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

أخبار سيئة لقراصنة البيانات

هذا المقال عبارة عن جزء من مقالتين حول موضوع التشفير الكمي، لذا أدعوك أن تلقي نظرة على ***الجزء الأول****، إن لم تفعل ذلك بعد، ليتيسر عليك فهم ما سنستعرض أسفله.*

من المؤكد أن فكرة التخلي عن الحساب البنكي وتحويل الأموال الخاصة إلى مكان سري آخر (ربما تحت قرميد وسط بهو المنزل) أمر في غاية الحماقة. لذا وجب التفكير في حل بديل، لكن المدهش أن مصدر التهديد ذاته، أي الفيزياء الكمية، هو المخلص. فإن أصبح التشفير باستخدام المفتاح المعلن غير مجد فلا تزال تقنية أخرى تسمى بالتشفير بالمفتاح المتناظر (**Secret Key Cryptography**) قادرة على الصمود.

فإن حدث أنك تريد إرسال كلمة المرور (**password**) سريا إلى صديق، وكلاكما يتوفر على نفس المفتاح السري، (**hmkqiwur**) مثلا، فكل ما عليك فعله هو تحويل حروف الرسالة السرية و المفتاح الى أرقام حسب العلاقة (**a=0 وb=1 وc=2 ...**) و بجمع العددين وإعادة تحويل العدد الناتج إلى كلمة حسب العلاقة السابقة ستحصل على الرسالة المشفرة (**wmcieklu**)، التي بمقدورك إرسالها عبر الإنترنت أو أية قناة إتصال غير آمنة أخرى دون خوف من أعين المتطفلين، باعتبار أن المفتاح السري اللاّزم لعكس العملية، وبالتالي استخراج الرسالة الأصلية لا يملكه إلا ذلك الصديق المعني.

مرة أخرى ستتوجه إلي مستغربا: لكن أين فيزياء الكم من كل هذا؟

ربما لم تنتبه إلى ذلك، فنجاح العملية رهين بتوفر كِلَا الطرفين على مفتاح سري خاص بهما تبادلاه في وقت سابق، أي أنه من اللاّزم وجود وسيلة آمنة للقيام بذلك في حالة ما إذا كان الطرفان بعيدين جغرافيا، وهنا بالضبط يمكن الاستعانة بميكانيكا الكم وقوانينها الغريبة لتحل لنا الإشكال.

باستعمال أحد البروتوكولات المعروفة باسم "التوزيع الكمي لمفتاح التشفير" (**quantum key distribution**)، والذي توظف فيه ظاهرة "التشابك الكمي" (**quantum entanglement**) التي تفيد بأن حالة الجسيمات الكمية، كالفوتونات مثلا، ترتبط فيما بينها بعلاقة معينة (لم يتمكن الفيزيائيون من تفيسرها بعد)، بحيث إن كان دوران الجسيم الأول عموديا فحتما سيكون دوران الثاني أفقيا، والعكس بالعكس. كذلك يوظف فيها مبدأ "هايزنبرغ للشك" (**Heisenberg's uncertainty principle**) الذي يقول باستحالة قياس حالة الفوتون دون التأثير عليه. وهكذا سنتمكن أخيرا من تبادل البيانات بشكل أكثر أمنا وأريحية.

ولتقريب سير العملية أكثر دعنا نفترض أن كلاً من (**Alice**) و (**Bob**) بحاجة إلى الاتفاق على مفتاح سري لتشفير مراسلاتهما دون أن تتمكن (Eve) من النجاح في الحصول عليه (الأسماء المستعملة هنا هي أسماء عشوائية ومتفق عليها لترميز أطراف العملية). كل ما عليهما فعله إذا هو اللجوء إلى مولد حزم من الليزر الذي سيرسل إلى كِلَا الطرفين أحد أزواج الفوتونات المتشابكة عبر شبكة ألياف بصرية، وبتحويل استقطاب الفوتونات المستقبلة إلى ترميز ثنائي ستكون النتيجة سلسلة من الأصفار والوحدات (**1111000001111000101010**) التي يمكن ترجمتها إلى كلمة معينة،و ستشكل المفتاح السري.

من جهة أخرى، وفي محاولة من (**Eve**) للحصول على المفتاح ستضطر إلى قياس استقطاب الفوتونات كذلك، مما سيخلف أثرا لها وذلك حسب مبدأ "هايزنبرغ" السابق وبالتالي سيخلص كل من (**Bob**) و (**Alice**) إلى وجود طرف خارجي يتعقبهما.

وبما أن المشاكل لا تنتهي أبدا في حقل العلوم، فإن التشفير الكمي لايخلو من عيوب بدوره، ولعل أبرزها المسافة المحدودة اللاّزم إحترامها عند إرسال الفوتونات، والتي في الغالب لايجب أن تتعدى بضع عشرات الكيلومترات. ويعزى ذلك إلى احتمال تغير استقطاب الفوتون، أو حتى فقدانه بالكامل نتيجة الاصطدامات المتتالية مع الجسيمات الأخرى على طول المسافة المقطوعة، وغالبا ما يلجأ إلى حل هذه المشكلة بإضافة مكررات متباعدة بشكل منتظم تساعد على تضخيم الإشارات الضوئية والحفاظ على العشوائية الكمية لآلاف الكيلومترات.

المراجع: 1 2