المفتاح العام

لئن كان هويت ديفي ومارتي هيلمان اعتبرا معيار تشفير البيانات عملية مشبوهة، وربما ضرباً من الاحتيال من جانب شركة آي بي إم وحكومة الولايات المتّحدة، فإن تقديمه كان بطريقة غريبة هدية هامة للباحثين في جامعة ستانفورد. ذلك أن ديفي وهيلمان بعد أن قاما بالبحث المستفيض في البيانات الفنية المتوفرة، المتعلقة بالمعيار المقترح ـ والنظر في ما أهمل طرحه علناً ـ باتا يمتلكان موشوراً جديداً يمكنهما من تقدير جهودهما في هذا المجال. فمنذ أن سمع ديفي أولى التقارير عن المعيار الحكومي ذات يوم من عام 1974، أثناء تناوله لطعام في لوي، المطعم الصيني الذي يرتادهباقرة ستا نفورد، أخذ يتساءل في سره عن احتمال قيام وكالة الأَمن القومي بوضع باب سري فيه. وقاده هذا التساؤل إِلىٰ سؤال أعمق، يتصل بمفهوم الأبواب السرية. فهل يمكن تصميم شيفرة بكاملها حول باب سري؟

إن تصميم مثل هذا النِّظام ينطوي على تحديات ضخمة، لأنه يفرض حل تناقض أساسي. فالباب السري يوفر لمن يمتلك المعرفة المناسبة، الوسيلة التي يتجاوز بها الإجراءات الأمنية ليصل سريعاً إِلىٰ الرسائل المشفرة، وهو أمر يبدو فعالاً. ولكن مجرد فكرة ستخدام الباب السري في نظام أمني تبدو مجازفة

جنونية، وذلك لأن ثمة احتمالاً بأن يتمكن المتطفلون الأذكياء من إيجاد طريقة لاستغلاله. وهذه عين المشكلة التي ينطوي عليها الباب السحري في المباني: فإذا عجز الأعداء عن العثور عليه، كان بوسعك استخدامه للاختبار؛ أما إن استطاعوا معرفته فإنّهم يتمكنون عندئذ من بلوغ المكان الذي تختبئ فيه.

وهذه المفارقة جعلت إمكانية تصميم مخطط لباب سري أمراً مثبطاً للعزائم. ذلك أن أقوى منظومات التشفير قد صُمِّمت من كافة نواحيها، للحيلولة دون تسرّب محتوياتها. وإذن فالعبث في أجزائها الداخلية لتركيب باب خلفي ـ تسرب! ـ يمكن أن يؤدي بسهولة إلى إحداث عدة نقاط ضعف دونما قصد. وعندما عرض ديفي هذا الأمر على هيلمان، تو صل الرجلان كلاهما إلى أن منظومة كهذه ستكون على الأرجح أمراً غير عملي. غير أن ديفي ظل يعتقد أن هذه المنظومة جديرة بالملاحظة، فأضافها إلى قائمة كان يقوم آنذاك بإعدادها بعنوان «معضلات نظرية كريبتوجرافية طموحة».

ومع ذلك، ما زالت الأمور كما هي في بدايات عام 1975، والأسابيع تمضي بلا طائل، بالرغم من جهود ديفي السيزيفية [نسبة إلى أسطورة سيزيف الإغريقية] والتعاون المثمر الذي كان قائماً بينه و بين هيلمان. فهل كان مآل هذا الجهد الذي يقوم به للإحاطة بالكريبتوجرافيا أن يضيع ويذهب هباء؟ لقد كان لهيلمان وظيفة، على الأقل، تشغله. أما ديفي فكان بدون عمل. ومع أن الفترة التي أمضاها في العناية ببيت جون مكارثي كانت على قدر من الإمتاع، إلاّ أنه تجاوز اليوم الثلاثين من عمره ولا دخل لديه، ولا تأتيه أبحاثه إلاّ ببعض الدريهمات، وكان واضحاً أنّه لن يستطيع التغلّب على العقبات التي لا بد له من تجاوزها قبل أن يفوز بشهادة الدكتوراه. ومع أن ديفي كان مبتهجاً بطبيعته، إلاّ أن هذه الأمور التي كان يفكر ويعيد التفكير فيها باستمرار كانت مثبطة للعزائم.

وتسترجع ماري فيشر، مناسبة بلغت فيها معنوياته أدنى درجاتها، حين

دخلت غرفة نوم آل مكارثي ذات يوم، فوجدت ديڤي واضعاً رأسه بين يديه وهو يجهش بالبكاء. وتقول: «سألته عن سبب بكائه، فأجابني أنّه لن يكون له شأن في الحياة قط، وعليَّ أن أبحث عن شخص آخر [أرتبط به]، وأنّه ـ وأنا أذكر عباراته بالضبط ـ باحث عجوز منهار [بلا مستقبل].

ولقد حاولت التخفيف عنه والتهدئة من روعه. وقالت له يومذاك أنه رجل عظيم، إلاّ أن العالم لم يدرك، بعد، هذه الحقيقة. وكانت ماري تدرس المصريات، فأخذت تشرح له أن المصريين القدماء، كانوا يميِّزون بين الخصائص الشخصية الأصلية والخصائص المكتسبة. وكانت تعتقد أن «العظمة» من الخصائص التي لا تكتسب، فهي من قوام الشخصية الأصلية، وحسب المرء أن ينظر فيراها متجلية في صاحبها. وقالت له عندئذ: «إنني أعلم ما أنا ناظرة إليه، وأعلم أنّك رجل عظيم».

ولم يكن ديڤي يشعر بأنّه رجل عظيم، بل كان يشعر بأنّه رجل فاشل.

وفي أحد الأيام أحضر ديڤي وهيلمان معهما عالماً يعمل في حقل الكومبيوتر في جامعة بيركلي، يدعى بيتر بلاتمان، ليشهد إحدى الحلقات الدراسيَّة غير الرسمية في موضوع الشّيفرة، والتي كانا قد دأبا على إقامتها في حرم الجامعة. وبعد انتهاء تلك الحلقة، أوصل ديڤي بلاتمان بسيارته إلى مختبر الذكاء الاصطناعي في جامعة ستانفورد، وفي الطريق، أتى بلاتمان على ذكر صديق له يدعى رالف ميركل، وكان هذا منكباً على دراسة معضلة طريفة: كيف تستطيع أن تجري مكالمة مأمونة عبر خط غير مأمون، دون أن يكون بين الشخصين اللذين يتبادلان الحديث معرفة مسبقة؟ وغني عن القول أنّه طالما كانا على غير معرفة سابقة ببعضهما، فلن يكون هناك ما يسمح لهما بتبادل المفاتيح السرِّيَّة قبل أن يجري بينهما حديث خاص.

كانت هذه، بالنتيجة، صيغة مختلفة للسؤال الضخم الذي ظل يؤرق ديڤي طوال سنوات، أي: هل من الممكن استخدام الكريبتوجرافيا لحماية شبكة

مترامية الأطراف من عدوان المتنصتين والراصدين الذين يعنيهم تسجيل ما يسري عبر الخطوط؟ (أو بعبارة أدق، كانت هذه الصيغة تعكس ملاحظة ماري حول المعضلة التي تشغل فكر ديفي: في عالم مليء بالناس غير الجديرين بالثقة، كيف يمكن للمرء أن يستمر في إقامة اتصال حميمي بشخص يثق به؟). ولما كان ديفي لم يحقّق نجاحاً يُذكر في التصدي للمشكلة، فقد قال لبلاتمان أن خطة صديقه مستحيلة التحقيق. ويعتقد ديفي أن لهجته العصبية قد حملت بلاتمان على الاقتناع برأيه. إلاّ أن ديفي، وإن كان يجادل عاطفياً باستحالة تحقيق مثل هذه الخطوة الضخمة، فقد كان يعتقد في سرّه بعكس هذا الرأي، وراح عقله يجري بسرعة لاستيعاب ذلك الذي عرضه صاحبه؛ وكأنما كان يشعر في أعماقه بضرورة وجود مثل هذا الحل.

كيف يمكنك أن تبتكر نظاماً يتيح لأناس لم يسبق لهم الالتقاء ببعضهم البعض أن يتحدَّثوا بحرية واطمئنان؟ وأين يمكن إجراء الأحاديث كلها بكفاءة التكنولوجيا المتقدمة على أن تكون محاطة بحماية الكريبتوجرافيا؟ وكيف لك أن تحصل على رسالة مبثوثة إلكترونياً من شخص ما، وتكون على ثقة من أنَّها وردت من المرسل الذي تحمل الرسالة عنوانه؟

لقد جاهد ديفي أثناء بحثه لجمع المعلومات اللازمة في مناخ يكاد يكون كله سرياً. لكنه توصل إلى حصيلة تفوق توقعات أي شخص: الدوال (التوابع) الوحيدة الاتجاه. الحماية باستخدام كلمة السر. التحقق من الصديق أو العدو. الأبواب السرية. كان عقل ديفي يوحي له بأن الحل للمشكلة السرِّيَّة، والخصوصية لا بد كامن في مكان ما بين هذه الحصيلة كلها. وكان يعلم أن التوفيق بين الحمايات المختلفة التي توفرها هذه الأنظمة أمر لا محيص عنه لبحثه. وفيما أخذ يقدح زناد الفكر، ويزداد انشغالاً بموضوعه، بدأ يدرك السبيل للإفادة من هذه التقنيات، في التحقق من هوية الطرف الآخر. فأخذ يصنطع في ذهنه وسيلة يمكنه بواسطتها تنفيذ مشروعه عبر التوابع الوحيدة

الاتجاه تلك الظاهرة الرياضية حيث لا يمكن عكس أمر بذات القدر من السهولة الذي جرى حسابه به. وإن خطة كهذه ستكون، كما كتب فيما بعد؛ «تحدياً لا يمكن أن يأتي الرد عليه إلاَّ من شخص واحد، إنما سيكون في نظر الكثيرين حلاً حقيقياً». إنه بعبارة أخرى، نظام من «التحقق من جانب واحد» يقوم على سوء الفهم لمخا لف الذي خرج به صديق بيل مان قبل عدة سنوات: باب سري يعتمد على الدالة (التابع) الوحيدة الاتجاه، حيث يمكن إجراء عكس العملية الحسابية التي يصعب إجراؤها، إن توفر للمرء بعض المعلومات عن أسلوب تنفيذا لحساب الأصلي.

ولقد أدَّى هذا إلىٰ طرح موضوعا لمفتاح الذي سبق أن تناوله ديفي في أحاديثه مع مكارثي حول التجارة الإلكترونية. ولكنذ لك إنما كان نصف المعضلة. فما هو نصيب لخصوصية والسرِّيَّة من هذا؟ وهل يمكن أن تنجح فكرة الباب السري ذي الدالة (التابع) الوحيدة الاتجاه في نظام يحمل معضلتين: أولاً التحقق اللازم من كلمات لسر المستخدمة في الكومبيوتر وسواها من أدوات التحقق والتثبيت، وثانياً سرية الاتِّصالات؟

فيذ لك الربيع كان ديفي قد استقر على نظام في الحياة اتبعه أثناء إقامته في بيت مكارثي. فكان يقوم بتحضير وجبة الفطور كل صباح لماري وسارة، ابنة مكارثي ذات الأربعة عشر عاماً. وإذا انتهىٰ لفطور، مضت ماري إلىٰ عملها، بينما تذهب سارة إلىٰ المدرسة، فيما يبقى ديفي في البيت. وفي صباح أحد الأيام من أيار/ ما يو 1975، أمضى ساعات الصباح في التفكير وحيداً في البيت، بعد ذهاب زوجهو سارة. ثم عاد إلىٰ ما يشغل ذهنه بعد استراحة الغداء. وكان يفكر للمرة لأ لف بمشكلة وضع كلمة سرمأ مونة في شبكة الكومبيوتر. وواجهته من جديد مشكلة توفر الإداري الموثوق الذي يحمل كلمة السر. فكيف تستطيع استبعاد ذلك الطرف الثالث من المشروع كلياً؟ وفي وقت ما بعد الظهر، وجد الأمور تنجلي له فجأة: ابتكار نظام لا يوفر كل ما كان

يتصوره ديفي مؤخراً من خطة للتحقق من طرف واحد وحسب، وإنما يستطيع أن يحقّق التشفير وتفكيك الشيفرة بطريقة مبتكرة أيضاً. وهذه سوف تحقق له حل مشكلة الإداري غير الموثوق، والأكثر من ذلك كلياً.

كان الحل في تقسيمه المفتاح.

كان الاكتشاف الذي خرج به ديفي ينطوي على ما يبدو في تاريخ الكريبتوجرافيا هرطقة خالصة: مفتاح عام/ علني. حتى هذه النقطة كانت هناك، على ما يبدو، مجموعة من القوانين المندسة في التشفير، والتي تبلغ حدّ الفقيدة المسلَّم بها، ولا يملك أحد تجاوزها وإلاّ كان مصيره جحيم الكريبتو. ومنها أن المفتاح الذي جرى به «تشفير» الرسالة هو ذاته الأداة التي تُستخدم في فكّ تشفيرها. ولهذا السبب كان يشار إلى المفاتيح بالمتماثلة، ولهذا السبب أيضاً، كان الإبقاء على تلك المفاتيح سراً أمراً عسيراً جداً: لأن الأدوات التي يسعى إليها المتنصّتون، أي مفاتيح فكّ التشفير ذاتها، يجب أن تنتقل من شخص إلى آخر، وبالتالي تتواجد في مكانين، فتزداد بذلك احتمالات الخطر. ولكن ديفي النيّ امتلأ دماغه بكمّ هائل من المعلومات التي تكبّد أشد العناء في جمعها، على امتداد نصف عقد من الزّمن، بات يرى الآن احتمالاً، بوجود أسلوب آخر لمعالجة الموضوع. فبدلاً من استخدام مفتاح سري مفرد واحد، تستطيع أن تستخدم زوجاً من المفاتيح. ومؤدى ذلك أن المفتاح المتماثل، يُستعاض عنه بمفتاحين ديناميكيين، أحدهما يقوم بتشفير نص الرسالة، يؤدي مهمته على نحو يحول دون قراءتها من الغرباء، بينما مع تضمين الرسالة باباً سرياً. أما ثانيهما فهو أشبه بالقفل، ووظيفته فتح الباب السري ليسمح لحامله بقراءة الرسالة. وهاكم الروعة في هذه الخطة: أجل، إنه المفتاح الثاني ـ أي مفتاح الباب السري ـ وهو الجزء الثمين من هذا الترتيب الذي لا بدّ من إخفائه، طبعاً، وراء ستارة، بعيداً عن متناول المتنصتين المحتملين. أما القرين، المفتاح الآخر الذي يقوم بالتشفير، فليس من الضروري أن يكون سرّاً على الإطلاق.

بل الحق أنَّك قد لا ترغب في أن يكون سراً أصلاً، بل سوف يكون من دواعي غبطتك إشاعته بين القاصي والداني.

والآن، كانت فكرة توفير السرِّيَّة والخصوصيَّة باستخدام مفاتيح يجري تبادلها علناً، فكرة مجافية للبداهة، بل غريبة في ظاهر الأمر. ولكنها قد تنجح باستخدام رياضيات الدوال (التوابع) الوحيدة الاتجاه. وكان ديفي يعلم هذا، وأدرك في لحظة إلهام أنه يستطيع تنفيذ الفكرة باستخدام تلك التوابع.

كان ذلكم هو الحل للمعضلة. ومنذ تلك اللحظة، أصبح كل ما في عالم الكريبتوجرافيا في حال غير ما كان عليه.

أولاً، أن ديفي بتقديمه بديلاً للنُّظم التي تقوم على مفتاح متماثل واحد، أتى بحل لمشكلة كانت وثيقة الارتباط بنُظم الكريبتوجرافيا إلىٰ حدّ أنَّه لم يكن ليخطر ببال أحد تقريباً، أن هذه المشكلة قابلة للحل: عنينا بذلك صعوبة توزيع هذه المفاتيح السرِّيَّة على من يتلقون الرسائل السرِّيَّة مستقبلاً. فإذا كنت تنظيماً عسكرياً فقد يكون بوسعك حماية مراكز توزيع المفاتيح المتماثلة السرِّيَّة (والله تعالى يعلم أنَّه في أشد العمليات حساسيَّة ثمة سقطات أو ثغرات). أما إذا انتقلت مثل هذه المراكز إلىٰ القطاع الخاص، وجماهير الناس التي تضطر لاستخدامها، فلن يكون أمامك أكوام الأوراق من الإجراءات البيروقراطية الحتمية وحسب، وإنما التهديد القائم بالخطر من شيوع السرّ أيضاً. فانظر إلىٰ الأمر إن شئت من الناحية التالية: إذا كنت مضطراً لتفكيك رسالة مشفَّرة، أفلا يكون وجود مكان يختزن جميع المفاتيح السرِّيَّة فرصة لشخص بغيض للحصول على هذه المفاتيح إن بالسرقة، وأو بالرشوة، أو أي شكل من أشكال القسر؟

أما بوجود نظام المفتاح العام، فإنَّه سيكون بوسع كل شخص صوغ مفتاحه المزدوج الفريد، المؤلَّف من مفتاح عام وآخر خاص، ولا يمكن لطرف خارجي الوصول إلىٰ الأجزاء السرية من المفتاح. وعندئذ يمكن للاتِّصالات الخاصَّة أن تجري.

وهاكم كيف يعمل المفتاح المزدوج: افترض أن أليس ترغب في الاتّصال ببوب. فإذا أخذنا بتصوّر ديفي، فإنّها لا تحتاج إلاّ إلىٰ المفتاح العام الذي يملكه بوب. وهي تستطيع حيازته بأن تطلبه من بوب، أو لعلّها تلجأ إلىٰ ما يشبه دليل الهاتف الذي يحتوي علىٰ لمفاتيح العامّة. لكن يجب أن يكون مفتاح بوب العام ذاته، مفتاحه الشخصي، وهو شريط طويل من لبتات من وضع شخص واحد، ولا أحد سواه في العالم... بوب. ثم تقوم باستخدام ذلك المفتاح العام، بطريقة الدالة (التابع) الوحيدة الاتجاه، لتشفير الرسالة بحيث لا يمكن فكّ تشفيرها حسابياً إلاّ بواسطة المفتاح الخاص. النص الآخر من ذلك الزوج الفريد من المفاتيح (هكذا فالمفتاح السرّي هو «الباب السحري» في الدالة الوحيدة الاتجاه للباب السري التي كانت تشغل تفكير ديفي).

ولذلك حين تبعث أليس برسالتها المشفّرة، فلن يكون هناك إلاّ شخص واحد في العالم يملك المعلومات اللازمة لقلب المعادلة وتفكيك الشّيفرة: أي بوب حامل المفتاح الخاص. والآن افترض أن الرسالة المشفّرة وقعت في يد شخص متلهف لمعرفة ما الذي قالته أليس لبوب، ومن يهتم بذلك؟ إذا لم يستطع المتطفل الحصول على الشريك الوحيد للمفتاح العام الذي يحمله بوب ـ الأداة التي استخدمتها أليس، لتحويل الرسالة إلىٰ ما هو أشبه بفوضى لغوية ـ فإن اعتراض الرسالة، لن يأتي للمتطفل بأكثر من تلك الفوضى. وبدون ذلك المفتاح الخاص، فإن عكس عملية التشفير رياضياً تغدو أمراً بالغ الصعوبة. تذكر أن السير في الطريق الخاطئ في الدالة (التابع) الوحيدة الاتجاه أشبه بمحاولة جمع قطع طبق لعشاء إلىٰ بعضها البعض بعد أن غدت فتاتاً.

أما بوب فلا يجد، طبعاً، أي صعوبة في قراءة الرسالة الموجهة إليه حصراً. فهو يملك الجزء السري من المفتاحين، ويستطيع استخدام المفتاح الخاص في فك شيفرة الرسالة في لحظات.

وباختصار، فإن بوب يستطيع أن يقرأ الرسالة لأنه الوحيد الذي يملك كلا الجانبين من المفتاح المزدوج. أما الذين يملكون المفتاح العام، فلا ميزة لهم عندما يحاولون تفكيك الرسالة. أما حين يتصل الأمر بتشفير الرسائل، فإن القيمة لو حيدة لامتلاك مفتاح بوب العام يتجلّى، في النتيجة، بقلب الرسالة إلى كلام بوب، أي اللغة الوحيدة التي يستطيع بوب وحده قراءتها (بفضل امتلاكه النصف السري من المفتاح المزدوج).

إن وظيفة التشفير هذه، إن نملكا نت جزءاً وحسب من التصور الثوري الذي أتى به ديفي، وليس بالجانب الأهم بالضرورة. فقد قدم المفتاح العام في الشيفرة أول وسيلة فعّالة للتحقّق على الوجه الصحيح من هوية مرسل الرسالة الإلكترونية. وإن الباب السري، كما تصوره ديفي، يعمل باتجاهين. فإذا قام أحدهم بإرسال رسالة مشفّرة بوساطة مفتاح عام يخص شخصاً ما، فإن المرسَل إليه المقصود وحده الذي يستطيع قراءتها. أما إذا عكست العملية. أي إذا قام أحدهم بتشفير نص ما بمفتاحه الخاص، فلا يمكن فكّ التشفير إلاّ باستخدام المفتاح العام الذي يطابق قرينه المفتاح الخاص. ولعلك تتساءل عن الغرض من ذلك؟ إذا تلقيت رسالة من شخص يزعم أنه ألبرت آينشتاين، وتساءلت إن كان هو ألبرت آينشتاين حقاً، فإن لديك الآن طريقة للتحقق من صحة هذا الزعم، اختبار رياضي بمثابة الاختبار بمادة غبار الشمس الزرقاء. وذلك بأن تأخذ لمفتاح العام لألبرت آينشتاين، ثم تطبقه على النص المشفّر. فإذا كانت النتيجة نصاً واضحاً ولم تخالطه الترهات، غدوت على يقين من أن آينشتاين هو صاحب الرسالة، لأنه يحمل المفتاح الخاص الوحيد في العالم الذي يمكن أن يقدم رسالة يستطيع مفتاحه العام الملازم للخاص أن فكّ تشفيرها.

ومؤدى ذلك بعبارة أخرى، أن استخدام المرء مفتاحه الخاص في رسالة ما، يعادل توقيعك: إنه توقيع رقمي digital signature. لكنه يختلف عن التواقيع

التي تظهر بها شيكات المصارف، وأوراق الطلاق، أو تمهر بها كرات الرياضيين، فالتوقيع الرقمي لجون هانكوك، لا يمكن تزويره من أي شخص لديه قدر أدنى من المهارةاللاز مة لتقليد خطوط صاحب التوقيع الأصليو سماته المميزة. فالأمل ضئيل بأن يتمكن اللص منتحل التوقيع، من تقديم توقيع مزوّر بدون المفتاح السري.

كذلك ليس للمزور المحتمل، أمل بر صد خط هاتف شخص ما، ثم لاإنتظار حتى يظهر التوقيع الرقمي لضحيته، فيلتقطه بغرض استخدامه في تزوير الوثائق أو اعتراض الرسائل مستقبلاً. ذلك أن التوقيع الرقمي لا يلحق عملياً بالوثيقة أو الرسالة. بل يتداخل بصورة وثيقة مع الأرقام التي تشكّل محتوى المادةللمر سلة كلها. فإذا ما تم اعتراض الرسالة، فإن المتنصت لن يتمكّن أن يستخلص منهاالأدوا ت اللازمة ليضع توقيع المرسل على وثيقة أخرى.

إن هذا الأسلوب يكفل، صحة الوثيقة برمتها. فليس للعدو أملٌ بتغيير جزء صغير من لر سالة الموقعة رقمياً، إنما سيكون التغيير كبيراً (مثل تبديل النص من «إني لست مسؤولاً عن ديون زوجتي» إلىٰ «إني مسؤول عن ديون زوجتي» وتوقيع المرسل الغافل محمول بالرسالة). وإذا كانت الرسالة موقعة رقمياً بمفتاح خاص، إنما دون تشفير، فبو سع ذيإ لقصد المريب أن يعترضها ويستخدم المفتاح العامللمر سل الموزع على نطاق واسع لتفكيك الرسالة، ثم يعمد بعدئذ إلىٰ إحداث التغيير في النص غير المشفّر. ولكن ماذا بعد هذا؟ إن صاحبنا المزوّر سوف يحتاج، لكي يعيد إرسال الرسالة من جديد إلىٰ المفتاح الخاص لمهر الوثيقة بكاملها بالتوقيع. سوى أن هذا المفتاح لن يكون متيسراً، لأنه يبقى دائماً في حوزة المرسل الأصلي.

كذلك من الميسور للمرء أن يبعث بر سالة محاطة بالسرِّيَّة فضلاً عن مهرها بالتوقيع. فإذا أراد مارك مثلاً أن يوجّه أمراً إلىٰ مد يرة المصرفا لذي

يتعامل معه، لينور، فإن أول ما يفعله هو توقيع الطلب بمفتاحه الخاص، ثم يقوم بتشفير الرسالة باستخدام مفتاح لينور العام. فتتلقى لينور رسالة مشفَّرة مرتين: مرة ابتغاء السرِّيَّة، ومرة للتثبت والتحقّق. فتستخدم أولاً مفتاحها السري لفتح مغاليق الرسالة التي لا تستطيع سوى عينيها قراءتها. ثم تعمد إلىٰ استخدام مفتاح مارك العام، لتفك الرسالة التي تعلم أن صاحبها لا يمكن أن يكون سوى مارك.

وللتوقيع الرقمي، ميزة أخرى تتجلّى في استحالة إنكار صاحبه لدوره في توجيه الرسالة، لأنه لا يمكن لشخص سواه أن يأتي بمثلها وهي لموقعة رقمياً، وهو ذاته الذي يحمل لمفتاح الخاص الذي قام بعملية التشفير. وهذه الميزة الملزمة بقبول نص الرسالة تعادل خاتم الكاتب العدل.

ولقد أصبح من الممكن لأول مرة إجراء كافة المعاملات الرسمية من عقود وإيصالات وماشا به بوساطة للكومبيوتر دونما حاجة لمثول صاحب العلاقة شخصياً للتنفيذ.

باختصار، لم يأت ديفي بطريقة تكفل السرِّيَّة والخصوصية في عصر شاعت فيه الاتصالات الرقمية وحسب، بل فتح الطريق كذلك إلىٰ قيام شكل جديد كلياً من التجارة، هي لتجارة الإلكترونية التي لديها القدرة، لا أن تضارع الوثائق المعتمدة في التجارة حالياً فقط، وإنما أن تتفوّق عليها أيضاً. والأدعى للإعجاب، أن إنجازه كله تم بعيداً عن رقابة الوكالات الحكومية التي تمتلك حتى أصغر التفاصيل، لأكثر أنظمة الكريبتوجرافيا غموضاً.

ويا له من نصر لهويت ديفي! ثم يا له من فخر أصابه حين كاد، في لحظات، بعدما تفتق ذهنه عن أهم كشف في تاريخ الكريبتوجرافيا، أن ينسى ذلك كله. كان قد نزل إلىٰ الطابق الأرضي ليتناول زجاجة من المياه الغازية، وفي لحظة رهيبة واحدة وجد أن كل ما خطر بباله قد تسرَّب وتلاشى. فدار حول منضدة المطبخ، وإذا به يستعيد خواطره كلها، هكذا بسرعة البرق. إلاَّ أن

تلك الأفكار باتت لصيقة في هذه المرة لا تغادر رأسه. ومع ذلك، فإنه لم يعمد إلىٰ تدوين أفكاره، ثم لمع في خاطره، فجأة، أن الكومبيوتر الذي كان يحفظ فيه ملاحظاته غير آمن. ولهكن با لمستطاع حينذاك أن يقوم بتشفير أفكاره منعاً لوقوعها في يد المتطفلين. وإذن، فلا محيص له من أن يطلع مارتي هيلمان عليها وجهاً لوجه، حين يلتقيه.

لكن كان عليه أولاً أن ينتظر عودة ماري إلىٰ لبيت من عملها.

حينما عادت ماري فيشر من عملها في شركة بريتش بتروليوم، وجدت زوجهاينتظر ها عند الباب، وكان ذلك من غير عادته. وقد ارتسمت على وجهه نظرة غريبة، وسمعته يدعو ها إليه إذ لديه ما يحدّثها به.

قال هويت ديفي: «أعتقد أنني حقّقت اكتشافاً عظيماً».

وراح يشرح لها فكرته. ومع أن جانب الرياضيات من الموضوع يتجاوز إمكاناتها، إلاّ أن التصور الذي عرضه كان مفهوماً لديها بشكل صحيح. والأكثر من ذلك أن ماري التيلا حظت زوجها طوال سنوات عن كثب، وهو يصارع المشكلة، وجدت الحل مناسباً بل شعرياً كذلك. وتقول ماري في زوجها المولود تحت برج الجوزاء: «لطالما كان ذا شخصية مزدوجة، وأحسب أن فكرة تقسيم المفتاح نشأت من ذلك التوتر».

بعدما حقّق هذا كله لم يعد باحثاً عجوزاً منهاراً.

في تلك الليلة، نزل ديفي مشياً على الأقدام من التل إلىٰ منزل هيلمان ليحدثه، لأول مرة، في أمر المفتاح العام. ولقد استغرق الأمر بعض الشرح، إلاّ أن هيلمان سرعان ما أدرك أهمية ما تمخض عنه العصف الدماغي لديفي. لكن بقي على الاثنين أن يصوغا هذا في مقال علمي، ثم ينشراه. وكان مارتي هيلمان يعرف المكان المناسب؛ فقد تلقى دعوة قبل حين لكتابة دراسة حول التفاعل المتبادل في نظرية المعلومات لمجلة آي إي إي IEEE، فانتهز

المناسبة، وعرض على رئيس تحرير المجلة اقتراحه بأن يتعاون وديفي في تطوير هذا التصور، فرحّب بالفكرة أشد الترحيب (IEEE هي الأحرف الأولى لـ Institute of Electrical and Electronical Engineers مؤسّسة مهندسي الكهرباء والإلكترونيات، وهي جمعية أكاديمية هندسية مرموقة، وتتولّى إصدار عدد من المجلات، ولبعضها أشد النفوذ في مجالاتها). فشرع الاثنان في العمل فوراً، وهما يواجهان حقيقة أنكل ما لديهما هو هذا التصور الذي اكتشفه ديفي وما ينطوي عليه من إمكانية الانتقال بالكريبتوجرافيا إلى عصر جديد.

كان هذا التصور يبدو أحياناً، حتى لهيلمان، كما يتذكر فيما بعد، «ضرباً من الجنون». وفي أحد الأيام قرّر اطلاع زميله القديم في شركة آي بي إم، هورست فايشتل. وكان ما جرى بينهما حديث غريب. ذلك أنّه ما أن شرع هيلمان في الكلام حتى قال له فايشتل أن لديه عشرين دقيقة فقط للحديث، لأنه في طريقه إلى موعد مع الطبيب. فأخذ هيلمان يعرض له بسرعة أنه وديفي قد تغلبا على مشكلة توزيع المفتاح بوساطة باب سرّي يعتمد على الدالة/ التابع الوحيدة الاتجاه، ويسمح لك باستخدام مفتاح عام/ علني؛ لكن فايشتل لم يقبل بذلك على الإطلاق. وقرّع هيلمان قائلاً: «إنّك لا تستطيع تنفيذ هذا الذي تقوله!» وتا بعربحا ضر فيه من أن لكريبتو جرافي الفلمنكي العظيم أوجست ليرتشوف قد وضع في كتابه العظيم: الكريبتوجرافيا العسكرية La Cryptographie Militaire، الصادر عام 1881، ست قواعد صارمة ينبغي ألا يحيد المرء عنها عند وضع شيفرة مأمونة، وإحداها: أن السرّيّة كلها ينبغي ألا تكون في النّظام، بل في المفاتيح. وخلص عبقري الآي بي إم الذي كان وراء جهاز لوسيفر إلى التساؤل، كيف لكما حتى أن تفكرا بجعل المفتاح عاماً وعلنياً؟ (لو لم يكن فايشتل على عجلة من أمره لمقا بلة الطبيب، فر بما كان قد أدرك أن فكرة ديفي وهيلمان، تتمثّل بكثير من الكياسة للشروط الصارمة التي وضعها كيرتشوف، من حيث أن أمن نظام المفتاح العام يكمن في حقيقة أن المفتاح الخاص يظل أبداً في ملك صاحبه ولا يستطيع الوصول إليه أحد سواه).

إلاّ أن فايشتل كان على صواب في أمر واحد، وهو أن التصور الذي أتى به ديڤي هرطقة. لكن «الهرطقة هي طريق التغيير» على حد قول هيلمان. ولقد انقطع هذا الثنائي طوال الأسابيع القليلة التالية للعمل المحموم على بناء الأساس الرياضي لنظرية المفتاح العام في الكريبتوجرافيا. وكان هيلمان قد عرف في تلك الأثناء السبيل إلى نجاح تعاونه مع صديقه الزئبقي: «غالباً ما كان هويت يرى، وهو يقلب أفكاره، أمراً ما في شكله الجنيني، أولاً، فالتقطه أنا، لأجعل منه نتيجة أكثر صقلاً».

وفي هذه الحالة كانت النتيجة بحثاً بعنوان: «أساليب كريبتوجرافية لعدة مستخدمين». كان هذا البحث، بمعنى ما، عملاً مرجعياً يعبّر عن فكرة المفتاح العام، بينما كان صاحباه يحرقان خلايا عقليهما وهما يحاولان العثور على طريقة، لتنفيذ هذا التصور وتطبيقه فعلاً. وقد اعترفا في بحثهما المنشور بأن: «ليس لدينا الآن لا البرهان على وجود أنظمة تقوم على المفتاح العام ولا نظام للعرض العملي». ومع أنّهما كانا قد أرسيا الأساس الرياضي لمثل هذا النّظام، فقد ظلا يتابعان البحث في الظلام عن التوابع الدقيقة ـ وخاصية الدوال (التوابع) الوحيدة الاتجاه للباب السري ـ التي تكفل تحقيق هذا التصور. ومع ذلك، فإن أولئك الذين تلقوا المسودات الأولى للبحث، وجدوا فيه انعطافاً مثيراً للدهشة، عن الحكمة التقليدية السائدة في الكريبتوجرافيا، وإغارة على أرض لم يجرؤ أحد، منذ عهد تريثيميوس حتى تورينج، على الخوض فيها.

أحقاً كان ذلك؟ طبعاً لو أن أحداً من وراء السياج الثلاثي أو أياً من أبناء العم الأجانب قد خرج بهذه الفكرة لما علم بها هيلمان وديڤي. ولو أن أحداً من العلماء نشر فعلاً بحثاً في هذا الموضوع، لكان ديڤي قد وقع عليه، بالتأكيد، أثناء البحث الواسع الذي اضطلع به في السنوات القليلة الماضية.

ولقد تبين أن ثمة شخصاً واحداً على الأقل، تشغل فكره ذات الأفكار التي كانت تشغل ديڤي وهيلمان.

في أوائل شباط/ فبراير 1976 تلقّى مارتي هيلمانو سالة غريبة من طالب يحضّر لنيل شهادةا لدكتوراه من جا معة كاليفورنيا في بيركلي:

عزيزي الدكتور هيلمان

قبل ثلاثة أيام حصلت على نسخة من ورقةعمل لك بعنوان «أساليب كريبتوجرافية لعدة مستخدمين». كنت قبيل اطلاعي على هذا البحث قد انتهيت من تنقيح بحث [لي] في الموضوع ذاته، ولسوف يقدم قريباً في كوميونيكيشنز أوف ذي أيه سي إم Communications of the ACM [جمعية الآلات الحاسبة Association of Computing Machinary]. (جرى تقديم البحث أصلاً في آب/ أغسطس 1975). وقد أرفقت بهذه الرسالة نسخة من هذا البحث آملاً أن تجدفيه ما يثير اهتمامك. والحق أني مسرور إذا علمت أن هناك شخصاً آخر معني بهذه المعضلة. فالذين أحاول مناقشتها وإياهم إما عاجزون عن فهم مجريات الأمور، وإ ما يعتبرون الحل أمراً مستحيلاً. ولحسن الحظ، أن الحل (الجزئي) المعروض في البحث المرفق أثبت أنّه ممكن. والآن، لو أننا نستطيع أن نتجاوز ما بلغناه!...

وانتهت الرسالة باقتراح: «إنإ مكانية القيام بعمل مشترك مطروحة، وإنني معني بهذالا حتمال. وأرجو أن يبلغني منك رد، متمنياً لك التوفيق في مسعاك».

وكان التوقيع باسم رالف ج ميركل، وعنوانه، في بيركلي يعكس كما يبدو، على سبيل المصادفة، السرعة التي باتت تسير بها الأمورهيست ستر يت Haste Street (Haste تعني عجلة).

وفي الواقع أن سم ميركل كان قد ظهر قبل بضعة شهور من ذلك

التاريخ: إذ كان هذا الطالب في بيركلي سبق أن ذكره لديفي صديق مشترك، هو بيتر بلاتمان، وهذا ما حفز ديفي على تشغيل آليات التفكير عنده وإقامة رابطة المفتاح العام الحاسمة. وقد بدا الآن أن ميركل قد أحدث انطلاقة، شبيهة بانطلاقة ديفي، معتمداً في أبحاثه على جهوده المستقلّة، ولا علة لديه سوى دماغه. وفوق ذلك أنّه حسب ما ورد في البحث غير المنشور الذي أرفقه برسالته، قد نفذ الحيلة التي كان هيلمان وديفي ما يزالان يتعثّران في تحقيقها، إذ وضع مخططاً لمفتاح خاص.

كان ميركل ابناً لرجل مثقف، شأنه في ذلك شأن مارتي هيلمان وهويت ديفي؛ فوالده كان المدير المساعِد لمخبر لونرس ليفرمور، وهو أحد أبرز مؤسّسات البحوث العسكرية في البلاد، حتّى توفي بسرطان القولون عام 1966. (تمتد مآثر آل ميركل إلى عم أبيه، فرد، وكان لاعب بيسبول، وعرف بهفوة شهيرة، هي إهمال لمس اللاعب الثاني، أثناء مباراة حاسمة لتحديد الفائز في راية السباق الوطني للأندية عام 1908). وكان الفتى رالف ميركل، كما هو مفهوم، هاوي علم ومبرزاً في الرياضيّات، ولما انتسب إلى الجامعة في بيركلي، بات متحمساً للكومبيوتر. أما بالنسبة للكريبتوجرافيا، فيخبرنا أنه «لم يبد أي اهتمام كبير ملحوظ في هذا الحقل». ولكن الحال تبدّل في فصل الخريف الجامعي عام 1974، حين اختار في الفصل الأخير، قبل التخرّج، دراسة مشروع دراسي يعرف بـ «سي إس 244» CS 244 في موضوع سلامة وأمن الكومبيوتر. قام بتمديد ريسها لانس هوفمان، وهو أستاذ مساعد في قسم الهندسة الكهربائية وعلوم الكومبيوتر. وكانت الشروط الأساسية للنجاح في هذه الدورة تنفيذ مشروع، بالإضافة إلى تقديم امتحان في شهر تشرين الثاني/ نوفمبر. وحسب قول هوفمان «إن علامات النجاح متدرجة بشكل منحني. لكنك إن حققت التفوق في صف حافل بالعباقرة، فلن تخشى شيئاً! لأنك ستنال علامة إيه A».

كان هوفمان قد أدخل ضمن مقرر سي إس 244 تدريس مادة الكريبتوجرافيا، إنما ليس على مستوى عالٍ. ذلك أن أشكال الشيفرة التي تعتمدها الحكومة كانت من الأسرار،بينما كا نت تلك الأشكال المستخدمة في القطاع الخاص، بل حتّى في الجامعات، بدائية نسبياً. ويعترف هوفمان اليوم: لم نكن نتوسع في هذا المجال وتفاصيله. وإني واثق من أنني كنت أو س شيفرة قيصر وما شابه. ولا تنس أن كل ما كان لدينا يومذاك هو الشيفرات البديلة، والشيفرات المتبدلة، والتجميعات المركبة.

ومنذ اللحظة الأولى التي بدأت فيها الدورة في 1 تشرين الأول/ أكتوبر، بواقع حصتينأ سبوعياً، حتّى 5 تشرين الثاني/ نوفمبر، موعد تقديم أوراق البحث، كان رالف ميركل يميل إلىٰ التفكير بشكل أكثرطمو حاً. إذ ما أن سمع بوظيفةللكريبتو جرا فيا من حيث أنّها وسيلة لحماية المعلومات من تطفّل المتنصتين، حتّى وجدته يكاد لايتو قف عن لا نشغال الذي ما انقطع الناس منذ عهد يوليوس قيصر عن اعتباره المعضلةالأ سا س: ابتكار منظومات كريبتوجرافية أكثر منعة، وأقل قابلية للتفكيك مما هو شائع اليوم، ويمكن تشفيرها أو تفكيك شيفرتها بمفتاح متماثل.

وبدلاً من ذلك، ولأسباب ما تزال غير واضحة، إلاّ أنّها تتصل بطبيعة عقل ميركل غير التقليدي، ركّز اهتمامه على ما بدا له مظهراً غريباً، وتحدياً لمعضلة أشد جذرية. فقد كان السيناريو الكريبتوجرافي الأساسي، يفترض الضعف في قناة الاتّصال. وكانت هذه هي الحال حقاً في الإرسال البرقي والبث الإذاعي، وموضوع مادة الدراسة في المقرر الذي يدرسه هوفمان، أي شبكاتا لكومبيوترا لمفتوحة. ولكن ما هي الإجراءات التي بوسعك الإفادة منها، إن شئت الاتصال بشخص لا يملكمفتا حاً متماثلاً مأموناً متفق عليه مسبقاً؟ هل هناك طريقة يستطيع بها هذان الشخصان إجراء حليث مع بعضهما البعض بطريقة عفوية وواضحة لكليهما، ولكنها معماة على من يحاول التنصّت

عليهما؟ وهذه المشكلة، كما بات ديفي وهيلمان يدركان الآن، لم يتصد لها أحد من قبل، لأنها تنأى بلا ريب عن الحل.

أما ميركل الذي لم تفسده المعرفة بنظرية الكريبتوجرافيا أو تاريخها، فكان لاهياً عن استحالة تحقق المهمة التي يتصدّى لها. وكل ما قام به هو محاولته حل المعضلة وحسب. كان الجانب الحاسم في الوضع يكمن، في رأيه، في اختلا ف ظروف الشخصين اللذين أرادا التخاطب فيما بينهما واحتمال وجود متطفل. هنا، ينهمك هذان الشخصان في الحديث بشكل إيجابي بينما المتنصّت مستمع سلبي. ولقد أدرك ميركل أن الحل يكمن في استغلال التآمر بين المتحادثين، أثناء حديثهما، فينشأ بذلك وضع يستطيعان فيه، كما يقول: «تشويش عقل المستمع السلبي، ولو سمع كل ما يدور بينهما من حديث». وشرع الرجل يقدح زناد فكره في هذا الأمر حتّى كاد أن يستحوذ عليه. وفي إحدى ا لليالي من تشرين الأول/ أكتوبر 1974، وبينما هو جالس في سريره، في شقته الصغيرة، يحدق في سقف الغرفة، رأى الرجل نفسه وقد وجد الحل الممكن للمعضلة.

أحجيات:

هاك الخطة التي تفتق عنها عقل ميركل في عتمة الليل في غرفته. الوضع التقليدي: يريد بوب وأليس التحادث في أمر ما. بوب هو المرسل وأليس هي لطر ف المستقبل لرسالة سرية. ولكن هناك لسوء الحظ متنصّت غير مرغوب فيه، هو إيف التيتستطيع سماع كل ما يمكن أن يدور بين الطرفين. فكيف يمكن لبوب أن يبعث برسالة تستطيع أليس قراءتها، وتعجز إيف عن إدراك فحواها؟ عليه أولاً ابتكار أحجيات كل واحدة منها هي رسالة مشفّرة جرى تشفيرها بوساطة مفتاح صغير نسبياً، مفتاح يمكن معرفته بقدر مقبول من الجهد في الهجوم بالقوة الغاشمة؛ وهذه مهمّة صعبة إلاّ أنه يمكن بالكومبيوتر الذي تملكه أليس. وفي هذا يقول ميركل: «وهذا سببو صف الأمر بالأحجية،

ا للغز، وإنها لمعضلة يصعب حلها، لكن الحل ممكن، بالبحث وتجربة مختلف تر كيبات الأَرقام في مدىا لمفتاح». وبوب لا يبتكر بوساطة الكومبيوتر الخاص به أحجية واحدة فقط، بل الآلاف، وربما الملايين. وهذه كلها ترسل إِلىٰ أليس.

تقوم أليس، في نهاية المطاف، بنشر هذه الأحجيات على الأرض وتختار إحداها عشوائياً. (إيف قادرة طبعاً على اعتراض هذه الأحجيات كلها، لكنها لا تدري ما الذي اختارته أليس منها). ثم تقوم أَليس بمعالجة الأحجية التي اختارتها بأن تجعل كومبيوترها يبحث في مدى المفتاح حتَّى تقع على الحل. ويشتمل هذا الحلعلى شريط من الأَرقام، إنه الرسالة التي تضمنتها تلك الأحجية بعد تفكيك شيفرتها. هنا يكون حل تلك الأحجية بين يدي أَليس وبو ب معاً. إن بوب يعرف الحل، طبعاً، لأن الأحجية من ابتكاره، وهو يملك الحل لكل الأحجيات التي أرسلها. غير أن إيف لا تملك ذلك الحل. ولئن تكن قد اعترضت كل ما أرسلهبو ب إِلىٰ أَليس، إلاَّ أنها لا تملك الوقت ولا الكومبيوتر المتطور للعثور على الحلول لهذه الأحجيات كلها، بالإِضافة إِلىٰ أنَّها تجهل الأحجية التي اختارتها أليس.

أما الخطوة التالية لأَليس، فهي إعلامبو ب بالأحجية التي اختارتها. وهذا أ مر يسير؛ ذلك أنالأحجية ا لمشفَّرة تتضمَّن مؤشراً (إِشارة تقول، مثلاً، «هاك أنا الأحجية رقم 3!»). ومفتاحاً رقمياً طويلاً. وهكذا، حين تعيد أَليس الرسالة، (الأحجية رقم 3)، فإن بوب يستطيع العثور على المفتاح المتضمن في الأحجية. وهنا يكون لدى كليهما مفتاح سرِّي يشتركان فيه، ويستطيعان استخدامه في إجراء المزيد من الاتِّصالات السرِّيَّة. وربما تكون إيف قد سمعت بالأحجية رقم 3، لكنها لن تدري أي أحجية من ملايين الأحجيات هي المقصودة. لتتذكر، أن عليها أن تحل كافة الأحجيات حتَّىتبلغ ا لمفاتيح. ولئن يبدو هذا ممكناً ستخدام كومبيوتر عملاق على درجةعا لية من التطور، فإنه

يقتضي من المتنصت بذل جهد أكبر مما بذله كل من أليس وبوب، ربما بملايين المرّات. لكن مقدار الجهد اللازم ليس هو النقطة الهامّة.

وهاكم النقطة الهامة: لقد استطاع رالف ميركل، في شقة صغيرة في بيركلي، وبعيداً تماماً عن مجال وكالة الأمن القومي، أن يجد طريقة يستطيع بها شخصان، دون اتفاق مسبق بينهما على مفتاح سري، أن يرسلا رسالة سرية، تحبط الجهود التي يبذلها متنصّت مجتهد لتفكيكها.

ورُبّ سائل يسأل عما هي العمليات التي تجري في عقل من يأتي بمفهوم جديد كل الجدة في الكريبتوجرافيا، ذلك المفهوم الذي يدحض التيار الفكري السائد في هذا الحقل على امتداد أكثر من ألف عام؟ ويقول ميركل في هذا: «كان أول ما خطر ببالي، إن هذا الحل عظيم؛ ولعلي أستطيع بواسطته تنفيذ ربع مشروع». ولئن بدا هذا القول بعيداً عن المغالاة، إلاّ أنه كان مع ذلك ينم عن مبالغة في التفاؤل. وكان الاتفاق هو أن يعرض ميركل للبروفسور هوفمان، موضوع بحثه أو «ربع المشروع»، فأسرع بكتابة عرض لما يعتزم القيام بدراسته. وكان ذلك العرض مختصراً بالضرورة ويشوبه الغموض. ويقول ميركل في ذلك مفسراً: «لم أستطع أن أذكر أي دراسات سابقة في الموضوع تقول أن المشكلة هامة وجديرة بالبحث لأنني لم أقع على دراسات سابقة تقول أن هذه المشكلة هامّة. وحسبت [عن حق] أنه ليس ثمة دراسات سابقة. ولذلك كان ما كتبته بشكل أساسي: مدونة صغيرة». وعلى سبيل الدعم، ذكر [لأستاذه] أنّه كان يعتزم كتابة بحث في تكثيف البيانات.

بعد أن قرأ لانس هوفمان الاقتراح، قال لصاحبه أنه من الأجدى له الكتابة في مشكلة تكثيف البيانات.

حاول ميركل إقناعَ ستاذه بأن موضوعه أجدر بالبحث، وأعاد اقتراحه عدة مرات في محاولة لحمل هوفمان على التسليم بأن الموضوع مثير للاهتمام، على الأقل، ليكون جديراً بالمتابعة. لكن هوفمان ظل ثابتاً على موقفه ولم يقبل

حتّى أن يمنحه تلك المنة البسيطة. فما هو السبب؟ يجيب ميركل: «لأكن مهذباً، وحسبي أنأ قول أنه كما يبدو لم يفهم ما كنت بصدد قوله آنذاك. ولذلك انقطعت عن متابعة الدراسة في هذه الدورة».

لم يكن ميركل قد عرف، بعد، بأمر مارتي هيلمان. لكنَّه كان يريد شخصاً ما، أي شخص، ليطمئنه بأن ما أملته عليه فطرته كان صحيحاً، وأنَّه وقع على أمر ذي شأن. غير أن ردود الفعل التي قابله بها الأكاديميون في بيركلي،كا نت مماثلة لما بدر من هوفمان: «كان القوم بصورة أساسيَّة يحدِّقون في وجهي مستغربينما كنتأ قوله أشد الاستغراب، وحجتهم في ذلك أن الموضوع، على ما يبدو، غريب جداً. وأخيراً، قدَّم له أحذ أساتذته، ويدعى روبرت فابري، بعض التشجيع، وقال له إن الفكرة جيدة، فحاول أَن تقوم بنشرها. وهكذا التفت ميركل إلىٰ بحثه وأعاد صياغته بشكل أكاديمي أفضل، آملاً أَن ينشر في مجلة [جمعية الآلات الحاسبة] كوميونيكيشنز أف ذي إيه سي إم ACM ذات المكانة الرفيعة. وقد جعل عنوان بحثه «اتِّصالات مأمونة عبر قنوات غير مأمونة»، وقدَّم موضوعه رسمياً في آب/ أغسطس 1975، إلىٰ رئيسة التحرير: سو جراهام.

وفي 22تشر ين الأول/ أكتوبر 1975، وجهت جراهام رسا لة إلىٰ ميركل قا لت فيها أن «خبير اً متمرساً في الكريبتوجرافيا قد اطلع على البحث المقدم ووجده غير صالح للنشر. (لم تذكر الرسالة سم القارئ، أو القارئة، جرياً على عادة إغفال الاسم، لكن القراء يتم اختيارهم عادة من بين الراسخين في حقلهم العلمي). وكان العيب الظاهر في ذلك البحث، وفق قول ذلك القارئ، هو عين الفرضية التي يقوم عليها، أي القول أنه من الممكن قيام نظام كريبتوجرافي دون ضمان تسليم المفاتيح. وهكذا إذن، فإن ما جعل فكرة ميركل ثورية هو نفسه ما جعلها مرفوضة أيضاً. وقد عبَّر القارئ عن رأيه بالقول: «إني آسف لإعلامكم بأن البحث لا يتفق والرأي السائد الآن في الفكر

الكريبتوجرافي. والتجربة تبين أن من الخطورة بمكان تداول معلومات جوهرية علناً». ولقد تكلفت سو جراهام ذاتها جهداً عظيماً لتؤكد اتفاقها في الرأي والقارئ، فنطالعها تقول في رسالتها: «لقد قرأت التقرير شخصياً وأزعجني فيه خاصة خلوه من الإشارة إلى المراجع. أفليس هناك شخص آخر عالج هذا النهج [؟]».

وإن الجواب فيما يتعلّق بالبحوث المنشورة حصراً، هو بالنفي.

انتاب ميركل يومئذ شعور بخيبة الأمل، لكنّه لم يشعر بالهزيمة. ولعله لم يكن متفاخراً متهوراً مثل والده، الذي وُصف ذات مرة بأنه «مزيج مثالي من عالم الفيزياء والبائع الشاطر»، وعرف بمزاجه العصبي ودخوله بسيارته الباكارد المكشوفة المتعبة ساحة الوقوف لمختبر ليضرمور بسرعة كبيرة. غير أن الشاب ورث عن أبيه روح الدأب والمثابرة. وراح يشذّب في مقاله وينقّح ولم ينقطع عن ذلك بالرغم من رفضه من عدة دوريات. ويقول في هذا: إن الملفت في الأمر كيف أن عملية النشركانت تؤدي إلى تحسينات متزايدة، إلاّ أنّها كانت سيئة جداً في تناول موضوع يختلف كل الاختلاف عن المعهود». لكنّه كان واثقاً من أن الفكرة التي عرضت له كانت جديرة بالمتابعة: «لا يمكن أن تكون الفكرة خاطئة لأنها بسيطة. ولم يكن من الواضح إلى أين ستقودنا، إلاّ أنه كان واضحاً جداً بضرورة عرضها. وكنت أريد بشكل أساسي نشر تلك الفكرة والإعلان [على الملأ] هاكم فكرة بسيطة، وهي توضح طبيعة المشكلة وتبين حقيقة أن لها حلاً ممكناً، وأنّهابات الآن مشكلة بحث محددة. لندعُ بعض القوم إلينا، ولنر عندئذ أي جديد سوف يتمخض عنه بحثنا».

في أوائل عام 1976، وكان ميركل قد بدأ يشعر بالإحباط، أخبره زميل له أنّه يعرف بعض الأشخاص الذين يشاطرونه اهتمامه، وأبرزهم مارتي هيلمان. وجدير بالذكر أن من بين المواد التي كان هيلمان يقوم بتدريسها، مادة تبث عبر دارة مغلقة ما بين ستانفورد وبيركلي. وقد استطاع ميركل

الاستماع إلى إحدى لحلقات المذاعة، وأدرك فوراً أن مارتي هيلمان كان بالفعل يشاركه التفكير في الأمور ذاتها التي تشغل فكره. وفي الوقت الذي أخذت فيه مسودة البحث الذي وضعه ديفي وهيلمان حول «أساليب كريبتوجرافية لعدة مستخدمين» توزع على البعض قبل أن تُنشر استطاع ميركل الحصول على نسخة منها. وبدلاً من الشعور بالضيق لأن هناك من سبقه إلى نشر هذه الأفكار، انتابه إحساس بالغبطة لكون تصوره بات موضوعاً يطبّق فعلاً. وكان أن حفزته الفكرة عند اطلاعه على البحث أن يسعى للانضمام إلى الباحثين في جامعة ستانفورد؛ وهذا ما جعله يوجه رسالته إلى هيلمان المؤرخة في 7 شباط/ فبراير والتي اقترح فيها قيام تعاون بينهما، مرفقاً بها مسودة بحثه، بدلاً من نبذة عن حياته.

كان بحث ميركل كشفاً بالنسبة لديفي وهيلمان، إذ لم يكن ليخطر ببال أي منهما أنه سيرى أفكارهما تطبق حقاً قبل مضي فترة من الزمن. ورأى الرجلان في تصور الأحجية، الذي بلغه ميركل تطوراً مؤكداً، وإن كانت تعتوره المشكلات. وهكذا سرعان ما غدا ميركل جزءاً من النقاش بين ديفي وهيلمان حول تطبيق المفتاح العام. ولقد تساءل ميركل كيف يمكن لفكرة الأحجية التي خرج بها أن تندمج وذلك لضرب من المفتاح العام الذي أخذ به ديفي وهيلمان في إطار منظومتهما الكريبتوجرافية. ثم اقترح في رسالة مؤرخة في 2 نيسان/ أبريل 1976 منظومة تسمح بأن يكون لكل مستخدم مجموعة خاصة فريدة من الأحجيات ـ وتكون هذه في ذاتها المفتاح العام. «وهكذا إذا شاء أحدهم أن يبعث برسالة إلى الجهة ألف A فما عليه إلاّ أن يختار عشوائياً إحدى أحجياتها. ثم يعمد إلى تشفير الرسالة وإرسالها إلى الجهة ألف A. وتقوم الجهة ألف بفحص مفتاح الأحجية مستخدمة بطاقة الأحجية على وجه الرسالة. ولو أراد سواهم قراءة الرسالة لما استطاع، لأنه لا يملك معرفة مفتاح الأحجية». كما كتب ميركل.

ولقد قام ميركل بالتفكير في كيفية الاستفادة من الأحجيات المندمجة في

نظام المفتاح العام، في تلقي الإيصالات باستلام الرسائل. ولما بلغ هذا الحد، جعل من فكرته هذه طعماً مغرياً، وأسر بأنّه يبحث عن عمل في فصل الصيف. وأشارت جملة الختام في رسالته إلىٰ المثلب العملي في منظومته، أن مستوى الأمان الذي توفره الأحجيات، إنما كان على المستوى الحدودي رياضياً Polynomial، وليس على المستوى الأسي Exponential الأشد صرامة. وإذن، فإن على المتنصت أن يجهد نفسه كثيراً حتّى يتمكن من حل الأحجيات، لكن عامل الجهد ذاك كان محدوداً بعدد الأحجيات. ولنفترض أن أليسأر سلت إلىٰ بوب؛ وفق نظام الأحجيات المشفّرة، مليون أحجية ليختار منها المناسب، غير أن المتطفلة إيف، كان لديها كومبيوتر أسرع في إجراء العمليات الحسابيةأ لف مرة من ذاك الذي يستخدمه بوب. (ليس في هذا الافتراض مبالغة، إذا أخذنا بعين الاعتبار، أن ثمة حكومات غنية، ولديها موارد كومبيوترية ضخمة، وربما رغبت بفك الرسائل المشفّرة التي يصدرها أو يتلقاها هذا الطرف أو ذاك). وقد تتمكن أليس من حلأ لف أحجية، في حين أن بوب يستغرق الوقت ذاته لحل أحجية واحدة مختارة عشوائياً. فإذا احتاج بوب إلىٰ دقيقة لحل أحجية واحدة، فإن أليس تحل مليون أحجية في حوالي ست عشرة ساعة، وهذا وضع لا يحتمل إطلاقاً بالنسبة لأولئك الذين يحتاجون حماية قوية. وحتّى لو كان كومبيوتر أليس لا يزيد قوة عن الكومبيوتر الذي يستخدمه بوب، فإن أليس تستطيع حل كل الأحجيات في أقل من عامين. وإذا كان الحفاظ على السرّيّة ضرورياً، فإنّه ليس بالمرغوب، أيضاً. (من جهة أخرى، فإن مثل هذه المدة كافية للتحقّق والتثبت، طالما أن معرفة مفتاح التوقيع بعد عام من استخدامه لن يوفّر للعدو أي ميزة ذات شأن). إن أي نظام تشفير يعتد به، عليه أن يكفل ـ مهما تكنا لدالة الوحيدة الاتجاه المستخدمة ـ وجود علاقة أسية، رياضياً، بين الحسابات السهلة للمرسل والمهمة الأصعب المفروضة على المتنصت. وهذا كفيل، من الناحية المثالية، بزيادة حجم عمل الخصم إلىٰ حد يتطلب آلاف، أو ملايين أو مليارات السنين لإنجاز المهمة. وكان ميركل يأمل بالتوصل إلىٰ

طريقة تجعل منهجه يفي بهذه الشروط. فكتب إلىٰ هيلمان يقول: «ربما نستطيع أن نصل إلىٰ الأسية في نهاية هذا الصيف».

بينما كان ميركل يقدح زناد فكره بحثاً عن طريقةللو صول إلىٰ الأسية، كان اهتمام ديفي وهيلمان منصباً على ابتكار طرقهما الشخصية لتنفيذ منظومتهما الخاصة بالمفتاح العام للشيفرة. ذلك أنّه إذا لم تتوفّر لهما طريقة ما لو ضع أفكارهما موضع التطبيق أو على الأقل إثبات إمكانية وجود خطة عملية لذلكفلسو ف يبدو تصوار لمفتاح العام للشيفرة مجرد حيلة من حيل العقل الرياضي.

وكانت إحدى تلك الطرق، ما عرضه دونالد كنوث: عالم الكومبيوتر في جا معة ستانفورد، والذي أكسبته سلسلة كتبه الموسوعية «من برمجة الكومبيوتر» The Art of Computer Programming، التي ما زالت أجزاؤها تتالى، سمعة واسعة باعتباره حجَّة الخوارزمية الأكبر. فقد ذكرهما كنوث بظاهرة رياضيَّة طريفة: ففي حين أن ضرب عددين أوليين ببعضهما عملية بسيطة كلعب الأطفال، فإن عكس هذه العمليَّة ـ وتدعى التحليل إلىٰ عوامل ـ قد تسبِّب الحيرة للشيطان ذاته. فهل تصلح هذه الظاهرة ساساً لدالة (تابع) وحيدة الاتجاه شيطانيَّة يصعب اختراقها؟ ولئن لم يشأ ديفي وهيلمان متابعة هذه الفكرة فإن هناك آخرين اتبعوا هذا الطريق.

كان ثمة حل آخر ينطوي على تعقيد حسابي، التفت إليه ديفي وانقطع لقراءة كتاب مكرس له، وخاصة الفصل المتعلق بما كان يسمى دوال (توابع) إن پي لكا ملة NP Complete functions، وكتب ديفي فيما بعد، يصف تلك التوابع بأنّها «مشكلات لم يكن يعتقد بأنّها قابلة للحل في وقت حدودي بأي كومبيوتر محكم». وكان مؤدى ذلكبأن هذه المسائل هي من الصعوبة بحيث تجعلك تتخذ كومبيوتراً من طراز ماكنتوش أو حتّى كومبيوتراً عملاقاً من طراز كراي Cray (إذا كنت وكالة الأمن القومي) لتتمكن من حل المعضلة، وإذا ما عدت

للتحقق من النتائج بعد بضعة تريليونات من السنين، وجدت نفسك ما تزال بعيداً بُعداً شاسعاً، عن الحل. ولئن كان ديفي يحمل بعض الأفكار للإفادة من الحسابات المركبة في وضع صيغة لدالة كريبتوجرافيةو حيدة الاتجاه فإنّه لم يقيض له إيجاد طريقة لتنفيذها مع الأبواب السحرية.

ولقد تجلّى الأمل باقتراح من أحد زملاء هيلمان في قسم لهند سة الكهربائية، فيستا نفورد، ويدعى جون جيل، إذ لفت الانتباه إلى عملية رياضية تُعرف باسم «الأسية المتفردة» كتابع محتمل. ولما كان عكس هذه العملية، والمعروف (باللوغاريتم المتفرد) عملية بالغة الصعوبة، فإن هذه المسألة حملت معها إمكانية تحقيق المعيار الأساسي للدالة (التابع) الوحيدة الاتجاه: أعداد بسيطة يتسلى الأخيار بحسابها، جحيم حسابي للأ شرار الذين يريدون عكس العملية.

كان ديفي يعمل في مختبر الذكاء الاصطناعي في جامعةستا نفورد في أحد أيام أيار/ مايو 1976، لإعادة صياغة البحث حول المفتاحا لكريبتوجرافي العام، والذي كان يعده مع مارتي للنشر، في وقت لاحق من العام، في مجلةمؤ سّسة مهند سي الكهرباء ولإ لكترونيات البارزة آي إي إي IEEE، حين اتصل به هيلمان ليخبره بصوت منفعل أنّه يعمل على الأسية المتفردة، وأنّه توصّل فعلاً إلى نظام عمليللمسأ لة. ولما مضى في الشرح أدرك ديفي فوراً أن هيلمان استطاع ربط الخطوط المتشابكة لنظرية كانت تدور في رأسه طوال أسابيع.

ولقد قُيض للخطة المقترحة أن تُعرفبا سم خوارزمية ديفي ـ هيلمان. وتقوم على الافتراض بوجود طرفين يريدان الاتصال سراً؛ وأن بإمكان هذين لطرفين توليد مفتاح مشترك معاً، باستخدام الدالة (التابع) لو حيدة الاتجاه، ولا يملك المتنصّت معها اعتراضا لمحادثة. وهاكم طريقةا لعمل:

يختار الطرفان أولاً رقمين. ويتم هذا علناً، لأن معرفتهما لن تفيد المتنصّت. ثم يختار كل طرف رقماً سرياً خاصاً به، ولا يكشف عنه أوير سله

إلىٰ أحد. ثم عن طريق استخدام صيغة رياضية تتصل بالأسية (الرفع إلىٰ القوة التجبرية)، يأخذ كل منهما رقمه السري الخا ص به، ويقوم بعمليَّة حسابية قوامها ذلك الرقما لسري والرقمان المعلنانا للذان سبق اختيارهما. وبعد عملية السحق الرقمية القصيرة هذه يكون لدى كل منهما رقم سري متحوّل ويرسل هذا إلىٰ الطرف الآخر. وليس في إرساله عبر قناةمفتو حة أي مشكلة لأنه، في النهاية، رقم سري مشفّر، تمّت تعميته بوساطة الدالة الوحيدة الاتجاه وهو سهل التنفيذ إلاّ أن عكسه بالغ الصعوبة (ما مقدار صعوبته؟ إن فكّ العملية هو، نظرياً على الأقل، صعب كحل مسألة للوغا ريتم المتفردة. وهذا يقتضي إجراء مليون كوادريليون عملية رياضية أكثر من عمليات الأسية المستخدمة في تحويل الأعداد. تلكم هي الدالة الوحيدة الاتجاه!).

وبمقدورك اعتبار هذا الزوج الثاني من الأعداد بمثابة المواليد التي نتجت عن الأرقام المعلنة المتفق عليها صراحة على الملأ والأَرقام السرِّيَّة المكتومة. ومحاولة لمتخلا ص الرقم السري من الرقم الذي يجري في القناة المفتوحة أشبه بفحص الحامض النووي DNA في الخلية البشرية ومحا ولةا كتشاف مساهمة كل من الأبوين في تكوين كل جينة على حدة. وهذا ما لن تقدر عليه ما لم يكن بوسعكلوا صول إلىٰ الحامض النووي، إما من السائل المنوي أو من خلايا البويضة.

يقودنا هذا إلىٰ الخطوة الثالثة والأخيرة من خوارزمية ديفي ـ هيلمان. هنا يعتمد كل من الطرفين صيغة رياضية خاصة تجمع بين هذه الأرقام لمتحو لة مع الأرقام السرية الأصلية (الحامض النووي الأصلي!) الخاصة بالطرف الذي يقوم بلعمليَّة للوصول، إلىٰ رقم آخر. وهذه الصيغة تعمل بحيث يتوصل كلاهما إلىٰ رقم نهائي متماثل، بالرغم من أن الأعداد الأصلية لديهما مختلفة عن بعضها البعض. ويمكن تسمية هذا الرقم المتماثل «م»، الحرف الأولفي كلمة مفتاح. وهكذا يكون قد أصبح كل منهما مالكاً الآن لمفتاح رقمي مماثل لمفتاح صاحبه

ومصمّم على نحو لا يستطيع شخص آخر الوصول إلىٰ «م»، إلاّ إذا كان لديه أحد الأَرقام السرية الأصلية. والمتنصت لن تتوفر له، الفرصة لمعرفة الأَرقام السرية؛ ولن يملك ذاك الخصم إلاّ الصيغ المتغيرة التي يكاد يكون من المستحيل الاهتداء إليها.

لقد كانت خوارزمية ديفي ـ هيلمان أشد كفاءةوأ ماناً من نظام الأحجيات لميركل. لكن تلك الخوارزمية ظلّت دون التطبيق التام لذلك الطراز الذي كان يراود خيالهما من نظام المفتاح العام للشيفرة. ذلك أن ديفي وهيلمان لم يأخذا موضوع التوقيع الرقمي في حسبانهما، كما أنهما لم يوفرا الوسائل لتشفير الرسائل. إلاّ أن النظام الذي أتيا به، وفّر منهجاً يستطيع به من لم يسبق لهما التخاطب من قبل، استخدام قناة مفتوحة، ويحصلا على مفتاح سري. ويمكن استخدام هذا المفتاح في نظام تشفير تقليدي، مثل معيار تشفير البيانات لتعمية الرسائل، ثم تفكيك شيفرتها. (وأسلوب الخزان المزدوج هذا، طريقة للوصول إلىٰ مفتاح دون اتفاق مسبق، وطريقة أخرى للتواصل فيما بينهما سراً، عرف فيما بعد باسم «الهجين»).

وكان من شأن إدخالهما خوارزميتهماا لجديدة إلىٰ بحثهما «أساليب لعدة مستخدمين» بعد تنقيحه أن جعلت منه وثيقة أشد وقعاً من البحث ذاته في صيغته الأصلية. ثم قدّم البحث الجديد «اتجاهات جديدة في الكريبتوجرافيا» بتاريخ 3 حزيران/ يونيو 1976. وفي وقت لاحق من الشهر ذاته، عرضا بعض أفكارهما أمام مؤتمرين أحدهما في لينوكس‌بولاية ماساتشوسيتس والآخر في رونيبي في السويد، وقد قدر أن يكون لمشاركتهما عواقب لم يتعمداها، وتتصل بحقوق الملكية الفكرية. والحقّ، أن استغلال الملكية الفكرية كان آخر ما يخطر ببال هذين العالمين في حقل المعلوماتية. وعلى الرغم من العراقيل التي صادفاها بسبب رفض الحكومة توفير كافة التفاصيلا لمتعلقة بمعيار تشفير البيانات، كانا يعملان على ابتكار بديل علني كامل للكريبتوجرافيا ذاتها.

وفي تلك الأثناء، كان رالف ميركل، الذي بات الآن يتقدم في ادر سته، لنيل الدكتوراه في علما لكومبيوتر من جامعة كاليفورنيا في بيركلي، قد سلم أخيراً بأن مشروع الأحجيك ما زال بحاجة لكثير من الجهد. فبدأ عندئذ بالبحث عن منهج آخر لتنفيذ المفتاح العام. وقد عبّر عن هذا الوضع بقوله: «كان لدي خطط مختلفة تشتمل على دوائر وألعاب معقّدة، ومختلف أشكال المجموعات الجزئية». لكنها جميعاً لم تحقق له المطلوب. ومما زاد في عجزه الصعوبة المزمنة التي يعاني منها في التعبيربو ضوح عن الأفكار المعقّدة؛ وهذا ما جعل من العسير على زملائه الإشارة إليه بإجراء تعديلات على مشاريعه. وقد برّر ميركل ذلك في دفاعه بالقول: «إنك مضطر لأن تمد عقلك، فإذا بأمور غريبة عجيبة معقدة تداهمك أحياناً، ولا تستطيع عندئذ أن تعمل فيها تبسيطاً، إلاّ بعد أن تكون الفكرة قد نضجت، إلىٰ الحد الذي تصبح فيه نقية ويسهل عرضها بوضوح».

لبّى هيلمان عرض ميركل بالعمل معه، وقدّم له عملاً في البحث أثناء فصل الصيف. وإنه لأمر ينعش القلب أن يعمل المرء مع الشخصين الوحيدين في العالما للذين يدركان المشكلة على الوجه الأفضل. وقد وصف ميركل حاله يومذاك بقوله: «كنت منعزلاً حتّى التقيت هويت ومارتي. وكنت مستعداً لأن استمر فيا لضرب بقوة حتّى تتحقّق لي استجابة ما، إلاّ أنه لم يكن هناك من يهتم بمتابعة المشكلة». و لقد حل ميركل في ستانفورد وهو مقتنع بأن فكرته الواعدة تدور حولخطة للعثور على التوابع الوحيدة الاتجاه للباب السري لابا ستناد إلىٰ مسألة توابع إن بي الكاملة. وهذا النظام يقوم على مسألة رياضية تُعرف بالحقيبة Knapsack. ولاستيعاب هذه الخطة تدخل، حقيبة، وكما يقول ميركل: «إن أساس الفكرة. هي أن تضع الأشياء في الحقيبة، بحيث تمتلئ حتّى أطرافها دون زيادة أو نقصان». ووصف ديفي هذه المسألة بأنّها شبيهة بحالهو ظف الشحن الذي يجدأ ما مه مجموعة من الرزم المختلفة الأشكال

والأحجام ويضطر معها لإيجاد أفضل طريقة لإدخالها في حقيبة البريد. والحل المثالي هو الذي يسمح بحشو الرزم واستغلال كل بوصة من الفراغ. والحق أنَّه من الأصح القول، حسب خطة ميركل، أن على الموظف معرفة الترتيب المناسب لوضع الرزم. بحيث تتفق وحدود الوزن المسموح للحقيبة أن تستوعبه. وإذا كان عدد الرزم قليلاً، فلن يكون من الصعب التوصّل إلىٰ الحل المثالي، لكن المسألة تغدو أصعب إذا كان عددها كبيراً.

وبما أن ميركل أراد من هذه الحقائق تأدية دور الدالة الوحيدة الاتجاه للباب السري، وهذا أمر يسهل على الشخص المناسب حله، لكنَّه يكاد يكون من المستحيل على أي شخص آخر تفكيكه، فقد كان عليه إيجاد طريقة لتذليل هذه المعضلة لصاحب المفتاح الحقيقي. واستطاع تحقيق ذلك بواسطة شكل أسهل من مسألة الحقيبة هو الحقيبة المنتفخة. وفي هذه المسائل، يجري ترتيب الأوزان بشكل يجعل اكتشاف الحل ضرباً من التسلية. واكتشف ميركل طريقة تحول هذه العمليات السهلة إلىٰ مشكلة الحقيبة العادية الأشد تعقيداً، حيث يجري ترتيب الأوزان على نحو ليس فيه ذلك النوع من اليسر.

كانت تلك عملية معقَّدة، إلاَّ أنَّها منطقيَّة. وأساس ذلك أنَّه إذا أراد شخص ما أن يتلقَّى رسالة خاصة، فعليه البدء بحقيبته المنتفخة، وهي بالضرورة مفتاحه السري. ثم يكون له استخدام ذلك المفتاح لصنع الحقيبة العادية العسيرة على الحل لتكون المفتاح العام. واعتماداً على هذه الصيغة التي ابتكرها ميركل (وهو يعمل مع هيلمان) أمكن جعل الحقيبة الثانية تقوم بوظيفة تشفيرية بجعل الرسائل معماة على نحو لا يمكن إعادتها إلىٰ ترتيبها الأصلي إلاَّ على يد شخص لديه المقدرة على حل مشكلة تلك الحقيبة الثانية. وهذا يعني، عملياً، أن ثمة طريقة وحيدة لتنفيذ هذا الأمر، وهي استخدام المفتاح السري، وهو الحقيبة المنتفخة (اليسيرة على الحل).

أ ما الطريقة غير العمليّة فهي إنفاق بضعة مليارات من السنين في حل المشكلة بالهجوم بالقوة الغاشمة.

هل هناك طريقة ما للتغلّب على النّظام أكثر بساطة من استخدام الكومبيوتر ذات القدرات الفائقة في الهجوم الشامل بالقوة الغاشمة، بأمل الحصول على المفاتيح قبل انقضاء النهار؟ أو بعبارة أخرى هل يستطيع محلّلو الشيفرة أن يجدوا طريقاً مختصراً، أو ضعفاً يستغلونه للوصول إلى المفتاح السري؟ الحق أن ميركل كان شديد الثقة بأن النّظام خال من كل ضعف، وقد بلغت به الثقة أنّه علق على باب مكتبه إعلاناً. ثم كتب إلى هيلمان: «إني أعرض جائزة 100 دولار لأول شخص يتمكّن من اختراق النّظام. وقلما طلعت عليه بعض الأشخاص هنا، وخلصت بعد الإصغاء إلى الصمت، إلى أن الحل، إن وجد، هو على الأقل ليس بالبسيط الذي يُستهان به». وعمد، لتزويق الأمر، إلى تبسيط المهمة إلى حدّ عظيم بأن طلب إلى عدد من المعنيين بفك الشيفرة حل المعضلة بعد تخفيض مستوى صعوبة مسألة الحقيبة إلى الحد الذي كان ميركل يعلم معه أن ثمة، على الأقل، احتمالاً بعيداً بأن يتمكن شخص ما من الفوز بالجائزة. ثم يعمد بعد ذلك، إلى رفع قيمة الجائزة إذا استطاع أحد حل المسألة كما وضعها. ولكن ما حصل، على حد وصفه: «لم أجد أحداً يهتم بالموضوع. وقد حسبت أن المهتمين سيتدافعون إلى حل المشكلة إذا رضت مالاً للحقيبة [العصية على الحل، احتمالاً]، لأن الاحتمال قائم بأن يتمكن أحد من معالجتها فعلاً، أو يعتقد على الأقل، بأن ثمة احتمالاً بإمكانية حلها». (وقد وضع بحثاً مع هيلمان في عام 1978، حول نظرية الحقائب).

وفي تشرين الثاني/ نوفمبر، نشر بحث ديفي وهيلمان «اتجاهات جديدة في الكريبتوجرافيا» في مجلة آي إي إي إي IEEE وكان اكتشافاً، وضربة حقيقيّة تنزل بالإمبراطورية. (استوحى الكاتبان العنوان من جذور جيلهما، مستذكرين دار النشر التي تسمى الاتجاهات الجديدة والتي تصدر طبعات شعبية لكتب ذات

مستوى فكري رفيع، وتعتبر من الكتب المقدّسة عند أبناء جيل التمرد مثل «بانتظار جودو» و«سيد هارتا»). وقد استهل الكاتبان مقالهما بعبارة مدوية: «إننا نقف اليوم على عتبة ثورة جديدة في الكريبتوجرافيا». وآية ذلك أن عصر الكومبيوتر يسمح بتطبيقات زهيدة لتكاليف لأدوات التشفير، وهي أدوات ضرورية لعالم يقدم وسيلة «للاتّصال بين لناس أو بين أجهزة الكومبيوتر عبر العالم، لا تكلف جهداً وتتميّز برخص الثمن». لكن الكريبتوجرافيا التقليديّة لا تستطيع، بسبب مشكلة توزيع المفتاح، وعدم توفّر عنصر التوقيع الرقمي اللازم، أن تعالج هذه التحديات: «فاستخدامها سوف يكلف مستخدمي هذا المنهج من أسباب الضيق لشديد، ما يذهب بالكثير من فوائد المعالجة عن بُعد». وهكذا نرى أن ثمة حاجة لأمر جديد، وسيلة يمكن بها إجراء وتبادل المحادثات فعلاً بين أطراف ليس بينهم لقاء سابق، والتثبت من صحة التواقيع لتوثيق المخاطبة بين لمر سل والمتلقي، مع السماح بالتوقيع الرقمي. إن ديفي وهيلمان لم يكونا أول من عرض هذه المعضلات بصورة منهجية واضحة، من فوق المنابر وحسب، بل قاما أيضاً فيما بعد بعرض الحلول لها بواسطة المنهج الذي ابتدعاه، المفتاح العام لأنظمة الشيفرة.

ولقد راودت ديفي ذات يوم أحلام صورت له وضع مدونته عن الاكتشاف العظيم في لكريبتو جرافيا، لا في صورة البحث الأكاديمي، بل بشكل رواية جاسوسية. فلطالما خاب أمله في الكتب التي تنتمي إلى هذا النوع من الأدب، والذي يتضمن في حبكته اكتشافات تقنية ذات شأن، وكان مصدر خيبته افتقار تلك الروايات للإقناع عندتصو ير الفتوحات العلمية التي تعرض لها؛ فهي تقوم، حسب وصفه، على «أقدام من صلصال». ويتابع ملاحظاً: «وجدت نفسي لسوء الحظ، أني حين توفر لي الاكتشاف العلمي، لا أدري كيف أكتب رواية، وكان علي إقناع نفسي بالنشر في المجلات العلمية الاختصاصية، مثل كل إنسان آخر». ولكن حسبه من ذلك أن البحث الذي نشره مع مارتي هيلمان

كان مشوقاً كأي رواية من مستوى أكثر الكتب رواجاً على مدى الزمن. وكان هذا هو العلم الذي اخترق الحواجز التي لم تبلغها روايات الخيال العلمي، حتّى ذلك الحين؛ ففي صيغها الرياضيَّة كان مخطط الاتِّصالات في القرن الحادي والعشرين.

اختتم ديفي وهيلمان بحثهما بالملاحظة أنه طوال تاريخ الشيفرة كان الهواة هم غالباً الذين يأتون بالجديد في الكريبتو جرافيا. وذكر توماس جيفرسون الذي ظل ابتكاره لجهاز دولاب التشفير يستخدم طوال قرنين بعد ذلك، كما أنَّهما ذكرا الهواة الأربعة الذين خرجوا، كل على حدة، بتطبيقات الآ ت الإلكترونية الدوارة التي غلب طابعها على أجهزة الشيفرة من طراز إنجيما، أثناء الحرب العالمية الثانية. ثم أنهيا المقال بالتعبير عن أمنية بأن تكون جهودهما بداية مجهود يبذل لتغيير مشهدالكريبتو جرافيا الحديثة: «إننا نأمل بأن يلهم هذا آخرين (سوانا)، للعمل في هذا المجال الساحر الذي كانت المساهمة فيه تلقى الردع حتَّى الماضي القريب [تحت تأثير] احتكار الحكومة التام تقريباً».

ولقد تحطّم هذا الاحتكار على يدي متسلل سابق في معهد ما سا تشوسيتس ذي شعر طويل مسترسل ومستشاره ذي المزاج العاطفي، خريج جامعة ستانفورد.