

## المعيار

في 17 آذار/ مارس 1975، صدرت وثيقة حكومية جافة أحدثت موجة من الصدمات كادت أن تنزع الغطاء عن عملية الشيفرة المتواضعة التي كان يقوم عليها مارتين هيلمان في جامعة ستانفورد. وكانت [الوثيقة] تتضمن الإعلان عن إنشاء مكتب السجل الاتحادي Federal Register، في المكتب القهبي للمعايير NBS National Bureau of Standards إنبي إيس. وبدل ظاهر الأمر، على أنه واحد من مشاريع لا حصر لها في جدول أعمال تلك الوكالة، والتي إن اعتمدت أصبحت لقناة الرسمية في التعامل مع الحكومة، بالإضافة إلى أنها ستغدو المقصد السهل، للصناعة الخاصة، وكل من هبّ ودبّ. وتضمن الإعلان أمراً قلمياً يرد في النشرات العلنية، تقديم خوارزمية تشفير جديدة كل الجدة. وفوق هذا منيعة. وستعرف باسم معيار تشفير البيانات Data Encryption Standard أو اختصاراً DES ديز (كما يلفظ).

كان فريق العمل في ستانفورد قد بلغه أن هذه الخطوة الجديدة آتية بلا ريب - إذ سبق أن وجه المكتب القومي للمعايير (إنبي إيس) دعوات لتقديم مثل هذا المعيار - كما كان هيلمان يعلم أن زملاءه القدامى الموثوقين في آي بي إم، يعملون على وضع نظام موافق لمعيار الحكومة. ولذلك رُحِب الفريق

بالإعلان في بداية الأمر. ويستذكر هيلمان تلك اللحظة: «كان ذلك نبأ عظيماً. فقد أسعدنا أن نجد معياراً يعتمد في هذا الموضوع، وهللنا له باعتباره أمراً رائعاً».

ثم أخذ القوم في دراسة منظومة معيار تشفير البيانات فعلاً - وعلموا أن لوكالة الأمن القومي على ما يبدو يداً في نشوئه. فتحول حماسهم بعدئذ إلى فرع ورعب. وبدا جلياً منذ اللحظة الأولى أن الحل في الـ DES، يكمن في حجم مفتاح التشفير، وكان قياساً مترياً يحدّدها شرة مقدار قوة النظام الكريبتوجرافي. وكان يبلغ 56 بت Bit طولاً، وهو رقم مزدوج لـ 56 موقع. وبوسعك أن تتخيل هذا في صورة سلك فيه 56 قاطع كهربائي لتشغيل أو إغلاق كل واحد منها. ومع أن  $(2^{56})$  هو عدد ضخم في معظم الأحوال، إذ يعني وجود  $(2^{56})$  مفتاحاً محتملاً أو حوالي 70 كدريليون Quadrillion [رقم مؤلّف من 1 وإلى يمينه 15 صفراً. هـ. م] إلا أن هيلمان وديفي ذهبوا إلى أن هذا العدد، يعتبر صغيراً جداً بالنسبة لتشفير عالي المستوى. وكان اعتقدهما الثابت أن الكومبيوترات المتطورة، سوف تجهد نفسها، حتّى تجد الحلول لمثل هذه الرسائل المشفرة، عن طريق «البحث الموسع»: أي تجربة بلايين المفاتيح المركبة بسرعة البرق، حتّى تكتشف المفتاح الصحيح، الذي يجعل الرسالة تنتقل فجأة إلى عالم النصوص الواضحة. وهذا مثال كلاسيكي على «الهجوم بالقوة الغاشمة». ويقول هيلمان: «إن مفتاحاً كبيراً لا يكفل الأمن، لكن مفتاحاً صغيراً كفيف بتعريض الأمن للخطر».

ولقد كتب ديفي هذا المعنى في تحليل مبدئي للمعيار جدير بالاحترام، وقدمه في أيار/ مايو 1975، في نطاق تعليق عام، دعت إليه وكالة الأمن القومي: «إن حجم مفتاح يكاد ألا يكون مناسباً، إلا قليلاً، في أحسن الأحوال. وحتّى في هذه الأيام، فإن لعتاد (هاردوير) القادر على التغلب على النظام بالبحث الموسع، قد يثقل على ميزانية أي منظمة استخبارات ضخمة،

لكثه على الأغلب لن يتجاوزها». وذهب إلى القول، أن مؤسسة تتمتع بحرية الإنفاق قادرة على تصنيع آلة، مصممة حسب المواصفات المطلوبة، تستطيع فك أسرار مثل هذا المفتاح في غضون يوم واحد. وكتب يقول: «رغم أن تحليل الشيفرة عن طريق البحث الموسع ليس رخيصاً، لكنه مع ذلك ليس مستحيلاً. بل إن أقل تحتمن يطرأ على أسلوب تحليل الشيفرة، كفيل بأن يغير من التناسب بين الكلفة والأداء. إننا نقترح مضاعفة حجم مجال المفتاح حرصاً على منعة النظام».

اعتقد ثنائي ستانفورد عن سذاجة، أن حكومة الولايات المتحدة ربما ستأخذ بهذه النصيحة: حسن، الواقع أنكما مصيبان فيما ذهبتما إليه! فلنضعف حجم ذلك المفتاح السخيف! ولكن ما حدث أن استجابة لحكومة جاءت على قدر من المراوغة، مما حمل هيلمان على الارتياح بحقيقة دوافع المكتب القومي للمعايير. ثم أخذ هيلمان في الشهور اللاحقة، يشكك علناً في تلك الدوافع، متسائلاً إذا لم تكن خوارزمية معيار تشفير البيانات، خدعة جريئة من جانب الحكومة، لا لتضليل المواطنين فحسب، بل الأعداء الخارجيين كذلك، وإيهامهم بأنها تقوم بحماية المعلومات من التسرب، في حين أن وكالة الأمن القومي تستطيع الوصول إلى هذه المعلومات التي يفترض بأنها في حوز أمين. وتساءل هيلمان؛ وهو في أقصى درجات جنون الشك، إن لم يكن لمعيار التشفير «باب خلفي» زرعه فيه الكريبتوجرافيين الدهاة في فورت ميد. ومع أنه ليس هناك دليل مباشر على صحة هذا التساؤل، لكن، كان ثمة سبب يبرر الشك. كان هيلمان يريد أن يعرف لماذا تُعامل مبادئ تصميم الخوارزمية وأعمالها الداخلية كأسرار حكومية، إذا كانت الأمور مطروحة علانية، وتجري أمام الملا؟ ثم، إذا لم يكن لدى الحكومة ما تخفيه فلماذا تقومياً خفاء بعض الأمور؟

كان هيلمان وديفي أول من طرح التساؤل حول الأصول الملتبسة لمعيار

تشفير البيانات. إذ استمر الجدل حول هذا المعيار حتى حينما أصبح شبيهاً بمعيار الذهب في تحديد منعه الكريبتوجرافيا التجارية، وغداً موضوعاً لشكٍّ دائم بين الغرباء عن عالم الشيفرة والحريات المدنية. ولم يتضح أن نشوء وإجازة معيار التشفير كان بمعنى معين قصة ملهمة إلا بمرور الزمن، قصة ذات عناصر مشتركة مع البحث الذي كان يقوم به ديفي وهيلمان.

بدأت القصة مع أحد أشد الباحثين غموضاً في شركة آي بي إم IBM هورست فايشتل. كان هذا لا اختصاصي بكتابة الشيفرة الألماني المولد والذي عمل في وضع قواعد برنامج التحقق من الصديق والعدو هو الذي اطلع عليه هويت ديفي عن طريق ألان تريتر. وكان فايشتل يعمل في قسم البحوث لدى شركة آي بي إم في يوركتاون هايتس منذ أواخر الستينات، وعمله من الأعمال القليلة في القطاع الخاص التي تُعنى بالبحث في الكريبتوجرافيا.

والحق أن بعض زملائه راودهم الشك بأن فايشتل كان يعمل في خدمة وكالة الأمن القومي، ولعلهُ ما زال مرتبطاً بها بشكل من الأشكال، حتى أثناء عمله في شركة آي بي إم. ذلك أن سيرته الذاتية لا تنبئ، بالكثير. وما يُعرف عنه، أنه وُلد عام 1914 وغادر ألمانيا شاباً. وكانت عمته قد تزوجت من يهودي سويسري يقيم في زيورخ، وانضم إليهما فايشتل بحجة العناية بالعمّة في مرضها، قبيل بدء الرايخ الثالث بالتجنيد، ولولا ذلك لما أمكنه الهرب من ألمانيا. وبعد دراسته في سويسرا رحل إلى الولايات المتحدة عام 1934. وقبيل أن يكتب الجنسية الأمريكية، دخلت الولايات المتحدة الحرب العالمية الثانية، فوضع قيد ما وصفه ذات يوم بـ «الإقامة الجبرية» بما تقتصر تحركاته على منطقة بوسطن حيث كان يقيم. لكن أحواله تغيرت فجأة، ففي كانون الثاني/يناير 1944، مُنح الجنسية الأمريكية بالإضافة إلى حصوله على إجازة أمنية ووظيفة في موقع ليغ ا لحساسية، مركز كمبردج للبحوث التابع لسلاح الجو.

أما طبيعة عمله في ذلك الموقع فليست واضحة، ولقد كان شغوفاً بالرموز منذ فتوته، لكنّه أسر لديشي في أوائل التسعينات، بأنّه، وإن كان راغباً بالعمل في مجال الشيفرة، فقد أعلم بأن هذا ليس بالعمل المناسب في أثناء الحرب لمهندس ألماني المولد. ولكنّه من جهة أخرى، قال في مقابلة مع ديفيد كاهن أنّه عمل حينذاك على أنظمة التحقق من الصديق أو العدو. لكن ليس في الكريبتوجرافيا حصراً.

ثمة تناقضات في روايات فايشتل الأخرى عن نشاطاته. فقد روى لديشي أنّه كان عليه قبل منحه الجنسية الأمريكية أن يُعلم السلطات كلما غادر بوسطن لزيارة أمه في نيويورك. لكنّه قال لأحد العاملين معه ذات مرة أنّ والدته، لم تهجر إلى الولايات المتحدة حتّى بداية الحرب الباردة. كذلك يروى عنه قوله أنّ الولايات المتحدة هي التي قامت بتفريها من برلين الشرقية، تحسباً للعواقب في حال اكتشاف السوفييت، أنّ ابنها يعمل في مجال الشيفرة وأرادوا الضغط عليها.

إلاّ أنّه من المؤكد أنّ فايشتل، شرع يختص في أنظمة التحقق من الصديق أو العدو (آي إف إف) بعد الحرب. فقد رأس حينذاك مجموعة من الباحثين في الكريبتوجرافيا في مركز كمبردج للبحوث، وكان من مهامه اجتياز نظام تعرّف متطور يعتمد على اختراع جديد مذهل هو: الترانزيستور. وقد أمكن بهذه الأعجوبة الدقيقة تصنيع جهاز آي إف إف صغير إلى حد يمكن وضعه في مقدمة طائرة مقاتلة. وهناك مشروع هام آخر كان شاغل فايشتل لفترة طويلة، هو تصميم نظام تشفير منيع يعتمد على كتلة من الشيفرات. (يقوم هذا النسق على تشفير الرسائل بتقديمها في مجموعات أو كتل، مقابل الشيفرات المتدفقة التي يتم تشفير نصها أثناء جريانه أو تدفقه).

هل أعجبت وكالة الأمن القومي بعمل فايشتل، أم أنّها رأت فيه خطراً فحاولت خنقه؟ حسب رواية فايشتل لديشي، كان العاملون في القلعة، فورت

ميد، قد رصدوا عمله في سلاح الجو، وتوَسَّلوا بسلطة الوكالة لتوجيه عمله الوجهة التي يريدونها، لكن الوكالة اعتبرت مشروعه مصدر تهديد أيضاً، واستطاعت في النهاية القضاء على مشروع الشيفرة كلّه في مخبر كمبردج. ولما انتقل فايشتل في منتصف الستينات إلى العمل في شركة ميتري (شركة التعهدات العسكرية التي قامت فيما بعد بتوظيف هويت ديفي)، حاول دونما طائل تنظيم مجموعة هناللا ستئناف عمله في مجال الشيفرة. وقد عزا فشله للضغط الكبير الذي مارسه وكالة الأمن القومي لإحباط مشروعه.

ولذلك أخذ بنصيحة صديقه. آ. أدريان ألبيرت، ومضى ليعمل في شركة آي بي إم، التي بدت أكثر انفتاحاً للآخذ بمثل هذه الاهتمامات. (كان ألبيرت رياضياً، ويرأس الجمعية الأمريكية للرياضيات، وله باع طويل في كريتوجرافيا في الحكومة). وكانت شركة آي بي إم غنية إلى حدٍ يثير الدهشة، ومنافسوها قلائل، وكان قسم البحوث فيها مرتعاً فكرياً يلقي فيه علماء أفاضل، التشجيع للبحث في كل ما يثير اهتمامهم. ويقول آلان كونهايم، الذي غدا رئيس فايشتل في عام 1971: «إن لك الحرية متى عُيِّنت في يوركتاون، أن تفعل ما تشاء، طالما كنت تقوم بعمل ما. ولقد أدّى فايشتل عملاً - إذ صاغ فكرة وضع نظام للكتابة بالشيفرة».

إن الجانب الأكثر مدعاة للإعجاب في ما أبدعه فايشتل، لا يتصل بالرياضيات أو التكنولوجيا - أو حتى منعه أمام محللي الشيفرة - بل الحافز الكامن وراءه. ذلك أنه لم يقصد بالشيفرة المنيعة حماية أسرار الحكومة أو لمراسلات الدبلوماسية، بل أن صيانة خصوصيات لئس وأسرارهم - تحديداً قاعدة البيانات للمعلومات الشخصية للأفراد من متطفلين قد يسرقون محتوياتها، ويستخدمونها لضع ملفات شخصية مفصلة عن هؤلاء. وفي مقال لفايشتل نشره في مجلة سينتيفيك أمريكان Scientific American عام 1973 قال: «يشكل الكومبيوتر، أو سوف يشكّل قريباً، تهديداً خطيراً لأسرار لئس



اقتحام النظام بما كتشاف نقاط الضعف في بنيته، واستغلالها فيستعيد النص الواضح دون أن يكلف نفسه شن هجوم بالقوة الغاشمة. ومحلل الشيفرة يستطيع اقتحام النظام، إذا وجد في النص المشفر أدنى قدر من الانتظام. إن قوة لوسيفر شأنه في ذلك شأن أي شيفرة أخرى، تعتمد على منع الخصوم المحتملين من الوصول إلى مثل هذه الطرق المختصرة. ولقد خلت الشيفرة التي ابتدعها فايشتل من التي تنبئ بأسرار النص لأنه أخضع ذلك النص إلى جولة رياضية (حسابية) مضنية، تدور به في دوامة معقدة من الاستبدالات. وفي النهاية، وبعد ست عشرة «دورة» من التبادلات المحمومة مع الحروف الهجائية الأخرى، فإن كلمات النص والجمل تظهر ككتلة من حروف تبدو موضوعة بشكل عشوائي: أي نص مشفر بصورة غير مباشرة.

كانت قواعد الاستبدال الحاسمة يتم تنفيذها بوساطة صندوقين أو (صندوقاً - إس). ولم يكن هذان صندوقين بالمعنى المادي للكلمة، وإنما مجموعتان من المعالات البيزنطية غير الخطية تحدّد الطرق التي ينبغي بها تحريك الحروف. (يعتقد واحد على الأقل من زملاء فايشتل، هو الآن كونهاييم، بأن وكالة الأمن القومي هي التي قدّمت له فكرة لصندوقين - إس، في ورشة عمل أقيمت ذات صيف لتوفير تكنولوجيا يفهمها القائمون على الأمور في فورت ميد، ومن ثم اعتمادها وتعميمها. ويقول كونهاييم في هذا الصدد: «إنهور ست رجل بالغ الذكاء، لكن أحسب أنه كان يتلقّى توجيهاً وإرشاداً».)

إن لصندوقين - إس، لم يأتيا بمجموعة من الاستبدالات المنطقية للحروف وحسب، بل كانليستخذ مان أيضاً لعلو ما ت مستقاة من مجموعة من الأرقام تُؤلف مفتاحاً سريعاً لتغيير السياق كلما مرت التبتات عبر الصندوقين. وكان أمن النظام يعتمد، في النهاية، على هذا المفتاح. فبدون معرفة هذا المفتاح لن يستطيع عدو، ولو عرف كل القواعد التي يعمل بها لوسيفر، أن يحول النص المشفر إلى نص واضح بأسلوب هندسي معاكس.

كان يفترض أن مثل هذه المعرفة بقوانين النظام متوفرة؛ وقد أخذ في الاعتبار الاحتمال القوي بإمكانية معرفة المنتص بتفصيلات الشيفرة التجارية الموزعة توزيعاً حَسناً أكثر مما هو ممكن بالنسبة للشيفرة العسكرية التي يمكن إحكام السيطرة عليها بصورة أشد من الشيفرة التجارية. ومحلل الشيفرة إذ يحاول تفكيك شيفرة عسكرية يفتقد في الغالب للمعرفة بالنظام المستخدم في وضع الشيفرة؛ وتلك معضلة لا تقتضي توفر وقت طويل لتفكيك الشيفرة وحسب، بل معرفة واسعة بوسائل المخابرات السريّة أيضاً. وهناك شبكات تجسّس ضخمة، تتركّس جهودها لمعرفة أنواع الرموز التي يستخدمها العدو. ومن جهة أخرى، إذا قرّر بنك تسييس مانهاتن استخدام شيفرة آي بي إم لتشفير معاملاته المالية، فإن بوسع محتل أن يكتشف نظام التشفير الذي يستخدمه البنك. ولما كان ثمة احتمال بأن تحيز آي بي إم لأطراف أخرى استخدام هذا النظام، فإن قواعد العمل به تغدو على الأرجح متداولة على نحو واسع. وهكذا فإن السريّة كلها سوف تعتمد، في هذا العصر الجديد من التشفير غير العسكري، على المفتاح.

ولقد سعت شيفرة آي بي إم، إلى امتلاك عدة براءات ملكية للوسيفر وحصلت عليها. وأصبح هذا النظام الذي ابتكر في مختبر واطسون للبحوث التابع للشركة من موضوعات البحث. ولكنّه لم يكن يشبه المشاريع الخيالية السابقة لزمانها والتي كانت تجري في مختبر واطسون، إذ كان ابتكاراً يوفر حلاً فورياً لمشكلة راهنة ملحة - أمن البيانات في عصر الاتصالات - وله موقع طبيعي على درب الاستثمار التجاري السريع. وسرعان ما تحقّق أول تطبيق جاد للوسيفر، في نظام نقطة الدفع، فبنك لويديز في لندن، اعتمده في توزيع العملة الصعبة على الزبائن. ولا ريب بأنه كان إيذاناً بقدم أحداث أضخم لشركة آي بي إم والكريبتوجرافيا معاً. وكانت مسألة وقت وحسب، حتّى يبلغ طفل هورست فايشتل نضجه، فلا يعود مجرد مشروع للبحث؛ بل سيغدو مبادرة كبرى من آي بي إم. ولسوف يغير هذا، المشهد كله.

بينما كان فايشتل منصرفاً لتشذيب وتطوير لوسيفر، كان هناك مهندس في الثانية والثلاثين من العمر، يدعى والتر تكمان، يعمل في فرع آي بي إم في كينجستون، في نيويورك. وكان هذا قد أصبح من الموظفين الدائمين في الشركة بعد أن عمل لديها خلال شهور الصيف الثلاثة من عام 1957، ما بين تخرجه وتأديته الخدمة العسكرية. ولما انتهى من الخدمة الإلزامية، لم تقم آي بي إم بتوظيفه لديها مجدداً وحسب، بل أوفدته أيضاً إلى جامعة سيراكيوز لنيل شهادة الدكتوراه في نظرية المعلومات. وفي حين أن الغالبية من زملائه في الجامعة ظلّوا يتابعون العمل في الحقول الأكاديمية، فإن تكمان اتجلا ستفادة من معرفته في ابتكار تكنولوجيا متقدمة فعلاً، وكان أن لازم شركة آي بي إم، وانتهى بأن ترأس مجموعات الإنتاج.

كانت أحدث مهمة يتولاها تكمان في الشركة، تتصل بضعف غريب في أمن الكمبيوتر، يتجلّى بتسرّب شارات إلكترونية واهنة أثناء اتّصاله بأطراف أخرى وهذا ما يجعل متلصصاً حاذقاً، يستطيع استخلاصها في إعادة بناء المعلومات التي تظهر على الشاشة. وبالنتيجة تمثّل هذه العلامات رسداً غير مشروع لبيانات سلك و صلة التفريغ في الكمبيوتر. وقد طلبت الحكومة ابتكار أداة خاصة توفر لحواسبها الوقاية من هذه التسرّبات الممكنة الوقوع، فاستجابت آي بي إم لهذا الطلب، بابتكار ما أصبح يُعرف باسم تكنولوجيا تمبيست Tempest (العاصفة). واعتبر هذا الابتكار فوزاً عظيماً، وحين أنهت مجموعة تكمان عملها عام 1971، شاء أعضاؤها الاستمرار في العمل معاً، عوضاً عن توزيعهم بين مشاريع مختلفة، وفق الإجراء المعروف داخل الشركة بكلمة التشتيت الألمانية Volkerwanderung. ولكي يحصل ماير يدونه، كانوا بحاجة إلى مهمة جديدة. وكان رئيس تكمان يعلم أن ثمة أموراً مثيرة للاهتمام تجري في قسم العمليات المصرفية، وربما تتطلّب تطويراً وابتكاراً في مجال أمن الكمبيوتر، فاقترح أن يتولى تكمان وفريقه النظر في الموضوع.

ولقد صادف أن موقع قسم العمليات المصرفية في الشركة، كان على الطرف المقابل لمكتب تكمان في كينجتون. وسرعان ما اكتشف تكمان أن رئيسه أصاب، حين استجاب لما أمّلته عليه الغريزة، فبعث به إلى ذلك القسم. وكانت الشركة قد قرّرت بناء على تجربتها في مشروع مصرف لويدز، طرح فكرة كوى للسحب الآلي، حيث يستطيع زبائن المصرف سحب الأموال من حساباتهم دون الاضطرار لمقابلة موظف. وكانت أولى آلات السحب خزائن ضخمة لا تحتوي على الأموال فقط، بل كذلك على كافة الأجهزة الإلكترونية والكمبيوتر، اللازمة لعملية الصرف والسحب، وهي عملية مكلفة وصعبة. وكان الحل الأفضل، نشر البرنامج التطبيقي بين الكوة والكمبيوتر الرئيس في البنك، الذي يتولّى كافة المعالجات المعقّدة. ولم يكن هذا الحل ناجحاً وحسب، وإنما يتفق بعد ما أدركت شركة آي بي إم حديثاً، أن مآل النموذج الأساسي للكمبيوتر سوف يكون مقابر الخردة. ويشرح تكمان ذلك بقوله: «كانت معالجة المعلومات تتم داخل الكمبيوتر الرئيس. وكان الأمن النموذجي يقوم على أن تقفل باب غرفة مكتبك، بعد أن تقفل الإدراج، وأن يتولى حراسة المبنى رجل مسلح بمسدس. أما الآن، فإن أشد الناس التزاماً بالتقاليد في أرمونك يدرك أن معالجة المعلومات سوف تجري مستقبلاً خارج المبنى». وبما أن الحارس المسلح يمكنه التواجد في كل مكان، فلا بدّ من تغيير هذا النموذج من الأمن.

إن نظاماً يضحخ المال فعلاً لكفيل بأن يمثل تحدياً جدياً لأي نمط جديد من التجهيزات الأمنية لدى آي بي إم. فالأوامر الحاسمة التي تضيء الشارة الخضراء للفظ الأوراق النقدية من فئة العشرين دولاراً، سوف توجه مستقبلاً عبر خط الهاتف. وقد أدرك تكمان بسرعة مبلغ خطورة هذا الأمر. تخيل أن محتالاً عارفاً بالتكنولوجيا استطاع دخول خط الهاتف وتمكّن من تقليد الرسائل التي توجه الأمر بـ «ارم فئة العشرين دولاراً!».

وكان العلاج هو الكريبتوجرافيا. ومع أن تكمان درس نظرية المعلومات، فإنه لم يسبق له أن قام بأي عمل في مجال الشيفرة. لكنه سرعان ما اكتشف أمر النظام الذي ابتكره الباحثون في مركز البحوث في شركة آي بي إم في يوركتاون هايتس. وفي أحد الأيام، قام بزيارة مختبر واطسون، وسمع هناك فايشتل يتحدث عن لوسيفر. وللتو، دعا كلاً من فايشتل وآلان كونهام إلى الغداء. وكان أولها فعلة يومئذ سؤال فايشتل عن المصدر الذي استقى منه الأفكار لمشروع لوسيفر. فذكر له فايشتل، بلكنته الألمانية المميزة، دراسات كلود شانون المبكرة قائلاً: «إن أوراق شانون تبين الأمر كله».

وفي غضون ذلك، كان زميل تكمان، كارل ماير يبحث فيما إذا كان لوسيفر يصلح لأن يكون نسخة موسعة للنظام المستخدم في كوي الدفع (الصراف الآلي) في بنك لويدز. وخلص تكمان في النهاية إلى أن لوسيفر قد يحتاج على الأرجح إلى عدد من التعديلات قبل أن تتوفّر له المنفعة الكافية، بحيث يمكن الاعتماد عليه. لكنه يصلح الآن ليكون بداية جيدة. وهكذا تم الاتفاق بين آلان كونهام، ومجموعة نظرية لمعلو مات على أن يتولّى تكمان وفريق ماير في كينجستون، وضع خوارزمية منقّحة للوسيفر وإرسالها من ثم إلى يوركتاون لتقويمها واختبارها.

كان الاسم الذي عُرفت به الشيفرة هو: دي إس دي - DSD-1، قبل الموافقة على هذا الترتيب سأل أحد كبار المدراء في آي بي إم، عما يحمل هؤلاء الباحثين على الانشغال بلوسيفر، وهو يعرف أن ثمة خوارزمية أقل كلفة وأسرع عملاً. فقام تكمان بأخذ هذه الخوارزمية التي يفترض بأنها الأفضل إلى بيته، وفكّكها أثناء العطلة الأسبوعية. (وكان أن نشر وماير عملية التحليل في مجلة التجارة داتاميشن Datamation. ومنذ ذلك الحين، دأب تكمان على الإشارة إلى هذا لنصر بوصفه برهاناً على معرفة فريقه بما يفعلون - وليضمن عدم توقف العمل نتيجة تدخلات لا سند لها من المعرفة من المدراء في الطوابق

العليا. ويذكر أنه قال ذات مرّة لأحد المتسلطين الكبار، هؤلاء الذين يمكنهم بلقمة العيش: «إننا لا نستطيع التعامل مع هواة في الحقل. وليس هناك من طريقة رخيصة للقفز فوق خوارزمية الشيفرة. بل عليك أن تعمل وتعمل وتتاير على العمل، ثم أن تدقّق وتمحص وأن تكون مؤهلاً لذلك، وسوف يستغرق هذا وقتاً طويلاً».

وكانت هذه عملية صعبة إلى حد بعيد - كما كان يمكن لهويت ديفي أن يقول لمجموعة كينجستون - وذلك بسبب الافتقار للمعلومات اللازمة لتصميم نظام تشفير حديث له قوة نظام التشفير لعسكري. وفي ذلك قال تكمان متهدداً: «كان هذا كله من الأسرار المحظور الإطلاع عليها. بيد أننا استوعبنا من دروس الرياضيات السرّ الذي يجعل شيفرة ما عصية على الحل». ولقد قرأ أعضاء فريق العمل كل ما في المكتبة، لكن كان أكثر ما وقع بين أيديهم فائدة وعوناً هو، كما تنبأ فايشتل، أبحاث شانون. ثم محاوراتهم مع فايشتل ذاته. بيد أن أكثر ما شُغلوا به كان إعادة اكتشاف ما يعتبر من المعارف الشائعة لدى نساج الخوارزميات في فورت جورج ميد. ويقول تكمان: «كنا نجلس في غرف الاجتماعات، ونشغل بالكتابة على السبورة ونعلم أنفسنا».

وسيكون الوضع مثالياً لو أمكن انتقال فايشتل إلى كينجستون، وضمه إلى الفريق. ولذلك، لم ينقطع تكمان عن سؤال كونهائم: «ماذا يريد هورست أن يفعل؟ لسوف أو فر له غرفة مكتب جيدة خاصة به، وله أن ينتقل إلى هنا». وكان كونهائم يجيب: «لا، لا أعتقد أن هذا الترتيب سيكون له حظ من النجاح».

وأخيراً، أدرك تكمان السبب. وقد قال فيما بعد: «كان هو ست نسخة أوروبية عن جيمس ستوارت في فيلم «هارفي»، كائنات يعيش في عالم سحري صغير، موزعاً بين ما يجري في مؤسسة تجارية مثل آي بي إم، وهواياته. إنني لم أشعر أن هورست كان يفهم حقيقة عالم التجارة والمال - وخاصة عالم

التجارة في التكنولوجيا المتقدمة. كان يعيش معتكفاً، منكباً على البحث في يوركتاون، بينما كنا، نحن المجانين من كينجتون، المستعدين فعلاً لصنع منتجات، نبحت إن كان بوسعنا أن نقوم بشيء يأتي بالمال».

يوافق كونهيم على أن فايشتل كان في غير محله، في عالم التجارة، بل يتبين له مع مرور الزمن، أنه في غير موضعه في قسم البحوث من ذلك العالم أيضاً. ويروي كونهيم أن فايشتل اعتاد، منذ أن أصبح لوسيفر بيتعد عنه كاختراع له، ويزداد بروزاً كمنتج تجاري من آي بي إم، التأخر في الوصول إلى مكتبه في يوركتاون، فلا يعمل في مشروعه، بل يمضي سحابة يومه في إجراء المكالمات الهاتفية، بالألمانية. ويذكر كونهيم أن عمه فايشتل العجوز وعدته بإرث كبير، فكان يمضي الكثير من الوقت في التحدث معها بالهاتف لاسترضائها. (أصيب فايشتل بخيبة أمل مريرة، والعهد على كونهيم حين توفيت العمه بعد سنوات عديدة دون أن تخلف له شيئاً).

يعتبر المقال الذي نشره فايشتل في مجلة سيتيفيك أمريكان عام 1973، واحداً من أكثر الوصوفات العلمية، للكتابة بالشيفرة وضوحاً، التي عرضت للجمهور منذ سنين - ويمكن تفسيره بأنه ضرب من التمرد. وبالتأكيد، أن مثل هذه الصراحة التي تناول فيها المقال الخفايا الكريبتوجرافية لمادة تعتمز شركة آي بي إم إنتاجها كان حرياً بها أن تشير في بعض الأوساط، أكثر من مجرد الاستغراب. فقد اعترضت وكالة الأمن القومي ذاتها، على ما يبدو، على نشر المقال؛ وأشار فايشتل إلى ضيق الوكالة بالمقال، ملاحظاً أيضاً أنها كانت ستسعى لإسدال الستار على مشروع لوسيفر برمته، كما سبق أن فعلت مع مشاريع أخرى له، لولا فضيحة ووترجيت يومذاك التي قلبت واشنطن عاليها سافلها.

أما مجموعة كينجتون، فكانت لاهية عن مثل تلك المؤامرات. فقد كان الأمر بالنسبة لهم، أن لوسيفر مجرد منتج قيد التطوير. فعملوا على التركيز على

هدف تعديل النظام وزيادة تعقيده، وصعوبته، بحيث يتمكن النص المشفر الصادر عنه من اجتياز اختبارات شانون لعشوائية المعلومات لظاهرة. وكانت أول خطوة وضع قائمة بما أطلقوا عليه اسم استكشاف المؤهلات، وهي سلسلة من الاختبارات الرياضية التي تقيّم مخرجات نظام الشيفرة - لر سالة المعماة - بحيث لا تحمل علاقة ظاهرة بالرسالة الأصلية، فتبدو كمجموعة من الحروف المرتبة عشوائياً. وتكون محصلة محتوى المعلومات الظاهرة، في مصطلح كلود شانون صفرأ.

من المؤكد أن نسخة فايشتل من لوسيفر، حاولت أن تبلغ هذا الوضع المثالي، لكنّها ظلّت دون هذا لهدف المنشود. وكان أقوى مكوناته صندوق - إس، حيث تتم أعقد الاستبدالات، أي التحولات اللاخطية المصمّمة لدفع محللي الشيفرة إلى الجنون. فقرّرت مجموعة كينجستون تزويد النموذج الجديد المطور من لوسيفر دي اس دي - 1، بصناديق استبدال أشد مرواغة ودهاء. وتقرّر زيادة عددها من اثنين كما في لوسيفر إلى ثمانية.

وزاد من تعقيد ذلك الجهد، ما طلب توفيره في النسخة الجديدة، وهو أن تكون مدمجة وسريعة. فكان المطلوب على حد تعبير تكمان، أن تكون هذه النسخة «زهيدة الثمن وسريعة». ولتوفير هذه المتطلبات كان ينبغي استيعاب الخوارزمية كلها في رقاقة chip واحدة. وهكذا تم توزيع جزء آخر من الفريق، ويعرف باسم مجموعة في إل إس أي VLSI، اختصاراً لـ Very Large Scale Intergration الدمج/ التكامل الواسع النطاق، بين مختبرات كينجستون وآي بي إم في بيرلنجتون بولاية فيرمونت، وقد أنيطت بهذه المجموعة مهمّة وضع نظام التشفير كلّ في رقاقة واحدة بحجم 3 ميكرون. وكان من المقدّر أن تخرج لشركة - إن سارت الأمور على ما يرام - بأصغر وأقوى آلة تشفير عرفها العالم.

ولقد قَدَّم فريق كينجستون وهو يعمل ضمن هذه الشروط، نسخة دي إس دي -11 لمعقَّدة، والتي ما زال يُشار إليها حتّى لك الحين با سم : لوسيفر . وكان مقدراً، إن سارت الأمور جيداً، أن يستوعبوا سيفر الجديد كتلة من نص واضح يتألَّف من 64 بت، ثم يعالجها عبر عملية مضمّنة من تغيير مواقع الحروف والتكتيل، والتوسيع، والربط، والاستبدال الذي يعتمد على مفتاح رقمي Digital Key، ثم تكرر العملية خمس عشرة مرة أخرى، ليكون المجموع ست عشرة دورة. وتكون المحصلة 64 بت، مما يبدو ضرباً من فوضى رقمية، حشد لا يمكن أن يعود للا نظام، إلاً بواسطة شخص يقوم بعكس عملية التشفير باستخدام المفتاح الرقمي لذي حدّد الكيفية التي تمّت بها عملية التعمية بخلط الحروف .

وبعد هذا، كان فريق مختبر واطسون يتولّى محاولة القيام بالهجوم للتحقق من سلامة العملية برمتها .

ومع أن هورست فايشتل، لم يكن معنياً ببناء النموذج دي إس دي -1، فقد ساعد زملاءه في البحث على تسريع عملية الاختبار. وفي 11 كانون الثاني/يناير 1973، جمع فايشتل خمسة من زملائه في مجموعة أمن البيانات في بوركتاون هايتس، وعرفهم لأول مرة على شيفرة لوسيفر. وقد أثار أحد أعضاء المجموعة، وهو ألان تريتر (عالم الكمبيوتر الغريب الأطوار ذاته الذي عرّف هويت ديفي إلى أصول نظام التحقق من الصديق أو العدو آي بي إف) شكوكاً حول جدوى المشروع برمته. فهل تريد شركة آي بي إم أن تجازف بوضع نفسها في خطر، في محاولتها أن تكون قوة في عالم الكريبتوجرافيا التجارية الجديدة؟ وماذا لو أمكن تحطيم شيفرلوق سيفر؟

أثارت هذه الملاحظات التي أبدتها تريتر الاهتمام، إذ بدت صدق لبعض الملاحظات التي أوردها أحلاماً سائذة في جامعة كيس ويسترن ريزيرف،

ويدعى إدوارد جلاسر، وإن لم يأت بدليل على صحتها. فهذا الرجل الكفيف، وهو واحد من سلسلة لا حصر لها من لمتشارين الذين توظفهم شركة آي بي إم بميزانيتها غير المحدودة، ادعى حسب رواية كونهمايم، بأنه لو أعطي عشرين نموذجاً من نصوص مشفرة مع النص الأصلي الواضح (وهو ما يُعرف بالهجوم على نص واضح منتقى) لاستطاع تفكيك نظام لوسيفر. (تبين فيما بعد أن ذلك زعم خادع مقبول في ظاهره وحسب).

لكن الفكرة فهمت على نحو جيد، وقد كترها تريتير في مذكرة وضعها في وقت لاحق من ذلك العام. فكتب فيها: «قد كنا/ نحن في وضع مكشوف على نحو غير مألوف». وأبرز في ملاحظته حول استخدام لوسيفر لأول مرة في كوة الصرف في بنك لويدز، العواقب المترتبة إذا ما ترك النظام مكشوفاً على نحو ما، شأنه في ذلك شأن الكثير من الأنظمة التي سبقته والتي كانت تبدو «منيعاً». وكتب في ذلك يقول: «إذا استطاع شخص إنجاج مفتاح يصلح لشفرة لوسيفر، فلسوف يقبض له النجاح بالتأكيد إن قام بمحاولة ذكية وحسنة الإعداد وهذا استخدام القوة بتفريغ كافة كوى الصرف الآلي للنقود من محتوياتها أثناء العطلة الأسبوعية».

أثارت هذه الملاحظات التي أبداهاتريتير الاهتمام، إذ بدت صدى لبعض الملاحظات التي أوردها أحد لآ ساتذة في جا معة كيس ويسترن ريزيرف، ويدعى إدوارد جلاسر، وإن لم يأت بدليل على صحتها. فهذا الرجل الكفيف، وهو واحد من سلسلة لا حصر لها من لمتشارين الذين توظفهم شركة آي بي إم بميزانيتها غير المحدودة، ادعى حسب رواية كونهمايم، بأنه لو أعطي عشرين نموذجاً من نصوص مشفرة مع النص الأصلي الواضح (وهو ما يُعرف بالهجوم على نص واضح منتقى) لاستطاع تفكيك نظام لوسيفر. (تبين فيما بعد أن ذلك زعم خادع مقبول في ظاهره وحسب).

إلا أن مثل هذه الخسارة، إنما كانت بداية ذلك النوع من المخاطر التي تواجه شركة آي بي إم بأخذها بالوعد الضمني بالأمن الذي حملته الكتابة بالشيفرة. وليست المشكلة هنا في التعويض لبنك لويديز عن خسارته، ولو بلغت أكداً من فئة العشرين دولاراً، فذلك في استطاعة الشركة العملاقة، بما لديها من احتياطي ضخمة من النقد. فالأدعى للقلق هو استعادة ثقة الناس متى فقدت. ثم هناك، بعد، الدعاوى والمحاكم.

ولقد كتب تريتر: «لو قدر انتهاك أمن [لوسيفر] أو أي منتج مشفّر قد نظرته لاحقاً [للتداول]، وذاع السر، فإن الضرر الذي سوف يلحقه بنا هذا الأمر في السوق يفوق الحصر. فضلاً عن الأضرار الفعلية والاحتمال المائل بدفع تعويضات ضخمة، بقرار من المحكمة بعد الادعاء والمقاضاة في قضية ستكون الشغل الشاغل للصحافة والصناعة والجمهور».

ومن جهة أخرى، يبرز السؤال: هل بوسع شركة آي بي إم صرف النظر عن متابعة الكريبتوجرافيا؟ لقد كان عملها عصراً لمعلومات، وليس بوسعاً لشركة تسويق مثل هذا العدد الكبير من الكمبيوتر، إن لم توفر وسيلة لحماية البيانات وهي تتقل من كومبيوتر إلى آخر. وإذن، فإن الافتقار إلى الكريبتوجرافيا، يشكل عقبة يحسب حسابها أمام تعميم الكمبيوتر أمريكياً، والعالم ذاته. فتم عقد اجتماع على مستوى عالٍ في 5 شباط/فبراير عام 1973، لمراجعة «أحوال الكريبتوجرافيا والخطط الموضوعة لأجلها، داخل شركة آي بي إم برمتها». وكما قال تريتر في تلخيص ما تم في الاجتماع فيما بعد: «بدا أن ثمة اتفاق عريض... على أن آي بي إم غدت ملتزمة إلى الأبد بموضوع الشيفرة، ولا بد لها من امتلاك الخبرة من عدة حقول في هذا المجال. وفي الوقت ذاته، فإن الهجوم على لوسيفر سيكون أكثر حدة».

ولقد جرى ضم خبير من خارج الحلقة هو جيم سيمونز، الأستاذ بقسم الرياضيات في جامعة نيويورك في ستوني بروك، وكان قد مارس الكريبتوجرافيا في معهد تحليل الدفاع، التابع لوكالة الأمن القومي في جامعة برنستون، للقيام بهجوم مركّز على لوسيفر لاختباره. فعمل يومئذٍ إلى جانب ثلاثة باحثين من يوركتاون هايتس طوال سبعة أسابيع من أواخر ربيع عام 1973. ولم يكن هذا العالم قد أصدر تقريره بعد، حين أخذ المعنيون في الشركة يشيرون الأخبار الطيبة، وهي أن سيمونز ورفاقه لم يتوصّلوا إلى قهر لوسيفر.

كتب سيمونز في تقريره المؤرخ في 18 آب/ أغسطس 1973: «إن آلة لوسيفر أشد منعة مما قدرت أصلاً». لكنّه مع ذلك، لم يمنح لوسيفر خاتم المصادقة عليه. وقد خلص سيمونز في هذا التقرير إلى القول: «يبدو من المستبعد أن يتمكن طالبان في المرحلة الثانوية، من التغلب على لوسيفر في إطار بحث في مادة العلوم. ولكن من جهة أخرى ليس لدينا ما يكفي من الدلائل للثقة بأن لوسيفر لن يلين تحت ضربات جيدة التنظيم اولتسديد، يوجّهها محلّ شيفرة محترف». وكان القلق يساور سيمونز من إنه إذا وُضع لوسيفر، وهو في حالته الراهنة، للاستخدام في الأغراض التجارية، فمن المحتم تقريباً استخدامه لحماية «نقل أشياء ذات أهمية حقيقية» (مثل المال والأسرار المهنية)، وهذا ما يوفّر الحافز للقيام بجهد لا بدّ وأن ينجح في النهاية لاختراعه. وهكذا، فإن لوسيفر، إن بدا لـ أي بي إم بداية طيبة، فإن على الشركة، كما قال سيمونز محذراً أن تجهد أكثر لتخرج بنتائج محسّنة. وخلص في تقريره إلى القول: «الواقع أنّه ليس ثمة خيار آخر».

وفي غضون ذلك ظلّت الشركة تتساءل، إن كان لوسيفر سيصمد أمام

الامتحان. ففي مذكرة سرية صدرت في شهر أيار/ مايو 1973، شدّد كبير العلماء لويس برانكومب، وهو يلخص إجماع اللجلا ا استشارية العلمية، على ضرورة قيام الشركة بـ «إرساء بنية كريتوجرافية، وتكنولوجيا، واستراتيجية إنتاج موحدة». وكتب، إن لوسيفر ليس بالمرشح الوحيد في هذا. ولكنه اعتبر في مذكرة أخرى أن خطة مجموعة كينجستون هي الأفضل، مع تحذير واحد: «إلا أن يكون ثمة دليل واضح على وجود ضعف ذي أهمية».

استمرت الاختبارات عدة شهور، وكان يقوم بها باحثون من القطاع الخاص بتكليف من الشركة. ويصف تكمان ذلك بقوله: «كان ألان يقدم لهم الخوارزمية، قائلاً: «هيا فكوها! كل ما أطلبه منكم تفكيكها وحسب». ولا ينقطع عن القول، وهو يعود ليقدم تقريره: ما ملحد ا استطاع أن يجد فيها ثغرة. وأخيراً وصلت إلى النقطة السيكلوجية لسحرية، ورأيت أن هذه الآلة لا تعاني من أي ضعف، وإذن، فليس ثمة حل مختصر لتفكيكها. وقلت للباحثين: دعكم من هذا يا شباب، ولنركّز على تطبيق هذا المنتج الآن».

ومع ذلك، فإن معظم أساتذة الرياضيات الذين كانوا يتلقون روايتهم ليناطحوا لوسيفر يعتبرون هواة بالمقارنة مع محللي الشيفرة العالميين خلف السور الثلاثي. فكيف يمكن للشركة الوثوق بسلامة الخطة فعلاً؟ فالشركة ما كانت بالتأكيد راغبة في معرفة نقاط ضعف لوسيفر، ثم أن تكتشف ذات يوم أن محلل شيفرة كان يعمل في المخبرات السوفيتية كي جي بي سابقاً، ويعمل لصالح المافيا حالياً قد استطاع تنظيف خزائنها من النقود.

في بداية عام 1974 قدر تكمان أن فريقه قطع نصف الشوط من العمل. وفي هذا يقول: كانت لدينا فكرة جيدة عن كمية الخوارزمية التي يمكن تحميلها لرقاقة واحدة». وكان معظم هذه الخوارزمية قد تمّت كتابته. ولكن حدث في ذلك العام أمران كان لهما الأثر العميق على المشروع. الأول جعل

هذا المشروع علنياً وطرحه على الملأ، والثاني ألقى عليه ظلاً خفياً من الشك، قدر له أن يستمر جيلاً من الزمن.

لم تكن أي بي إم المؤسسة الوحيدة التي أدركت الحاجة لما سمة للحماية الكريبتوجرافية في عصر الكومبيوتر. فقد كان يشاركها هذه لنظرة المكتب القومي للمعايير، وهو الوكالة الحكومية التي تتولّى وضع المعايير الصناعية التجارية. فقد كان البيروقراطيون والعلماء هناك يعتقدون بضرورة تركيزاً لحماية الرقمية في نظام واحد، أحسن اختباره في تشفير المعلومات، ويمكن للناس كافة استخدامه. ولذلك قرّر المكتب القومي للمعايير طلب خوارزمية تشفير قياسية. (رفضت وكالة الأمن القومي تقديم حدى الشيفرات التي تستخدمها خوفاً من اطلاع الغرباء عليها، وهذا من المحرمات التي لا يمكن التفكير في انتهاكها). وفي 15 أيار/ مايو 1973، نشر المكتب القومي للمعايير في مجلة فيدرال ريجيستر، عدداً من المعايير الدقيقة التي ينبغي توفرها في هذه الخوارزمية لقياسية.

ولم يكن مفاجئاً، أن المكتب القومي للمعايير، لم يتلق في ذلك الحين أية عروض تلبّي تلك المعايير المطلوبة، ولو بشكل مبهم. ذلك أن معظم المختصين بالكريبتوجرافيا، والوحيدين الذين لديهم المقدرة والخبرة لقبول هذا التحدي، كانوا يعملون خلف السياج الثلاثي، وكانت بحوثهم التي يجرونها هناك لا تنشر ولا يكشف عنها.

ومع ذلك، فقد كان ثمة نظام تشفير واحد قيد التطوير بدا ملبياً للكثير من احتياجات الحكومة، هو لوسيفر دي إس دي - 1. ورأى لويس بلانسكو مب، كبير العلماء لدى أي بي إم - وكان هو نفسه، وليس من قبيل المصادفة، رئيساً سابقاً للمكتب القومي للمعايير - على وجه الخصوص، أن هذا العمل الذي يجري تطويره، يمتلك المقومات اللازمة لمعيار التشفير اللازم للجيل القادم.

كان والت تكمان مناهضاً لهذا الرأي بسبب المقايضة التي ينطوي عليها طرح لوسيفر المعدل كمييار فيدرالي، إذ يقتضي أن تتنازل الشركة عن حقوق الملكية الفكرية، وهذا يعني بالضرورة تقديم الخوارزمية - وليس بيعها - للعالم. وفي هذا يقول: «كنت من هذا النمط النموذجي لمدير مبيعات رأسمالي. إنني أعمل في هذا المشروع لأجني المال، وليس لرعاية حركة اجتماعية عظيمة». وذلك ما عرضه تكمان أمام أحد كبار مدراء آي بي إم، بول ريزو، الذي كان يحتل يومئذ المنصب الثاني في أعلى السلم في الشركة العملاقة. كذلك عرض برانكومب وجهة النظر الأخرى المتمثلة في جعل الاختراع عاماً. وأخيراً تدخل ريزو في النقاش الدائر، مشبهاً لوسيفر بعنصر أمان، فهو إذن مفيد للمجتمع كله. وكانت حجته هي: إذا استطاعت شركة فورد أن تنتج حولاً للأمان أفضل مما لدى منافسيها، وفيه نجاة الأمهات والآباء، فهل كانوا سيسمحون لجنرال موتورز أن يستخدموه في سياراتهم؟ الأفضل أن تعتقد بأنهم سيفعلون ذلك، لأنه رأي صائب. إن [الممثل الشهير بخطاباته المؤثرة] جيمس ستيوارت ما كان ليستطيع أن يأتي بموعظة أقوى من هذا البيان، ولقد كان بوسع المرء سماع الكمان وهوي عزف أعذب الألحان، حين انتهت الخطبة. ولم يقنع هذا الحديث مجلس إدارة الشركة وحسب، بل امتد أثره إلى تكمان ذاته، الذي دعا إلى اجتماع عند عودته إلى كينجستون، ليقول لجماعته «حسناً يا شباب، لنا سوف نتخلى عن هذا الذي بين أيدينا».

ولم يكن معنى ذلك التخلي عنه كلياً، طبعاً. فالطرق التي استخدمت في تحويل لوسيفر إلى رقاقة، والأساليب التي سوف ينفذون بها الآلة في إطار حل كامل، والحيل الصغيرة التي تمكنهم من استغلالها إلى أقصى حد... هذه كلها، تشكل مواد تجارية مربحة للنسخ التي ستبتكرها آي بي إم عن الأصل دي إس دي - 1. أما الشركات الأخرى، فلن يتاح لها إلا الحصول على الخوارزمية

ذاتها. وإذن فُزبَ ضارّة نافعة، ولربما أتى التخلي عن الآلة وطرحها على الملاء بربح وفائدة، من وجهة النظر التجارية.

كان الشعور السائد في شركة آي بي إم، أن مجرد تسليم صيغتها للمكتب القومي للمعايير، كان كافياً لتتويج دي إس دي - 1، كمعيار ومثل يُحتذى. ومع أنا لموعد المحدّد لتقديم الاستجابة لطلب المكتب القومي للمعايير لتقديم عروض لخوارزميات تشفير في عام 1973 قد انتهى، قبل فترة طويلة، فقد كتب برانسكومب لخليفته في المكتب القومي للمعايير، روث ديفيس في تموز/ يوليو 1974 يعرض ما وصفه بـ «خوارزمية شيفرة بمفتاح تحكّم» تم تطويره في لينجستون. ولما وجد المكتب هذا المرشح الجديد لأثير مطروحاً للمنافسة، كزّر الإعلان عن طلب عروض لخوارزميات تشفير، وقد نشر هذا الإعلان في مجلة فيدرال ريجيستر، بتاريخ 27 آب/ أغسطس 1974. ولم يبرز يومئذ أي منافس. وهكذا قدر للوسيفر المعدل دي إس دي - 1، أن يعرف باسم جليل وإن كان ينم عن أصله معيار تشفير البيانات Data Encryption Standard. ولقد غدا هذا الاسم معروفاً بين الراسخين في علم الأرقام، حتّى أنّهم لم يأخذوا باسمه للمركب الكامل، بل شرعوا يشيرون إليه بلفظ مختصر: ديز Dez.

وفي ذلك الوقت، كان ثمة تطوير دقيق آخر يتصل بتحول لوسيفر. وجرى ذلك في بدايات عام 1974 حينما تلقى والت تكمان ما صار يصفه لاحقاً بـ «تلك المكالمة الهاتفية القاتلة». وكان للمتحدّث رئيسه، الذي أخبره بأنّه مضطر للقيام برحلة إلى مقر وكالة الأمن القومي لتهدئة خواطر القوم هناك، مما أثاره لوسيفر بينهم.

لم يجد تكمان في هذا الحديث ما يطمئن فؤاده. لكنّه أدرك أهمية مسابقة العم سام (الحكومة الأمريكية). فالحق أن شركة آي بي إم كانت تدخلها نتاجها مادة تربتوجرافية للقطاع التجاري أرضاً غريبة. وإذا لم تنل إجازة التصدير اللازمة لإرسال رقاقة الشيفرة إلى الزبائن في مختلف أرجاء العالم، فالأجدر

عندئذٍ صرف النظر عن هذه الصناعة. فما هي الفائدة من منتج لشركة عالمية مثل آي بي إم تشمل عملياتها الكرة الأرضية، إن لم تستطع بيعه في السوق العالمية؟

ولذلك مضى تكمان ليقوم بأول زيارة له إلى فورت ميد. وتأمل بعينه السياج الثلاثي وأفراد الحرس من مشاة البحرية، ثم أوقف سيارته في المكان المخصص للزائرين، ودخل المبنى الصغير المشيد بالإسمنت المسلح، حيث على الغرباء الذين لا يحملون إذناً مسبقاً بالزيارة، ملء كمية من الأوراق ثم الانتظار لاستدعائهم. وبعدئذٍ جاءته سيدة متقدمة في السن وسارت به في متاهة من الممرات ليصل إلى أحد المدرء من المرتبة الثانية هو المكلف بالقضية، ويأتي بعد نائب المدير مباشرة. ولم يكن الرجل يرتدي اللباس العسكري أو حتى بذلة رسمية. وأسرع يعرض اتفاقية بالمقايضة: إننا نريد أن تكون لنا السيطرة على تنفيذ هذا النظام. أنتم تقومون بتطويره سرّاً، ونحن نتابع عملكم ونقترح التغييرات. إننا لا نريد أن يتم تسويقه في برمجيات مشفرة، بل في رقائق وحسب. ثم إننا لا نريد أن يصدر إلى بلدان معينة على الإطلاق، وسوف نسمح لكم بتصديره إلى البلدان الواردة أسماؤها على قائمة إجازات التصدير فقط، إذا ما حصلتكم على رخصة التصدير. ومنح تلك الإجازة مشروط بتوقيع الزبائن الذين نوافق عليهم على تعهد بعدم إعادة تصدير المنتج إلى أي طرف آخر.

استمر الكلام على هذا المنوال لفترة من الوقت، حتى أتاحت لتكمان الفرصة للرد. فسأل ممثل الوكالة، وقد وجده يحصر حديثه بالمحرمات والمحظورات والشروط، وأهمل الحديث عما ستثاله آي بي إم مقابل جهودها: «وهذا مقابل ماذا؟» أجاب رجل وكالة الأمن القومي: «ستتألون بالمقابل شيئاً مفيداً جداً». وكان التعويض قيام الوكالة بإجازة الخوارزمية، بأن يقوم محللو الشيفرة الأعميون فيها بتحليلها واختبارها، فإذا لمسوا ضعفاً، رصدوه، ثم

عمدوا إلى تقويمه . وعندما تمضي الزوبعة الرياضية تنال الشركة إجازة لا تُقدَّر بثمن، ترخيصاً يكفل نيل ثقة الزبائن: خاتم المصادقة من وكالة الأمن القومي بأن السّر في الحفظ والصون.

كان هذا عرضاً قوياً، لأنه يتوجه إلى أقوى مخلّوف تكمان مباشرة - وهو إمكانية اكتشاف محلّلي الشيفرة الخارجين عن القانون حلاً مختصراً يسمح لهم باعتراض أسرار الزبائن، بل وسلب أموالهم أيضاً، وبذلك يعرّضون الشركة العملاقة ذات الشهرة الأسطورية لخرج على نطاق عالمي و مجزرة قضائية. وهكذا، عوضاً عن اضطرار الشركّلا اعتماد على الهواة النابهين. قليلي الخبرة، في يوركتاون والمشاورين الذين تستخدمهم كيفما تُفق، ها هي ذي يعرض عليها امتلاك منتهى التدقيق والتمحيص: المعيار الذهبي في تحليل النصوص المشفّرة. فكان أول ما قام به تكمان فور عودته من فورت ميد مقابلة رئيسه، ليحثه على «قبول العرض والعمل مع هؤلاء القوم». وكان ذلك حلاً طابت له النفوس في أعلى المراتب، وهم في المقام الأخير مرادفون «للمؤسسة» [الحاكمة]. وهكذا غدا الجهد المنفرد الأهم الذي ينهض به القطاع الخاص في الكريبتو جرافيا في البلاد، لم يكن سوى ذلك العمل الذي كان يقوم به هويت ديفي، وهو ما يزال مغموراً، بعد، ويعارك أفكاره الغريبة في جامعة ستانفورد، ومحورها التوابع الوحيدة الاتجاه، في القبضة الودود، لكن الحازمة، لوكالة الأمن القومي.

كان الأمر المقلق الذي ساور الباحثين يومذاك، احتمالاً اكتشاف وكالة الأمن القومي - وهي ليست، ذراعاً لوزارة لتجارة، بل وكالة استخبارات، وقصر أشباح مطلق - ضعفاً ضحاً في معيار تشفير البيانات، ثم الصمت عنه، وهم مطمئنون ليقينهم بأنّ بوسلهم ستخدّم هذا الدرب الميسّر في تفكيك الرسائل المعماة في شيفرة الشركة. ولقد أدرك تكمان المجازفة الكامنة في هذا الوضع. وأخذ يصدّ لشارات على امتداد الشهور والأعوام لتالية، فيما كان

تطور المشروع يأخذ مداه. وفي النهاية، غدا الرجل مطمئناً إلى سلامة نوايا الوكالة، وفي هذا يقول: «لو أنهم ضلّلوني لنزلت القبر مخدوعاً». ولذلك كنت أرصد هؤلاء القومو جهاً لوجه. إنني من هواة الأفلام و لقد شاهدت من التمثيل الحسن والردىء. ولو خدعني جماعة الوكالة، لضلوا سبيل مهنتهم، وكان ينبغي عليهم الذهاب إلى هوليوود واحتراف التمثيل».

ومنذ تلك اللحظة أصبحت عملية تطوير معيار تشفير المعلومات ديز، تتم من الناحية العملية خلف السياج الثلاثي. ثم أصدرت الحكومة قراراً سرياً يكتّم براءة اختراع هورست فايشتل للوسيفر المعروف باسم نظام مفتاح متنوع لمصفوفة شيفرة Variant Key Matrix Cipher System. وفي 17 نيسان/ أبريل 1974 بعث محامي شركة آي بي إم المكلف ببراءات الاختراعات بمذكرة إلى الفريق القلم على بحوث الشيفرة في يوركتاون هايتس وكينجستون، أن فحوى القرار يحظر نشر للبحوث في هذا الموضوع ومناقشته علناً بأي شكل، إلاً بإذن خطي من مفوض براءات الاختراع. كان كل ما يحيط بالأمر سراً حتى وجود أمر السريّة ذاته يعتبر سراً، والحديث عنه جريمة خطيرة خطيرة تسليم خوارزميات الشيفرة لمسافر من مطار كينيدي. وإفشاء المعلومات عنه عرضاً دون قصد، كفيل بأن يغرم المرء 10000 دولار، أو عقوبة السجن عامين، أو كلا العقوبتين معاً، كما ورد في المذكرة. ولكن الأمر منح آي بي إم إذناً خاصاً بالكشف عن هذا الموضوع في نطاق ضيقاً شخصاً مشهود لهم بالولاء والأمانة والحفاظ على الأسرار، من الموظفين في الشركة من أو يعملون معها، وتقتضي مهماتهم المشاركة في تطوير أو صناعة أو استخدام المادة موضوعاً لتفاهم». ولولا هذا الاستثناء، ما كان بوسع آي بي إم الاستمرار في جهودها هذا، بسبب الصعوبة الجلية في التعاون في مشروع ينطوي على المجازفة، بالتعرض لعقوبة السجن جراء الاعتراف بوجوده لشخص يتعاون وإياها.

كانت متطلبات وكالة الأمن القومي سرّيةً متشدّدةً بالغة الصرامة بما يخص تحليل معيار تشفير البيانات ديز. ولذلك فإن أي أمر - مطلق أمر - يلقي الضوء على عمل محللي الشيفرة في فورت ميد، يعتبر من أعظم الكبائر، وكان الاتفاق المعقود بين الوكالة والشركة يرسم بوضوح حدود ما يمكن للعلماء في الشركة جمعه من المعلومات جرّاء هذا التعاون بينهما. فقد فرض على الشركة الاقتصار على عدد محدود من العلماء، ممن يعملون في تقويم المشروع ومراحلته، ووضع قوائم بأسماء هؤلاء الأشخاص دورياً. وكان الإحتكاك بين الأزرق الكبير Big Blue [شركة آي بي إم] والمتطّّل الكبير Big Snoop [وكالة الأمن القومي] يقتصر على سلسلة من الاجتماعات التي يطلّع فيها الطرفان على تطورات العمل، وفق قواعد دقيقة مضبوطة مثل مسرحية كابولي يابانية: تقدم الآي بي إم المعلومات، بينما يقوم جماعة الوكالة لتقييمها بصمت. ولم يكن مسموحاً خوض المجتمعين في الأحاديث المطولة؛ وكان محظوراً على جماعة الوكالة «الخوض في مناقشات تقنية مع ممثلي الشركة تتصل بالمعلومات المعروضة». وقد جرت القاعدة على أن يعقد جماعة الوكالة جلسات تشريح بعد تلك اللقاءات لمعرفة ما إذا كان العلماء في آي بي إم قد وقفوا على معلومات أو أفادوا من تقنيات «ذات طبيعة حسّاسة». فإذا كان الجواب بالإيجاب، اضطرت الشركة وبات عليها إبقاء تلك المعلومات طي السريّة.

كانت وكالة الأمن القومي تعرف بالتأكيد ما لديها، وقد أبدت عناية خاصة بأسلوب اكتشافه الباحثون في الشركة، يشار إليه في مختبرات واطسون باسم: «الهجوم تي»، ثم بات يُعرف لاحقاً باسم «تحليل الشيفرة التفاضلي». وهذه سلسلة معقّدة من المعالجات الرياضية التي تتطلّب الكثير من النصوص الواضحة المنتقاة (لا بد للمهاجم من أن تتوفّر له مجموعات من المراسلات الأصلية والنصوص المشفّرة بعد المعالجة، والقيام بمقارنتها ببعضها البعض). وكان الباحثون في مختبرات واطسون قد توصلوا في وقت ما من ذلك العام، إلى أن

في شيفرة آي بي إم ضعفاً يجعلها عرضة في ظروف معينة للسقوط أمام الهجوم تي - فيمكن للعدو إذا ما شنَّ هجوماً ناجحاً معرفة أجزاء من المفتاح . فكان أن قام فريق من الباحثين في آي بي إم بإعادة تصميم الصندوقين - إس ، للحيلولة دون إتاحة الفرصة لنجاح هذا الهجوم؛ ولم يعد بوسع المهاجم أن يستفيد من الهجوم تي بشيء يُذكر .

ولقد انتاب جماعة وكالة الأمن القومي ضيق شديد لسماع النبأ . إذ يبدو أن أمر الهجوم تي كان معروفاً - وسراً بالغ السريّة - وراء السياج الثلاثي . وللمرء أن يتخيّل ضيق الوكالة، عندما وجدت أن فريق الشركة لم يكتب باكتشاف الخدعة (التي كانت الوكالة تستخدمها في كشف شيفرات الأعداء) وحسب، بل ابتكر مجموعة من مبادئ التصميم لمواجهةتها أيضاً . ولم يحتمل جنود الشيفرة في فورت ميد احتمال تسرّب مثل هذه المعلومات إلى المكتبات العامة في هذا الحقل . وهكذا كان، أن شدّدت الوكالة قيود السريّة حيال الشركة .

ويذكر تكمان: «لقد طلبوا منا وضع خاتم السريّة على كل وثائقنا . فعمدنا إلى ترقيم كل وثيقة ثم وضعها في خزائن آمنة مغلقة، لأنّها في عرف حكومة الولايات المتّحدة سريّة . وصدر الأمر أن نقوم بذلك . فقمّت به» .

كان دان كوبر سميث هو الرجل الذي قام على الأرجح، بمعظم العمل المتعلّق بالهجوم تي في آي بي إم، وقد ظلّ يمتنع عن الخوض في أمره، طوال عشرين عاماً . ولم يكشف هذا الرجل مبادئ تصميم الصندوق - إس ، إلّا في عام 1994 ، وبعد ما كان باحثون آخرون قد اكتشفوا الأمر ووصفوا الأسلوب قبل ذلك بزمان طويل، وبشكل مستقل عن آي بي إم . وفي مقال تقني نشرته مجلة آي بي إم ريسيرش جورنال، كتب كوبر سميث: «لقد تقرّر بأن الكشف عن جوانب التصميم، كفيّل بأن يعرض للملأ أسلوب تحليل الشيفرة التفاضلي،

وهو أسلوب فعّال يمكن استخدامه في تحليل الكثير من الشيفرات. وهذا من شأنه إضعاف المزايا التي تتمتع بها الولايات المتحدة في التنافس، وتتفوق فيها على بلدان أخرى في مجال الكريبتوجرافيا».

ولقد تحقّق لآي بي إم في النهاية الوصول إلى مبتغاها، أي الحصول على شهادة براءة صحة لمعيار تشفير البيانات ديز، من وكالة الأمن القومي. (وكان هذا عاملاً هاماً ليضع المكتب القومي للمعايير خاتمة با لمصادقة على أن يكون معيار تشفير البيانات معياراً فيدرالياً). غير أن الشركة دفعت ثمناً غالباً لالتزامها بأمر وكالة الأمن القومي، والإبقاء على مبادئ تصميم الصندوق - إس سرّاً. فقد كان وضع لصناديق - إس في نظام معيار تشفير البيانات ينطوي على استبدلات وتغييرات أساسية معقّدة دونها أشد الأنظمة تعقيداً. وكانت أفضل طريقة يتطّيع الغرباء التوسل بها لتقدير ما إذا كانت هذه التحولات الغربية قد قصد بها إنتاج شيفرة أصعب من سابقتها، أو أنهطلعت سرّاً لتوضع في باب خلفي يتيح لوكالة الأمن القومي تحقيق ميزة على سواها في تفكيك الشيفرات، يكمن في معرفة سبب اختيار المصممين معادلاتهم. وكان رفض الشركة شرح المنطق الذي يقوم عليه تصميم الصندوق - إس قد شجّع نقاداً مثل ديفي وهيلمان، على الاثتر سال في شكوكهم والتفكير في مختلف النظريات التي تنطلق من فكرة الأبواب الخلفية السريّة.

وإن القول، بأن خوارزمية معروفة للقاصي والدانيته سُتت على مخطّطات سرية أدّى إلى شيوع حالة من الارتياب الشديد، وأصبح غذاء للنقاد استمر أعواماً. ولكن هذه الفكرة كانت بالنسبة للوكالة أمراً محسوماً، وغير قابل للنقاش. ولعل بنك العقول في فورت ميد رأى أنه قد يكون من قبيل الشر الذي لا بد منه، السماح بإطلاق خوارزمية شيفرة منيعة في عالم المصارف والشركات الضخمة. أما السماح بإذاعة التكنولوجيا المعقّدة التي قد تشجّع الغرباء على اختبار شيفراتهم الخاصّة... فأمر ما كانت الجماعة لتقبل به إطلاقاً.

كانت محصلة تلك الواقعة أنها اختزلت في ذاتها معضلة، على وكالة الأمن القومي، أن تعترف بوجودها، ولو لنفسها. فقد ظل الجماعة في فورت ميد طوال سنين عديدة واثقين من أن مثل هذه المعلومات لن تخرج إلى العلن، بعد ابتكارهم أسلوباً فذاً مثل تحليل الشيفرة التفاضلي. ولكن تلك الأيام ولّت. لتأخذ بعين الاعتبار أن مجموعة آي بي إم توصلت إلى حالة الهجوم تي منفردة، دون معونة من الحكومة. وتحليل الشيفرة التفاضلي هو في النهاية طريقة رياضية تنتظر الاكتشاف على يد كائن ما، خارج السياج الثلاثي، ولديه اهتمام بالشيفرة المعقدة. وغني عن القول، أنه ما كان بوسع وكالة الأمن القومي احتكار مثل تلك الحيل الرياضية أكثر مما يستطيع عالم فلك اكتشاف غمامة كونية لم يسبقه إليها عالم آخر، وكأنت تغطي السماء لتبينها راصد ذات يوم في المستقبل.

كانت هذه حقيقة العصر القادم: الشيفرة العلنية: وسواء رضيت وكالة الأمن القومي أم لم ترض، فإن أصحاب العقول الذكية لا بد وأن يكتشفوا من جديد الأفكار والأساليب التي كانت قيد الحجز في فورت ميد، ولعل هؤلاء سيأتون بعد، ببعض ما لم يكن ليخطر ببال حتى صفوة الكريبتوجرافيين وراء السياج الثلاثي.

إذا وضعنا لصناديق - إس جانباً، كان العنصر الأكثر مثاراً للجدل هو طول مفتاح معيار تشفير البيانات. كان لوسيفر الذي قدمه هورست فايشتل محددًا بمفتاح من 128 بت (خانة ثنائية)، لكن من الجلي أن وكالة الأمن القومي ما كانت لترغب لمعيار التشفير القومي - وإن اقتصر استعماله على المؤسسات المالية والشركات الضخمة - أن يبقى المعلومات مقفلاً عليها في مثل هذه الخزنة الجبارة. ولذلك، ففي الوقت الذي شقت فيه الخوارزمية طريقها عبر السياج الثلاثي، وطرحتم كعيار قومي محتمل، تم اختصار طول المفتاح إلى نصف، ثم زادوا في اختصاره حتى غداً هزيباً نسبياً لا يزيد عن 56 بت.

وليس من العسير على المرء أن يتبين أثر هذا الاختصار، فلنفترض أن أحد محللي الشيفرة عجز، وهو يحاول اختراق معيار تشفير البيانات، عن اكتشاف طرق مختصرة لتفكيكه. لذلك، فإن الطريقة الوحيدة أمام المتطفل لتفكيك رسالة مشفرة هي أن يشن هجوماً بالقوة الغاشمة، متوسلاً بكل تركيبة محتملة حتى يبلغ المفتاح الذي استخدم في عملية تشفير الرسالة الأصلية. وهذا البحث شبيه بحالة لص الخزائن الذي يجهد في تحريك قرص القفل حتى يعثر على مجموعة الأرقام التي تفتحه. وهو بحث يستحيل تنفيذه بالنسبة لمعيار التشفير، ولو استخدم المرء كومبيوتراً يستطيع إجراء الحسابات بسرعة عالية، وذلك بسبب «مدى المفتاح» الواسع جداً (المدى العددي الذي يحتوي كل تركيبات المفتاح الممكنة). والمفتاح الذي يتألف من 128 بت، هو مفتاح كبير جداً. وإذا حاول كومبيوتر التعامل مع مليون مفتاح كل ثانية - أي مليون مجموعة رقمية مختلفة على قرص الخزانة - لاستغرقت تجربة كل مفتاح محتمل، دهوراً.

ما هو تأثير اختصار المفتاح إلى النصف؟ لتقدير هذا الأثر عليك أن تذكر طبيعة الحسابات الرقمية. إن كل بت (خانة ثنائية) في المفتاح الثنائي شبيه بشوكة على الطريق، لا بد لمفكك الشيفرة من التعامل معها ليلبغ التركيبة الصحيحة من الوحدات والأصفار Ones and zéros. وكل شوكة تمثل اختياراً عشوائياً بين الدورة الصحيحة والدورة الخاطئة؛ والمفتاح الذي يتألف من 128 بت، يعني: أن عليك تقدير الطريقة الصحيحة لتحريك القفل 128 مرة في كل صف. ولمضاعفة صعوبة العملية، يكفي أن تضيف شوكة أخرى، وتكون بذلك قد ضاعفت عدد الطرق المحتملة للتعامل مع الشيفرة مرتين. مع أن إحداها فقط هي الطريقة الصحيحة ما زالت على حالها. وبالمقابل، فلاختصار الصعوبة إلى النصف، لا يتحتم أن تقسم عدد الشوكات إلى النصف، بل يكفي أن تزيل شوكة واحدة وحسب.

ولذلك، فإن استبعاد بت واحدة من حجم المفتاح يعني أن الرسالة

المشفرة مأمونة بنسبة النصف عكلاً نت عليه من قبل . ثم إن الانتقال من مفتاح يتألف من 128 بت إلى آخر يتألف من 127 بت، يعني اختصار عنصر العمل اللازم في حل الشيفرة إلى النصف . فإذا انتزعت منه بت أخرى، فأصبح حجم المفتاح 126 بت، تكون قد قسمته إلى النصف . وهكذا دواليك .

ووفقاً لتكمان، فقد رأت مجموعة كينجستون أن مفتاحاً من 128 بت لا يعتبر إسرافاً فحسب، بل سوف يتطلب مساحة أكبر للرقاقة وحسابات أكثر أيضاً . وفي ذلك يقول : «لقد تحتم علينا وضع الخوارزمية كلها هناك، والصناديق - إس، وكل شيء . و كنا نستخدم رقاقات سي إم أو إس CMOS [أنصاف نواقل تتمتعها ستهلاك منخفض للا استطاعة . هـ . م .] بقوة 2 ميكرون، وكا نت البيانات الواردة بعرض 8 بايت bytes [البايت يعادل 8 بت] . وهكذا كان طول المفتاح الأول 64 بت، هي مناسبة تماماً لرقاقة واحدة، وعدد يقبل القمة على بايتات مؤلفة من ثماني بتات .

كان هذا تقليصاً عظيماً، إذ اختزل الزمن اللازم للبحث الكامل على الكومبيوتر الذي يؤدي نظرياً عمله بواقع مليون مفتاح في الثانية، من بلايين السنين إلى حوالي 300 ألف عام . ومع ذلك، فما زال طول المفتاح المؤلف من 64 بت كبيراً، في منتصف السبعينات، خاصة وأنه كان من المتفق عليه أن تكنولوجيا الكومبيوتر ستظل دون التطور الذي يسمح بأعمال بحث بمثل هذا القدر، من السرعة على مدى العقدين التاليين .

لكن مجموعة كينجستون قامت، بعد ذلك، باختصار ثان، لم يكن في ظاهر الأمر مبرراً، بحيث أصبح طول المفتاح 56 بت، وهو من الناحية الرياضية غير مناسب، وفجأة دخل الصورة حتمال الهجوم بالقوة العاشمة . فما هي قيمة مجرد 8 بت حتى تحدث هذا التأثير؟ حبك هنا التذكّر أنه كلما تقلّص المفتاح بمقدار بت واحد، ازدادت سهولة تفكيكه بمقدار الضعف . وهكذا أدى اختزال الثماني بتات إلى جعل حل الشيفرة أسهل بمقدار 256 مرة، أي اختصار الزمن

من 300 ألف سنة إلى ما يزيد قليلاً عن ألف سنة. أو بعبارة أخرى أن نسبة الصعوبة قد تقلصت، وأصبح بالإمكان الآن استعراض مدى المفتاح في أقل من يوم واحد، بينما كان سابقاً قد يشغل كومبيوترات العدو ما بين كانون الثاني/يناير وآب/أغسطس.

فماذا كان تفسير آي بي إم لهذا الأمر؟ حسب قول تكمان أن الإجراء المتبع في الشركة في تصميم العتاد، كان ترك عدد معين من البتات الإضافية من أجل «تدقيق التكافؤ» Parity checks ضرب من التزامن للتأكد من صحة قراءة الإشارات الإلكترونية. ويقول تكمان: «إنه من المواصفات الداخلية التي تحددها آي بي إم»، وهو يعترف في الوقت ذاته، بأنه شرط «أحمق» ويتابع قائلاً: «إننا لم نعد نأخذ به، لكن في ذلك الوقت كان لدينا معياراً، وهكذا اضطررت لتقليص حجم المفتاح [للتسع للبتات الإضافية]».

لم يكن تكمان يعتقد أن في هذا التقليص الإضافي، ما يعرض معيار تشفير البيانات للخطر فعلاً. (كان هورست فايشتل يعارض في قرارة نفسه هذا الرأي، ويؤثر مفتاحاً من 128 بت. غير أنه لم يعد مشتركاً في هذا لمشروع، ثم سرعان ما ترك العمل في شركة آي بي إم ذاتها بعد حين). واعتقد تكمان وزميله كارل ماير بأن مفتاحاً يتألف من 56 بت بتنوعاته المختلفة، التي تبلغ 70 كدريليون، هو أكثر مما يلزم لحماية أسرار التجارية، والمالية التي سيقوم بها معيار تشفير البيانات. ويذهب تكمان إلى أن الفكرة التي يقوم عليها المعيار هي توفير مستوى من الأمن لشبكات الكومبيوتر مماثل ما يتمتع به الناس في مجال عملهم الفعلي: «أدرج المكاتب المغلقة، للغرف التي تحتوي على الكومبيوتر، والمستخدمون الأوفياء ذوو اللباقة والكياسة». لم يكن المقصود حماية الأسرار العسكرية، التي تنقل عادة في حقائب يدوية متفخخة مربوطة إلى أيدي أشخاص يحملونها ويحرصون عليها، أو يعهدون بها إلى جواسيس لديهم أوامر بابتلاع الحبوب السامة عند اعتقالهم.

وهناك آخرون، على كل حال، كانوا يعتقدون بأن هذا الاختصار مرده ضغوط ممارستها وكالة الأمن القومي. ومن هؤلاء المرتابون داخل أي بي إم ذاتها، مثل ألان كونهام، رئيس مجموعة الرياضيات في مشروع معيار تشفير البيانات. ويقول كونهام معرضاً بوضوح عن التفسير الذي قدمه تكمان: «ست وخمسون بت أمر شاذ. [فلا بد] أن الحكومة قالت إن أربع وستين بت كبير جداً - فليكن 56 بت». فما الذي جعل الآي بي إم توافق على هذا الطلب؟ إنك تدرك أن لها مصالح تجارية في جميع أرجاء العالم. ولا تستطيع تصدير قلم رصاص إلى خارج الولايات المتحدة دون إجازة تصدير. وليس هذا كل ما في الأمر، فعندما تلوح [وكالة الأمن القومي] بالوطنية والأمن القومي فإنك لا تملك المجادلة في هذه الأمور».

أما بالنسبة لغرباء أمثال: مارتين هيلمان وهويت ديفي، طبعاً، كان حجم المفتاح دليلاً على أن وكالة الأمن القومي قد أضعفت مستوى المعيار خدمة لأغراضها المشبوهة. ففي الشهور التي أعقبت إشهار المعيار، دأب الكريبتوجرافيين في جامعة ستانفورد على توجيه سيل من الاقتراحات والاعتراضات إلى الجهة المكلفة بالاتصال في المكتب القومي للمعايير، وأخذ شعورهم بالإحباط يزداد، حين وجدوا المسؤولين هناك، لا يقطعون عن القول بالبحاح على أنغليس في الموضوع ما يدعوا للارتياح. ثم وصل هيلمان إلى القناعة بأن المكتب القومي للمعايير، لم يكن يمثل رأي أعضائه، وإنما كان يؤدي دور العميل لفورت ميد.

وللبرهان على رأيه فيما يتصل بضعف حجم المفتاح، تحدى هيلمان مديراً تنفيذياً في شركة أي بي إم، كان يعرفه أن يدحض قناعته وديفي بأن مفتاح معيار التشفير هذا يمكن أن تغلب عليه آلة قوية متطورة في يوم واحد. وفي ذلك الوقت، كان الباحثون في جامعة ستانفورد قد ذهبوا في تقديراتهم إلى أنه يمكن إنتاج آلة كهذه بكلفة 20 مليون دولار. وإذا أمكن معرفة مفتاح واحد كل

يوم، على مدى خمس سنوات، فإن كلفة تفكيك كل مفتاح 10 آلاف دولار. وهذا استثمار لا بأس به إذا تضمنت بعض لرسائل المفككة بيانات هامة مثل مواقع مخزونات النفط لاستراتيجي، وخطط الدمج بين الشركات الضخمة - فمعلومات كهذه تعادل ملايين الدولارات. ويقول هيلمان: «وحتى لو بلغت الكلفة 100 ألف دولار فلن يضيرنا ذلك، لأن سرعة الكمبيوتر سوف تتضاعف عشر مرات خلال السنوات الخمس لتالية، ولن يكلف الحل سوى عشر كلفته الحالية». ويروي هيلمان أن المدير المذكور في الآي بي إم وجّه أمراً للباحثين لاستقصاء الموضوع، ويقول أن هذا المدير: «اتصل بي بعد حين وقال إن الأرقام التي توصل إليها الباحثون لديه، تجري في الملعب ذاته مثلنا، كانت عبارة «في الملعب ذاته» هي العبارة ذاتها التي استخدمها [هذا المدير]. لكنه أفادني بأن حجم المفتاح حدده المكتب القومي للمعايير، وليس الآي بي إم».

وفي الوقت ذاته، كان المسؤولون في المكتب القومي للمعايير يؤكدون في ردودهم على رسائل هيلمان المتكررة والتي كانت تزداد حدة باطراد، أن دراساتهم تبين أن آلة كالتي يتصورها سوف تمتغرق إحدى وتسعين عاماً لتستقصي مدى مفتاح معيار تشفير البيانات. وكان واضحاً أن هؤلاء القوم لا يلعبون في نفس الملعب الذي يلعب فيه هيلمان.

كان هيلمان يعتقد أن ذلك كله يعتبر دليلاً ساطعاً، على أن معيار التشفير كان منذ البداية خداعاً؛ فهو في الواقع، المخطط الأصلي، الذي وضعته وكالة الأمن القومي. إن المكتب القومي للمعايير الذي يفترض فيه أنه غير خطر - هو الوجه العلني لوكالة الأمن القومي ترك للآي بي إم تصميم لخوارزميات على نحو مستقل. وقد أتاح هذا الأمر [للمكتب القومي للمعايير ووكالة الأمن القومي] إنكار كل علاقة لهما بالموضوع، فكان بالإمكان عندئذ التملص من أي التزام أو ارتباط به، فإذا سئلوا، أجابوا: سمعوا يا جماعة، لسنا نحن الأشباح من طبخ ذلك، وإنما صاحبة العلامة الزرقاء العتيقة (آي بي إم). لكن الأشباح،

إلى حملوا الشركة على اختزال حجم المفتاح إلى مجرد 56 بت، وبات هزياً إلى حد يثير الحنق، تحقق لهم ما أرادوا ونالوا مبتغاهم. وفي هذا، يقول هيلمان شاكيًا: «لقد كانوا يدركون أن السيطرة على حجم المفتاح من شأنهم، وبذلك، يستطيعون في نهاية المطاف السيطرة على قوة المعيار.»

كان هذا التفسير هولاً لطف فيما قيل. أما إذا شئت أن تنحو إلى الشك والريبة - وكان هيلمان وزملاؤه ينحون إلى الريبة بشدة، شأنهم في ذلك شأن أي مصمم شيفرة متمكن من موضوعه - فأنتك سوف تظل تتساءل مع ذلك إن كان في الأمر باب سرّي يتيح للمخادعين في فورت ميد تفكيك رسالة مشفرة ترسل عبر معيار تشفير البيانات خلال ثوان. وإلا، فما الذي يحملهم على إحاطة مبادئ التصميم بالسرية؟

وفي مطلق الأحوال، رفض هيلمان لأخذ بتقدير الحكومة بشأن الإحدى وتسعين سنة، وقرّر تجاوز الموظفين في المكتب القومي للمعايير الذين كان يجري وإياهم مراسلاته. وفي 23 شباط/ فبراير 1976 بعث برسالة إلى إبيوت ريتشاردسون الذي كان بوصفه وزيراً لتجارة، الرئيس الأعلى للمكتب القومي للمعايير وعرض له شكواه:

«إنني أكتب إليكم، والقلق لشديد يساورني، من أن تكون وكالة الأمن القومي قد أثرت بطريقة خفية على المكتب القومي للمعايير بما يحد، بشكل خطير، من قيمة المعيار المقترح، ومما قد يشكّل خطراً على خصوصية الفرد. إنني أعني بهذا القول معيار التشفير المقترح والذي قصد به أن يوفر الحماية للبيانات السرية أو الخاصة التي تستخدمها الهيئات الفيدرالية غير العسكرية. ولا ريب في أن هذا سيغدو معياراً مفروضاً بحكم الواقع في عالم التجارة أيضاً.»

... إنني لعلّي ثقة من أن وكالة الأمن القومي وهي تؤدي دورها بمساعدة المكتب القومي للمعايير في التصميم والتقييم للمعايير الممكنة، قد ضمنت لنفسها القدرة على تفكيك شيفرة المعيار المقترح.»

ولم يخفف الرد الذي تلقاه هيلمان من أرست أمبلر، القائم بأعمال مدير المكتب القومي للمعايير، الكثير من الثورة التي كانت تجيش في نفسه. فبدلاً من الرد المباشر على الاتهامات التي وجهها هيلمان، قدم أمبلر بعض التعليقات العامة، دافع بها عن معيار التشفير، مطرياً وكالة الأمن القومي لمساهماتها في ضبط الخوارزمية. ثم أرفق رسالته بأمر إداري يحدّد «وظائف ومسؤوليات وكالة الأمن القومي». وجاء هذا الأمر خلواً من الإشارة إلى العبث بخوارزميات القطاع الخاص.

في ذلك الصيف، انكبّ هيلمان وديفي، وخمسة أكاديميين آخرين على معالجة ذلك النّظام، وقدموا بحثاً بعنوان «نتائج محاولة أولية لتحليل شيفرة معيار تشفير البيانات التابع للمكتب القومي للمعايير». وكان هؤلاء الباحثون صريحين وواضحين في تبيان أسباب القلق الذي ينتابهم: إن كل خوارزمية حظيت بموافقة وكالة الأمن القومي، كانت «عرضة للشك مسبقاً» لأن «الوكالة لا تريد نظاماً منيعاً فعلاً يفسد عليها عمليات تحليل الشيفرة الاستخباراتية التي تنهض بها». ولذلك لم يكن مفاجئاً، أنهم وإن كانوا مقصرين جداً عن تفكيك مفتاح معيار تشفير البيانات، فقد توصلوا إلى أنه لا يمكن الوثوق بهذا النظام. واكتشفوا، إلى جانب قوة المفتاح، ما اعتبروه «بنية مريبة» في الصناديق - إس، وربما كان هذا، كما ذكروا، «نتيجة... باب مفخّخ وضع عمداً.

أما رجل الآي بي إم والت تكمان، فقد رأى في شكاوى ديفي وهيلمان مهزلة، منشوها جنون العظمة والجهل معاً. فالرجل ليس عميلاً سرياً - بل كان معنياً بإنتاج سلعة - وقد قاد فريقاً بكل ما أوتي من القوة والكفاءة لإنتاج سلعة جيدة! وكان يوماً سعيداً حين أنجز فريقه أول جهازين من معيار تشفير البيانات. وكان هذان صندوقين من المعدن بحجم صندوق صباغ الأحذية، وكل منهما محشو بالرقاقات، ويقع بين الكومبيوتر الرئيس والموديم. وإن وجود مثل هذا الجهاز عند كل طرف ينقل البيانات، يسمح لجهازي كومبيوتر بالتخاطب عبر

مجرى سري منيع على المنتصين، مهما يكن قول مارتي هيلمان. وقد أرسل أحد هذين الصندوقين إلى مقر شركة الآي بي إم في باريس، والثاني وُضع في مكتب ليو برانسكومب في إرمونك، وكان لهذين الصندوقين، بعد هذا، شأن في التاريخ. قام مكتب باريس بإرسال رسالة مشفرة إلى الآلة في إرمونك، التي قامت بعد ما تمت تغذيتها بالمفتاح المتماثل الذي يؤدي وظيفتي التشفير وتفكيك الشيفرة معاً بتفكيك شيفرة الرسالة وإعادتها إلى صيغتها الأصلية. ويذكر تكمان أن الرسالة أرسلت بعد استقبالها، إلى طابعة صغيرة ونشرت في كافة الصحف التي تصدرها الآي بي إم. وكانت رسالة ليس فيها ما يضير، طبعاً، لأنه كان معروفاً للجميع أنها سوف تنشر على الملأ».

لكن هذه السعادة لم تكتمل، إذ نالت منها الهجمات التي شنها هيلمان وأصدقاؤه. واضطر تكمان وزميله كارل ماير إلى الدفاع عن نفسيهما في ورشتي عمل عليتين، كان المكتب القومي للمعايير قد قام برعايتهما. وكانت ورشة العمل الثانية، التي عقدت في أيلول/ سبتمبر 1976، في مقر المكتب في جيتسبورج، في ولاية ماريلاند، الأحفل بالمنازعات والمشاكسات. وقد تمسك تكمان بموقفه وآرائه، قائلاً: «إني لم آت بخطأ!» وحجم المفتاح مناسب، وصنع آلة لتفكيكه لن يكلف هذا المبلغ المتدني المؤلف من سبع خانات الذي وصفه هيلمان بل 200 مليون دولار.

وإذا كان حجم المفتاح دون الطول المطلوب، فبوسع من يرغب، تصميم أجهزة لتشغيل معيار تشفير البيانات بضعف سرعته، بوساطة مفتاحين مختلفين. ولئن كانت هذه العملية صعبة التنفيذ، إلا أنها سوف تؤدي إلى زيادة حجم المفتاح حتى يبلغ 112 بت، وفي هذا ما يكفي لإرباك كل كومبيوتر لعين على سطح الكرة الأرضية طوال القرون القادمة. (ثم ظهرت بعد حين عملية عُرفت باسم «معيار تشفير البيانات الثلاثي» التي يستخدم فيها ثلاثة مفاتيح، وتتغلب على أشد الهجمات تعقيداً وقوة. بيد أن هذا كله كان أمراً غير ذي شأن

من الناحية العملية، لأن نسخة المعيار التي حُدِّت بـ 56 بت، هي النسخة التي اقترحت للمعيار).

ولقد فشلت مناشدة تكمان في تهدئة النقّاد. وكان هؤلاء يسألونه لماذا لا تنشر عناصر التصميم؟ هل وضعت في المعيار باباً مفتحاً؟

ثم جاءت مشكلة الصحف. وقد تدمّر تكمان من أن «هؤلاء الأساتذة الجامعيين طرحوا الموضوع على صحفيي النيويورك تايمز والواشنطن بوست. وبعد ذلك قام تكمان ذاته بإجراء مقابلة صحفية، بطلب من شركة الآي بي إم، حول هذا الموضوع. وبعد جولة قصيرة في صحيفة الواشنطن بوست وإلقاء نظرة على مكتبي الصحفيين: وودوارد وبيرنستين، اللذين أصبحا مؤخرًا من المشاهير، كرر تكمان ما سبق أن قاله لمراسل صحيفة التايمز: «أن وكالة الأمن القومي لم تجر أي تعديل على الخوارزمية، ولا أقامت باباً سرياً. انتبهوا يا شباب، إن هذا ضرب من السخف؟ إننا لن نجازف بشركة الآي بي إم كلها، بوضع باب سرّي في آلة من صنعها».

ومع ذلك، فقد أخذت الدعاية مداها. وكان الوضع سيئاً في ذاته، بعدما أخذت صحف التايمز والواشنطن بوست والوولستريت جورنال تنشر تصريحات تكمان والنقاد. بل الأسوأ من ذلك، أن والدته تكمان اتصلت به من معتكفها في فلوريدا بعدتها عدداً مبدية قلقها مما سمعت من الأصدقاء، بعد اطلاعهم على الصحف الصادرة في نيويورك، راجية ولدها الذي بدأ حياته على أروع ما يكون لطالب جامعي نبيه من بروكلين: «أرجوك، يا ولتر، أن تستقيل من الآي بي إم وتترك صحبة السوء هؤلاء». وأجابها تكمان مطمئناً بأنه لن يدخل السجن ليجاور إيرليخان، وهالدرمان [عضوان بارزان في حلقة الرئيس السابق ريتشارد نيكسون، وقد حكم عليهما بالسجن لتورطهما في قضية ووترجيت] فهو رجل مستقيم.

بعد الدعاية جاءت جلسات الشهادة أمام لجنة الاستخبارات في مجلس الشيوخ. وكانت هذه الجلسات سرّية مغلقة، وتجري خلف الأبواب الموصدة، والتقرير النهائي لتلك الجلسات كان سرّياً أيضاً؛ ولكن صدر ملخص عنه، ليطلع عليه الجمهور العريض. فقدمت محتوياته ذخيرة لكلا الجانبين.

فمن جهة، تبين أن هيلمان كان على حق في إصراره على ما هي السلطة، التي فرضت المفتاح بطول 56 بت: «أقنعت وكالة الأمن القومي شركة آي بي إم بأن مفتاحاً مختزلاً من 56 بت واف بالعرض». حسب ما ورد في التقرير. ولم يكن السبب في هذا الاختزال، كما ادعى تكمان، صرامة تصميم الرقاقة أو الحاجة لندقيق التكافؤ، بل ضيق الحكومة بما يزيد عن هذا المفتاح. وكانت الشركة تدرك أن تصدير الجهاز مشروط بترخيص من الحكومة بعد الموافقة على المستورد. ولكن وكالة الأمن القومي، للمكلفة بالتعاون مع المكتب القومي للمعايير في تقييم معيار تشفير البيانات، باعتباره معياراً حكومياً، ما كان متوقفاً منها قطعاً أن تمهر بخاتمها خوارزمية تستخدم، في رأي الوكالة، مفتاحاً أطول مما ينبغي. وهنا يبدو أن المفتاح ذو الـ 56 بت، قد وفّر لوكالة الأمن القومي قدرًا من الارتياح. ولئن كان العمل المطلوب لتفكيك شيفرة بهذا القدر من الطول، كبيراً إلى حد الإجهاد، فمن الواضح أنه إذا كان ثمة من يريد القيام بهجوم بالقوة الغاشمة لتفكيك شيفرة المعيار (ديز)، فهذه الجهة هي وكالة الأمن القومي ذاتها، بما لديها من أجهزة كومبيوتر ضخمة ذات قدرات هائلة، في الطابق الأرضي من مبنى القيادة ومحاطة بأقصى قدر من السريّة. وغني عن القول أن الشيفرة المثالية لنسبة لمستخدمي الجهاز هي أقوى الشيفرات الممكنة، بينما الشيفرة المثالية لوكالة الأمن القومي، من الناحية العملية، هي الشيفرة التي تكون من القوة بما يحول دون اختراق المجرمين والخصوم الآخرين لها، ومن الضعف بما يسمح للمليارات من دورات الكومبيوتر الخفية التي تعمل في فورت ميد من تفكيكها. فهل كان المفتاح

بطول 56 بت، هو المفتاح الملائم الذي يليها هذه الشروط؟ هذا ما لم تجب عليه الوكالة. بل ولن تجيب.

ولقد خلصت اللجنة، بالرغم من الاستنتاج الذي وصلت إليه من أن حجم المفتاح تحدد بطلب من الوكالة، إلى أنه ليس في الأمر خلل في العمل، سواء من جانب شركة الآي بي إم أو من جانب الحكومة. وقد كان قرار اللجنة أن حجم مفتاح معيار تشفير البيانات قد تقرّر بشكل معقول. وكان على مارتي هيلمان وأصحابه القبول به، أعجبهم ذلك، أم لم يعجبهم.

استغرق الأمر بضع سنوات، لكن الجماعة لم يلموا به في نهاية المطاف وحسب، بل كان عليهم كذلك مواجهة بعض الحرج. فكما لاحظت والت تكمان بزهو لم يكن هناك طوال عقدين من الزمن بعد قبول الخوارزمية رسمياً معيارين في عام 1977 من استطاع أن يجد وسيلة مختصرة لتفكيك رسالة مشفرة بمعيار تشفير البيانات. (طبعاً إذا كانت وكالة الأمن القومي قد تمكّنت من ذلك، فإنها لن تصرّح بذلك على الإطلاق).

في عام 1990 كشف محلّلو الشيفرات خارج هذا النطاق عن أسلوب تحليل الشيفرة التفاضلي، وأثبتوا أن بوسع المرء، في ظروف معينة (وهي كما يسلّمون، نادرة) معرفة مفتاح معيار التشفير، بقدر أمل من الحساب مما يقتضيه الهجوم بالقوة الغاشمة. لكن هذا كان بالضرورة «الهجوم آتي» الذي اكتشفته الشركة أثناء عملية التطوير التي قامت بها لتقوية الخوارزمية وتدعيمها مقابل هذا الهجوم. وقد ظلّت الآي بي إم تبقي الأمر سراً امتثالاً لطلب وكالة الأمن القومي. (وهناك جماعة من الباحثين، خرجوا لهجوم نظري آخر على المعيار، هو تحليل الشيفرة الخطي، سنة 1993 - لكن لا هذه الجماعة ولا تلك، تمكّنت من طرح تهديد للشيفرة).

وهكذا إذا كان حجم المفتاح هو نقطة الهجوم الوحيدة على معيار تشفير البيانات. وإذا كان لا بد للمرء من تكريس طاقات حسابية ضخمة لتفكيك رسالة واحدة، ثم عليه أن ينتظر أياماً وأسابيع وشهوراً حتى تنهار الشيفرة، فإن وكالة

الأمن القومي تكون قد أجازت أداة خارقة القوة لنشر أسلوب تشفير منيع في كافة أرجاء البلاد، وربما العالم أيضاً. ولطالما حمل القوم وراء السياج الثلاثي الانطباع بأن مستخدمي معيار التشفير سيكونون من المؤسسات المحافظة الموثوقة مثل المصارف والبيوتات المالية. لكنهم أخطأوا التقدير. فبدلاً من ذلك، جاء تطوير معيار التشفير، إيداناً ببداية عهد جديد لوسائل رخيصة الكلفة وفعالة في استخدام الكمبيوتر للحفاظ على خصوصية المعلومات الشخصية. فلم يقتصر استخدامه على المصارف وحسب، وإنما امتد ليشمل كافة الاتصالات التجارية، بل بات شائع الاستخدام في الاتصالات الخاصة أيضاً. ومع احتفاظ وكالة الأمن القومي بالسيطرة على تصديره، فإنه سرعان ما انتشر في حدود الولايات المتحدة دون عائق أو قيد. ولئن ظل المصنعون يخضعون لقيود التصدير ولا يستطيعون تسريقه وراء البحار، فالخوارزمية ذاتها، وجدت طريقها لتتسرب إلى الخارج، مما أتاح للمطورين الأجانب أن يخرجوا بنسخهم الخاصة عنها.

ولربما سر البعض في فرع أمن الاتصالات المسؤول في وكالة الأمن القومي عن حماية البيانات الأمريكية وهي تدور في أنحاء الكرة الأرضية، لحلول هذا العهد الجديد من الحماية. لكن هذا الأمر قد أثار نومة دعر بين العاملين في مجال استخبارات الإشارة، أي الذين كانت مهمتهم أن يكفلوا لجماعتنا سرعة اعتراض وتداول المعلومات الدسمة التي تجري حول الكرة الأرضية بصورة نبضات إلكترونية. فإذا جرى تشفير هذه النبضات، وغدت لا تقبل القراءة بسهولة، فسوف تقوم عندئذ مشكلة. ومما زاد في الأمر سوءاً، ظهور تقنيات كومبيوتر زهيدة الثمن، أتاحت - بل فرضت القاعدة - تغيير مستخدمي معيار التشفير للمفاتيح، ليس كل بضعة شهور، كما افترضت وكالة الأمن القومي، وإنما بصورة يومية أو أكثر من مرة كل يوم.

أجل، لقد كان معيار تشفير البيانات مشكلة تشغل الفورت ميد. وبعد

سنوات، بات حتى مارتين هيلمان، يدرك أن هجومه على المعيار كان يقوم على عتريات أكثر مما يستند إلى أساس صلب، وعلى حد قوله: «كانوا [وكالة الأمن القومي] يثقلون لعملاق، وأنا العقل الجبار. كنت أناطح الوكالة وهذا أمر من شأنه أن يدير رأس من كان شاباً في مقتبل العمر». أما الآن، فهو يعترف بأن للقضية وجهين: هما أن معيار تشفير البيانات كان بالرغم من حجم مفتاحه قوياً بما يكفي لتوفير قدر من الأمن للناس، ثم إن العملية ذاتها أشد تعقيداً وتكلفة، من مجرد قراءة نص معترض غير مشفر، وإن كان لوكالة الأمن القومي القدرة على تعبئة المصادر المالية والتقنية والعلمية والبشرية، على ما يفترض لتليين مفتاح معيار التشفير وإخضاعه بالهجوم بالقوة الغاشمة. وكان معيار التشفير أول درس تلقته وكالة الأمن القومي بأن عصرأ جديداً من أمن الكمبيوتر قد أطل، والمؤكد أنه سوف يعقد لها الحياة إلى حد كبير، ولربما إلى حد ضعفة المؤسسة برمتها.

ويذهب آلان كونهائم إلى الاعتقاد بأن القول الفصل في أمر معيار التشفير جاء من هوارد روزنبلوم، نائب الرئيس للبحوث والتطوير في وكالة الأمن القومي، حيث تفكك الكمبيوتر الضخمة شيفرات أصدقاء البلاد والأعداء، وتمحن الشيفرات التي قصد بها حماية أسرارنا الخاصة. ففي أحد الأيام، وبينما كان روزنبلوم وكونهائم يتحدثان عن معيار التشفير، أبدى المسؤول الكبير في الوكالة ملاحظة زلّ بها لسانه، لكن كونهائم بقي يتذكرها لسنوات طويلة، إذ قال: «لقد قمتم بعمل جيد أكثر مما ينبغي».

ويعلق كونهائم اليوم بسرور غامر: «ولم يكن المقصود بتلك العبارة حول الإطراء».