من قبل. ودون أن يفصح عن غرضه ـ إذ كان يأمل أنه سيكون واضحاً ـ اتصل بإلليز، الذي أشار إلىٰ أنه قد يطيب له أيضاً اللقاء معه.

في شهر أيلول/ سبتمبر 1982، كان ديفي قد خطّط لرحلة إلىٰ باريس، وسمح له جدول الرحلة بزيارة إلىٰ تشيلتنهام. كان ديفي وزوجته ماري فيشر قد غادرا باريس على أصوات الترانيم الكمية، التي كانت تصدح من كل جهاز راديو وتلفزيون، مرافقة لمراسم جنازة الأميرة جريس أميرة موناكو. طار ديفي

وفيشر إلىٰ مطار هيثرو وذهباً إلىٰ سالزبوري لقضاء عطلة نهاية الأسبوع. ثم قاد ديڤي سيارته وحيداً إلىٰ تشيلتنهام.

كان إلليز يسكن في أطراف المدينة؛ وخلف منزله كانت الأرض منحدرة، ويمكن للمرء أن يرى منظراً جميلاً للمدينة على مرمى النظر. وقد أطلق على منزله اسم ديلكوشا، التي تعني‌با لفارسية «المتعة الصغيرة». وكان يربي النحل في حديقة منزله. وفي ذلك الحين، كان إلليز في أوا خر الخمسينات من عمره طويل القامة انتشر الشيب في شعره. وكانت زوجته سيدة لطيفة؛و لديهما ابنة على وشك الالتحاق بكلية الاقتصاد بجامعة لندن. وبعد حديث قصير مع زوجة إلليز، اتجه ديڤي وإلليز إلىٰ إحدى الحانات.

ا ستدار ديڤي نحو إلليز بعد أن ركن السيارة. وقال: «أخبرني كيف ابتكرت «التشفير غير السرّي».

فسأله جيمس إلليز: «من يقول أنني قمت بذلك؟».

فأعطاه ديڤي سم المسؤول في وكالة الأمن القومي.

فسأله إلليز: «أتعمل عنده؟» فأجاب ديڤي بالنفي. إذ لم يكن طرفاً في أي مجتمع مغلق.

وبعد عدد من الأسئلة والأجوبة، أدرك ديڤي أن إلليز، لم يكن مستعداً للخوض في هذا الأمر. وبالفعل، تقابل ديڤي وإلليز عدة مرات بعد ذلك. وفيما كان من الممكن لهما أن يقتربا جداً من مناقشة الموضوع، لم يكن إلليز ليكشف القصة تماما» مثلما فعل ذلك بوضوح في أبحاثه. لكن العالمين أصبحا بعد ذلك صديقين. وبعد أن تعرّفت زوجة ديڤي علىإ لليز أكثر فأكثر، أصبح بمقدورها أن ترى بوضوح، الصلة بينإ لليز وزوجها، وتقول ماري فيشر: «كان كلاهما صوفياً».

من يدري ماذا كان يجول في ذهن جيمس إلليز ذلك اليوم؟ فقد كان

رجلاً وقع على فكرة ثورية وعاش ليرى الآخرين، يفوزون بالشهرة لإعادة اكتشافها؛ وتجشم عناء كتابة بحث يعرض لمساهمته وانتظر، بلا جدوى، لكي ينشر في حياته، إنه ذلك الرجل الذي رأى فكرته، عندماقد مها الآخرون، لم تزدهر فحسب بل خُلقت صناعة جديدة ومجتمعاً جديداً أيضاً، وأحدثت تحولاً جذرياً في الموضوع، نقلة نوعية لدرجة أن عالم الظلال لم يعد هو نفسه. إلاَّ أنه لم يكن بمقدوره، ولم يكن ليقوم بذلك، أن يخرق القوانين، ويكشف عن أسراره للآخرين، ولا حتَّى لقرينه في القطاع الخاص.

وفي تلك الحانة، ظل إلليز يدفع بصا حبه ديڤي، لأن يشرب حتَّى الثمالة، بينما كانا يتحدثان في كل أمرو موضوع، إلاَّ الشأن الذي جمع بينهما وأحكم الوثاق بينهما إلىٰ الأبد. ولكن قبل أن ينهي الحديث في الموضوع لم يتمالك إلليز نفسه عن الاعتراف بلباقة، بقول يزيد عن مجلدات، في أمر العالم الذي عاش فيه وعالم الكريبتوجرافيا الذي كان ديڤي يعمل على إقامته.

فقال أبو التشفير غيرا لسري لأبي كريبتوجرافيا المفتاح العام: «لقد أفدتم مما عملنا نحن». ثم لزم الصمت محافظاً على سره.