شفرة الكوانتم

فى تصريح لوليام كرويل William Crowel نائب رئيس وكالات الأمن القومى الأمريكية NSA ... قال «إذا جمعنا كافة الحاسبات الشخصية فى العالم وعددها حوالى ٢٦٠ مليون حاسب وأعطيناها جميعاً تعليمات لكى تعمل على فك شفرة رسالة واحدة مشفرة بأسلوب PGP فإن الأمر سيتطلب مدة تعادل ١٢ مليون مرة من عمر الكون لفك شفرة الرسالة» .

ويعبر هذا التصريح على المستوى التكنولوجى العالمى جداً الذى وصلت له إمكانات التشفير ، إلا أنه معروف أن المعركة مستمرة ولن تتوقف بين واحد فى الشفرة وكاسرى الشفرة وكما سبق وقيل أن جدول فيجنير لا يمكن كسر شفرته وأن شفرة الانجما الألمانية مستحيلة الكشف ولكن تطور الأحداث أثبت خطأ هذه الأقوال فإن ما قاله نائب رءوس وكالة الأمن القومى الأمريكى لا يمكن أخذه كنهاية مؤكدة حاسمة لمعركة الشفرة .

ويحاول المؤلف فى هذا الفصل الأخير إلقاء الضوء على مستقبل علم الشفرة والإمكانات التكنولوجية التى لا تزال حتى الآن فى ظل البحث والتنقيب والتى يمكن أن تشكل ثورة قادمة فى هذا العلم .

❁ ❁ ❁

وقد أصبح من المؤكد أن شفرة RSA ذات المفتاح العام وشفرة PGP الأكثر عملية أصبحنا نظامين قويين يصعب اختراقهما إلا من الأبواب الخلفية التى تعتمدان هذين النظامين يحتاجان للحاسبات فى عملهما وبالتالى يمكن استغلال بعض الصفات فى تكنولوجيا الحاسبات التى تسمح بهذا الاختراق .

وأول هذه الصفات هى تلك التى يطلق عليها اسم Tempest وهو اصطلاح اتفق عليه عالميا يعبر عن التقاط الإشارات الكهرومغناطيسية الصادرة من أجهزة الحاسبات بطريقة تسمح بقرائتها فأى جهاز حاسب يشع أثناء تشغيله إشعاعات كهرومغناطيسية فى محيطه الغريب فإذا أمكن التقاطها على حاسب آخر أصبح من الممكن قرائتها وهى فى هذه الحالة ستكون فى صورة نصها الواضح أى قبل إجراء التشفير عليها بواسطة برامج الشفرة فى الحاسب الأصلى .

لذا تسعى بعض شركات الحاسبات وبإيعاز من الحكومة الأمريكية إلى إنتاج حاسبات إلكترونية لا تشع ولا يمكن شراء هذه الأجهزة إلا بتصريح خاص من الحكومة الأمريكية . ويعتمد مكتب التحقيقات الفدرالى FBI فى بعض أنشطة

جمع المعلومات على تتبع الإشعاعات الكهرومغناطيسية الصادرة من حاسبات الأهداف التى يتابعها هذا المكتب .

أما الصفة الثانية فى تكنولوجيا الحاسبات التى تسمح باختراق النظم الشفرية المعقدة فهى صفة فيروس الحاسب أو ما يطلق عليه اسم حصان طروادة Trojan horse وهو عبارة عن برنامج حاسب يخترق النظام بطريقة مستترة ويقبع بداخله ويقوم بإرسال البيانات التى يتعامل معها النظام إلى جهات أخرى على أن يتم هذا الإرسال قبل تشفير البيانات .

وقد استخدم هذا الأسلوب من أجهزة المخابرات وبالتعاون مع الشركات المنتجة لحاسبات الشفرة وهناك قضية مشهورة فى ١٩٩٨ عن شركة كريبتو السويسرية Crypto AG التى استطاعـات عمل مخرج خلفى لآلاتها الشفرية (Back obor) (وهو أحد صور حصان طروادة) وقامت بتسويق هذه الآلات المحسبة لبعض دول العالم الثالث ووفرت للحكومة الأمريكية طريقة الاستفادة من هذه الأبواب الخلفية وكنتيجة لذلك استطاعت الحكومة الأمريكية قراءة اتصالات هذه الدول بطريقة واضحة وقد أمكن بهذه الطريقة القبض على الأفراد الذين قاموا باغتيال شهبور باختيار رئيس وزراء إيران السابق فى منفاه . من خلال تتبع الاتصالات الإيرانية الرسمية حيث كانت إيران أحد الدول التى اشترت أجهزة سركة كريبتو السويسرية .

❁ ❁ ❁

ونصل أخيراً إلى عالم الكوانتم Quantom وتأثيره المتوقع على قدرات الشفرة تركيباً أو فكاً . والكوانتم هى كلمة لم تحظى بعد بترجمة عربية معبرة عن معناها إلا أنها تصف العلم أو المجال الذى يتعامل مع حركة وسلوكيات الأجزاءمن المادة المتناهية الصغر أو أجزاء ما دون الذرة .

ويرى البعض أن هذا العلم هو ضرب من الخيال يؤدى أحياناً إلى لوثات عقلية فى حين يرى البعض أنه علم حقيق وأنه يشمل بداخله ملامح ثورة علمية عظمى مستحدث فى المستقبل .

ومن الأفكار الغريبة فى هذا العلم فكرة «تعدد الأكوان» multiverse أو فكرة «التفسيرات متعددة العوالم» "many - worlds inter pretations" ومعناها أن الجزيئات ما دون الذرة (مثل فوتون الضوء مثلاً) تتحرك فى نفس اللحظة فى عدة ألوان أو عوالم وبالتالى إذا أمكن السيطرة على حركة هذه الأجزاء أو برمجتها فإنه من الممكن الحصول على سرعات عالية فى تنفيذ المهام الموكلة لهذه الجزيئات .

فإذا أمكن بناء حاسب كوانتم Quantom Computer يعمل طبقاً لهذه

الفلسفة فإن عنصر الزمن الطويل جداً الذى رد فى بيان هذا الفصل على لسان نائبر مدير وكالة الفضاء الأمريكية يمكن اختصاره بدرجة عالية للغاية . ويرى البعض أن الدولة التى ستصل أولاً إلى حاسب الكوانتم ستشكل تهديداً خطيراً لسائر الدول وتؤدى إلى عدم توازن خطير فى العلاقات الدولية .

والشىء المطمئن بالنسبة لنا كأحد دول العالم الثالث أن علم الكوانتم لا يزال فى مهدة وقد يكون ضرب من الخيال ... من يدرى ؟