التشفير الكمي: عندما يكون مصدر التهديد هو نفسه مُؤمِّن الحماية – الجزء الأول

أخبار سارة لقراصنة البيانات:

ماذا لو أخبرتك أنني أملك آلة بمقدورها إيجاد العوامل الأولية لأعداد جد كبيرة؟ كيف ستكون ردة فعلك حينها؟ حتما لن تبالي لكلامي وهذا إن فهمت ما قصدته في الأصل، لكن خذها نصيحة مني: من الأفضل أن تنهض من مكانك حالا وتتجه مهرولا نحو أقرب وكالة بنكية وتسحب رصيدك المالي دون تردد. ربما ستسأل هنا: ولكن ما الدافع إلى القيام بذلك؟

نعم، سؤال وجيه، والإجابة: دعنا نفهم معا كيف تستطيع البنوك إبقاء مدخرات عملائها بعيدا عن أيدي المتطفلين.

حاليا، الطريقة المتداولة في حماية جميع المعاملات المالية تعتمد على ما يسمى بالتشفير باستخدام المفتاح المعلن (Public Key Cryptography) حيث يقوم المستخدم (البنك في حالتنا) بضرب عددين أوليين a وb فيما بينهما، فيكون الحاصل عددا c يطلق عليه اسم المفتاح المعلن، ويمكن لأي أحد معرفته، والذي سيقوم البنك بإرساله إليك بهدف استخدامه في تشفير بطاقتك البنكية مثلا، ومن ثم إعادة إرساله إليهم، دون أن يتمكن أي طرف ثالث من فك تشفيرها، مادام المفتاح السري (العددان الأوليان a وb) اللازم لذلك في حوزة وكالتك البنكية فقط.

يقصد بالعدد الأولي كل عدد صحيح طبيعي أكبر قطعا من 1، ولا يقبل القسمة إلا على نفسه وعلى العدد واحد. أما عملية إيجاد العوامل الأولية لعدد معين فيقصد بها تفكيك هذا العدد وكتابته على شكل جداء عوامل أولية، على سبيل المثال العددان 3 و5 هما العاملان الأوليان للعدد 15 (لأن: 3×5=15).

هنا ستتساءل، عزيزي القارئ: ماذا لو تمكن أحدهم من تخمين المفتاح السري؟ حسنا، هنا يكمن سر نجاعة العملية، فالطريقة الوحيدة المعروفة لإيجاد العاملين الأوليين لعدد كبير ما، هي تجريب جميع

الاحتمالات الممكنة، واحدة تلو الأخرى. وهو أمر غير وارد بالمرة، نظرا لأن الموارد الحاسوبية اللازمة لكسر أنظمة التشفير الحديثة تتعدى قدرة جميع الحواسيب التقليدية على هذا الكوكب متحدة فيما بينها، ولو استمرت في العمل آلاف السنين.

الآن وقد اتضحت الفكرة، قد تظن أنني أمازحك فقط بخصوص الآلة التي حدثتك عنها في الأول، مادامت غير ممكنة الوجود أصلا، لكن ليس بعد أن أخبرك أن مولودا / وحشا جديدا قادم في الطريق، إنه الحاسوب الكمي وقدرته الحاسوبية الهائلة التي ستمكنه من تجاوز أعقد خوارزميات التشفير خلال بضع ثوان، بتوظيف إحدى الخوارزميات التي ابتكرها بيتر شور، أستاذ الرياضيات التطبيقية بمعهد ماساشوستس للتكنولوجيا، سنة 1994.

إذًا، ما المعمول؟... لمعرفة ذلك أدعوك أن تكمل معنا الرحلة نحو الجزء الثاني من المقال.

المصادر: 1 2