عصر الحاسبات

اعتبرت آلة آلان تورنج التى استخدمها فى كسرة شفرة الانجما والتى سميت قنابل تورنج Turing Bombs بداية دخول التكنولوجيا فى مجال كسر الشفرة كما اعتبرت أول تمهيد لإنتاج الحاسبات الرقمية بمفهومها الحالى . وتلى هذه الآلة آلة أخرى أكثر تعقيداً أنشئها العلماء الإنجليز وأطلق عليها اسم Clossus واستخدمت فى كسر شفرة ألمانية خاصة جداً اسميتا شفرة لورنز Lorenz وكان هتلر يعتمد عليها فى تشفير الاتصالات بينه وبين جنرالاته .

وللأسف ولاعتبارات ضيقة الأفق تدعى الحفاظ على السرية تم تدمير هذه الآلة بعد الحرب ولم يبق لها أى أثرو مما أفقد الإنجليز سبقاً هاماً فى مجال إعداد الحاسبات الإلكترونية . واقتنص الأمريكيون الفرصة عندما تمكن عدد من علماء جامعة بنسلفانيا من بناء أول حاسب وأطلق اسم اياك ENIAC Electronic Numerical Integrator and Calculator وكانت أبحاث الشفرة صاحبة الفضل فى بناء هذا الحاسب .

ويبين المؤلف الفارق الضخم بين استخدام الحاسبات فى تركيب وتحليل الشفرة وبين الاعتماد على الأساليب اليدوية أو الميكانيكية وذلك فى النقاط الثلاثة الآتية :

١ – الشفرة اليدوية الميكانيكية محدودة بتصميم وبناء الآلة الميكانيكية مثل آلة الانجما وتعتمد قوتها على مكونات الآلة (عدد الخلاطات على سبيل المثال) فى حين أن استخدام الحاسب ليس له حدود ويمكن له أن يفترض عدد لا نهائى من مكونات النظام فإذا كانت الآلة الميكانيكية بها ٦ خلاطات على سبيل المثال يمكن لبرنامج الحاسب الإلكترونى أن يفترض وجود ٦٠ خلاط أو ٦٠٠ خلاط أو أكثر كما أنه يستطيع أن يعطى لهذه الخلاطات تصرفات متباينة تزيد بدرجة كبير من صعوبة الشفرة فبعض هذه الخلاطات يمكن أن يدور عكس عقارب الساعة والبعض الآخر مع عقارب الساعة وبعض الخلاطات يمكن أن يختفى بعد عشرة حروف مثلاً والبعض قد يدور بسرعة أكبر من غيره وهكذا وكل ذلك لا يتطلب إلا برنامج حاسب يتم إعداده ويحوى بداخله الأوامر التى تجعل الحاسب يتصرف كما يريد مصممى البرنامج .

٢ – الفارق الثانى هو فارق السرعة فمعروف أن سرعة الحاسبات تتفوق بكثير جداً عن سرعة الآلة الميكانيكية ومن ثم فإن الصعوبات التى قد يتعرض لها محللى الشفرية من مفاتيح شفرية ذات أرقام طويلة تتطلب عمليات حسابية مضنية وطويلة الأمد يمكن إجرائها بكفاءة بواسطة الحاسبات أحسن بكثير عن الآلات الميكانيكية .

٣ – الفارق الثالث هو أن الحاسبات بطبيعتها تتعامل مع أرقام فى حين أن الآلات الميكانيكية المستنبطة أساساً من تصميم الآلة الكاتبة تتعامل بالحروف وقد فتح ذلك آفاق واسعة فى مجال تركيب وتحليل الشفرة بالدخول فى استخدام المفاتيح الرقمية الأكثر صعوبة بدرجة كبيرة عن المفاتيح الشفرية الحرفية .

❁ ❁ ❁

وفى عقد الستينات بدأت الحاسبات تزداد قوة وفى نفس الوقت يزداد سعرها رخصاً وأصبحت بالتالى متاحة أكثر للاستخدام بواسطة قطاع الأعمال بالإضافة إلى عملائها التقليديين وهم الحكومات والقوات المسلحة وأجهزة الأمن وبدأ اهتمام قطاع الأعمال يزداد بشأن استخدام الأساليب الشفرية فى تأمين اتصالاته وتحويلاته المالية . وترتب على ذلك ظهور نوع جديد من المشاكل فى مجال علم الشفرة وهو الحاجة الملحة للأنماط Standards فمع تعدد النظم والاهتمامات وأساليب الشفرة كان هناك احتمال كبير لحدوث فوضى فى الاتصالات وقد دفع ذلك المكتب الأمريكى القومى للأنماط أن يعلن فى ١٥ مايو ١٩٧٣ عن طلب دراسة نمط شفرى للاتصالات .

وكان النظام الشفرى المرشح لتقديم هذا النمط هو النظام الذى أعدته شركة IBM للحاسبات واطلق عليه اسم Lucifer (ومعناه الشيطان) وكان العقل المفكر وراء هذا النظام هو العالم الأمريكى الألمانى الأصل هورست فيستل Horst feistel وقد اعتمد تصميم هذا النظام على أن يتم أولاً إدخال النص الواضح المراد تشفيره إلى ذاكرة الحاسب حيث يمثل داخلها بواسطة النظام الرقمى الثنائى Binary الذى تستخدمه الحاسبات أى أن يتكون من سلسلة من الأحاد والأصفار ثم يتم ثانياً إجراء عمليات تبادل معقدة بين أجزاء هذا النص وفقاً لترتيب معين مما يجعل الناتج النهائى (الذى هو أيضاً أحاد وأصفار) لا يمت بصلة للنص الواضح كما أنه مشفر بدرجة عالية الصعوبة ولا يمكن فكة إلا بإعادة عمليات الترتيب التى أجريت بطريقة عكسية واعتبر نظام Lucifer نظاماً قوياً بالفعل .

ولم يعجب ذلك وكالة الأمن القومى الأمريكى (National Security Agency) والتى يرمز لنا بالحروف الثلاثة NSA وهى الجهة المسئولة عن أمن الاتصالات فى الولايات المتحدة الأمريكية كما أنها الجهة المسئولة عن كسر شفرة اتصالات الغير والتنصت على محتويات هذه الاتصالات ويعنى وجود نظام شفرى قوى أن تتعرض مهام هذه الوكالة إلى عثرات وتزداد صعوبة تأديتها لمهامها .

ولم تحتمل هذه الوكالة احتمالية وجود اتصالات مدنية أو تجارية تتم ولا

تستطيع اختراقها وفك شفرتها . وتتردد آراء أن الوكالة تدخلت لدى هورست فيستل وفرضت عليه إضعاف عمليات التباديل التى يجريها النظام على النص الواضح بحيث يصبح عدد الاحتمالات التى يجب على كاسرى الشفرة بالوكالة التعامل معه لفك الشفرة لا يزيد عن مائة ألف مليون مليون احتمال (واحد وبجواره ٥٦ صفر) حيث رأت الوكالة أنها لديها الإمكانات التى تسمح لها التعامل مع هذا العدد وليس أكثر.

كما رأت أن هذا العدد يحقق أمنا كافيا للاتصالات المدنية والتجارية . وبعد إجراء التعديلات المطلوبة بواسطة NSA تم إعادة إشهار النظام فى ١٩٧٦/١١/٢٣ تحت اسم Data Encryption Standard ويشار إليه بالأحرف DES .

❁ ❁ ❁

وبعد هذا القدر من معالجة مشكلة الأنماط ظهر فى عالم الشفرة مشكلة أخرى أكثر صعوبة وهى مشكلة تبادل المفتاح الشفرى أو ما أطلق عليه اسم توزيع المفتاح Key distribution فإذا أراد طرفان إجراء اتصال شفرى مؤمن يجب أن يعلم الطرف المستقبل المفتاح الشفرى الذى اعتمد عليه الطرف الراسل فى تشفير رسالته لذا يجب عليهما الاعتماد على طرف ثالث لتوصيل هذا المفتاح وهذا يشكل نقطة ضعف جوهرية ويضعف بدرجة كبيرة مستوى تأمين هذا الاتصال . وقد ترتب على دراسة ومعالجة هذه المشكلة إنجازات هامة وعظيمة فى مجال علم الشفرة .

❁ ❁ ❁

مع بزوغ عصر الإنترنت والثورة الرقمية وازدياد استخدام الحاسبات الشخصية المرتبطة بالخطوط التليفونية فى تبادل الرسائل والمعلومات اتجه الناس إلى تشفير اتصالاتهم إلا أن هذا التشفير تطلب إيجاد وسائل آمنة لنقل مفاتيح الشفرة بين المرسلين والمستقبلين .

وقد كانت هذه القضية هى محور اللقاء بين ثلاثة علماء أمريكيين هم وايتفيير ديفى Whiotfield Diffie ومارتن هيلمان Martin Hellman ورالف ميركل Ralph Merkle .

وقد تركز بحثهم عن وسيلة علنية لتبادل مفاتيح الشفرة لا تؤثر على أمن الاتصال .

وكان المثال العملى الذى بدأوا به هو مثال الصندوق الخشبى فإذا أراد الطرف أ إرسال رسالة سرية إلى الطرف ب فإنه يضعها فى صندوق خشبى ويغلقه بقفل يملك مفتاحه فإذا وصل الصندوق إلى الطرف ب فإنه لن يستطيع فتحه ولكنه سيضيف قفل آخر عليه يملك هو مفتاحه ويعيد إرسال الصندوق إلى أ . وعند وصول

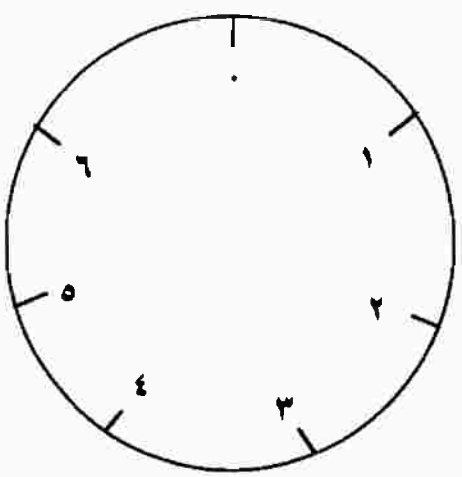
الصندوق إلى أ يقوم بإزالة قفله الأول ويعيد إرسال الصندوق إلى ب الذى سيكون باستطاعته فتحه فور استلامه لأنه يملك مفتاح القفل .

وعندما أرادوا تطبيق هذه الفكرة يرياضيا بنفس الطريقة وجدوا أن أ سيقوم بتشفير رسالته بمفتاح رقمى وعند وصول الرسالة إلى ب يقوم بتشفيرها هو الآخر بمفتاح رقمى وإعادتها إلى أ وهنا يجب على أ أن يزيل أثر مفتاحه الشفرى قبل إرسال الرسالة إلى ب مشفرة فقط بمفتاح ب الذى يملك بالفعل سره . وهنا ووجهوا بصعوبة كبيرة إذ يستحيل أن يفك أ مفتاحه الشفرى قبل أن يفك ب مفتاحه الشفرى لأن القانون الرياضى ينص على أن ما نفذ أولاً يفك أولاً وكان ترتيب التنفيذ كالتالى :

أ يشفر – ب يشفر – أ يفك – ب يفك ولكن ذلك يستحيل إذا أن الممكن رياضيا هو أ يشفر – ب يشفر – ب يفك – أ يفك . ولم يدخل اليأس فى نفوس العلماء الثلاثة وظلوا يبحثون حتى اهتدوا إلى أسلوب رياضى يسمى دالة الاتجاه الواحد One - way function .

فمن المعروف أن كافة الدوال الرياضية مزدوجة الاتجاه Two way function بمعنى أن نتيجة الدالة يمكن عكسها للوصول إلى بداية الدالة فإذا قلنا أن ٣س = ص وكانت س = ٢ فإن ص = ٩ فإذا علمنا ص فقط يمكن إرجاع الدالة إلى أصلها إذا علمنا س أيضاً .

ولكن دالة الاتجاه الواحد لا يمكن إرجاعها لأصلها وهى تعتمد على نوع من الحسابات يسمى «الحسابات طبقاً للنظام الرقمى» Modular Arithmetics فنحن نعرف النظام العشرى الذى يحوى الأرقام من صفر إلى ٩ ولكن يمكن استخدام نظم أخرى مثل النظام السباعى وأرقامه من صفر إلى ٦ ويتم بيانه طبقاً للشكل التالى :



فإذا قلنا ٢ + ٣ فإنها تساوى ٥

ولكـــن ٢ + ٦ تســـــاوى ١ (فى النظام السباعى) وبهذه الطريقة استنبط العلماء الثلاثة معادلة تعتمد على النظام الرقمى وهى :

$$Y^X \ (\text{mod } P)$$

يتم بمقتضاها تبادل المفتاح الشفرى بين الراسل والمستقبل دون مساس بسريته.

حيث Y رقم يتفق عليه بين الراسل والمستقبل

، X إجراء حساب للدالة

، mod P النظام الرقمى المتفقن عليه

ويتم تبادل المعلومات بين الراسل والمستقبل على خطوات خمسة كالمثال التالى وعلى أساس اتفاقهما بأن المعادلة هى $\text{س}^{\text{٧}} = (\text{mod})\ 11$

١ – يختار الراسل رقم وليكن ٣ ويبقيه سراً لديه ونرمز له بالرمز س .

وبالمثل يختار المستقبل رقمه وليكن ٦ .

ويبقيه سرى ويرمز له بالرمز ص .

٢ – يطبق الراسل المعادلة ذات الاتجاه الواحد .

$$\text{س}^{\text{٧}} = (\text{mod}_{١١}) = ٣٤٣\ (\text{mod}_{١١}) = ٢$$

وبالمثل يطبق المستقبل نفس المعادلة على رقمه

$$\text{ص}^{\text{٧}} = (\text{mod}_{١١}) = ١١٧٤٦٩\ (\text{mod}_{١١}) = ٤$$

٣ – يرسل الراسل نتيجة حسابه وهى ٢ إلى المستقبل ويستلم من المستقبل نتيجة حسابه وهى ٤ ويتم هذا الإرسال علنا إلا أن اختراقه أو التقاطه لا يعنى شىء بالنسبة للطرف القائم بالاختراق .

٤ – يطبق الراسل المعادلة على الرقم الذى ورد له من المستقبل وهو ٤ .

$$٤^{٣} = (\text{mod}_{١١}) = ٦٤\ (\text{mod}_{١١}) = ٩$$

٥ – الرقم ٩ هو المفتاح الشفرى الذى يستخدمه الراسل والمستقبل وتم تبادله فيما بينهما دون أى مساس بسريته .

وقد اعتبر إنجاز Diffie - Hellman - Merkle إعجازاً رياضياً وأثبت إمكانية نقل المفتاح الشفرى بأمان إلا أن تعدد الخطوات المطلوبة فى نقل المفتاح كان عائق بشكل صعوبة بالنسبة للحركة السريعة للمعاملات .

فتح إنجاز ديفى وزملائه الطريق للوصول إلى الحل الأمثل لمشكلة نقل المفتاح الشفرى والذى تمثل فى إعلان شفرة المفتاح العلنى Public Key cryptography وكان الفضل فى إنشائه فريق العلماء الثلاثى أيضاً رونالد ريفست Ronald Rivest وادى شامير Adi Shamir وليونارد أدلمان Leonard Adleman واشتهر بالأحرف الأولى من أسمائهم حيث سمى نظام RSA .

ويعتمد منطقه على أن يكون جزء من المفتاح الشفرى مذكور علنا فى دليل متاح لكافة المتعاملين ويسمى المفتاح العام Public Key فى حين يحتفظ كل فرد أو مؤسسة بالجزء الآخر من المفتاح والذى سيعتبر المفتاح الخاص Private Key .

فإذا أراد الراسل إرسال رسالة شفرة فإنه يبحث فى الدليل عن المفتاح العام للشخص الذى يريد مراسلته ويستخدم المفتاح العام فى تشفير الرسالة . ونظراً لأن هذا المفتاح العام سيستخدم فى دالة ذات اتجاه واحد فإنه من الصعب أن يتمكن أى فرد أوجهه من فك شفرته والوحيد الذى يستطيع فك شفرة الرسالة هو المرسل إليه من خلال استخدامه لمفتاحه الخاص فى عملية الفك .