خصوصية حسنة جداً

... أو (خ ح ج)

Pretty Good Privacy (PGP)

أدى التوسع فى استخدام النظام الشفرى RSA إلى ثورة فى الاتصالات الشفرية صاحبت ثورة المعلوماتية والتوسع فى استخدام الإنترنت والبريد الإلكترونى . وبقى عيب واحد فى نظام RSA يعوق التوسع فى استخدامه بشكل ملائم لاحتياجات قطاع الأعمال والمعاملات المدنية والتجارية وهو استهلاكه لوقت وموارد كبيرة نسبية عند فك شفرته لدى الجهة المستقبلة .

ويرجع ذلك إلى أن النظام يعتمد على نظرية الشفرة ذات الاتجاه الواحد أو بعبارة أخرى التى لا يمكن عكسها بنفس خطوات تركيبها للوصول إلى النص الواضح وتسمى هذه النظرية بالشفرية اللاسمترية asymmetric ويقابلها نظم التشفير التقليدية السيمترية symmetric .

وقد استطاع فيل زيمرمان Phil Zimmermann (العالم الأمريكى أيضاً) استنباط الحل العملى لهذه المعضلة بالنظام الذى أعطاه الاسم الوارد لهذا الفصل وهو اسم مستقى من قراءاته الأدبية .

وتبلورت فكرة زيمرمان ببساطة فى أن نظام RSA يعتبر نظام مثالى إلا أن المجهود الذى يبذله الطرف المستقبل يعين استخدام النظام لذا . وقد أبقى زيمرمان الجزء الخاص بالمفتاح العلمى لهذا النظام وأضاف نظام شفرى جديد سيمترى باسم IDEA وهو شبيه بالنظام المشهور DES السابق ذكره . وبالتالى يتم التراسل وفقاً للخطوات الآتية :

١ – يقوم الراسل بالتعرف على المفتاح العلنى لجهة الاستقبال ويستخدمه فى تشفير المفتاح الشفرى لنظام IDEA .

٢ – يقوم الراسل باستخدام المفتاح الشفرى لنظام IDEA فى تشفير النص الواضح لرسالته .

٣ – يقوم الراسل بإرسال شفرة النص الواضح وهى شفرة سيمترية وشفرة مفتاح IDEA وهى شفرة لا سيمترية .

٤ – لا تقوم جهة الاستقبال بالتعرف على مفتاح IDEA لأنه شفر بواسطة المفتاح العلنى لهذه الجهة .

٥ – بعد التعرف على المفتاح تقوم جهة الاستقبال بفك شفرة النص الواضح المشفر بطريقة سيمترية سهلة الفك ولا تحتاج إلى وقت مطول .

وقد قام زيمرمان بكتابة إجْراءات نظامه فى شكل برامج حاسب Softwar ووضعه على شبكة الإنترنت بحيث يكون متاح بسهولة لمن يرغب فى استخدامه . كما أضاف عليه بعض الأفكار الذكية التى تزيد من سهولة استخدامه دون أن تؤثر على مستوى آمنة فسمح للطرف الذى يريد إنشاء مفتاح شفرى لتشفير النص الواضح أن يحصل على هذا المفتاح بمجرد تحريك وحدة الفار المتصلة بالحاسب الشخصى تحريكا عشوائياً فى مختلف الاتجاهات ويترتب على هذا التحريك الحصول على قيمة رقمية للمفتاح الشفرى فريدة ولم يسبق استخدامها .

وقد آثار نظام PGP زوبعة فى الولايات المتحدة بسبب خشية الوكالات الأمريكية القومية المسئولة عن الأمن القومى من انتشار هذا النظام الشفرى فى المعاملات المحلية والدولية مما سيسبب لها إزعاج فى محاولة متابعة أى أطراف لها صلة إجرامية بالأحداث أو تنوى القيام بأعمال ذات طبيعة إجرامية .

وقد تعارض هذا الموقف مع الاتجاهات الداعية للحرية الفردية والحد من التدخل الحكومى فيما شكل مجابهة كبيرة فى بداية التسعينات .

وقد حاولت حكومة كلينتون فى ١٩٩٤ الوصول إلى حل وسط بإصدارها القانون المنظم للاتصالات الرقمية داخل الولايات المتحدة والذى سمى قانون شركة كليبر Clipper chip وبمقتضاه فإن أى جهة تريد تشفير اتصالاتها فإنها ستستخدم مفتاح شفرى يترتب فوراً على استخدامه أن يتم تسليم نصفه إلى أحد الوكالات الفدرالية والنصف الآخر إلى وكالة أخرى ويحفظ لدى الوكالتين بطريقة آمنة ولا يتم استخراجه منهما إلا بقرارات قضائية فى حالة الاحتياج إلى المفتاح لمتابعة تحقيقات إجرامية وسميت هذه الطريقة التى يتم فيها امتلاك المفتاح بشكل مشترك ومناصفة بين جهتين حكوميتين باسم المفتاح المملوك مناصفة Key escrow .

ولم يحظى هذا الإجراء بقبول واسع كما أنه كان متأخراً بسبب إتاحة نظام PGP على الإنترنت مما مكن كل من يرغب فى تشفير اتصالاته من إنزال نسخة من هذا النظام على الحاسب الخاص وقراءة تعليات استخدامه وتطبيقها بسهولة .

وتتواجد صفحة هذا النظام التى يمكن الحصول عليه منها على العنوان التالى :

http://www.pgpi.com