فك رموز نص مشفر بتقنية RSA

تعتبر خوارزميات التشفير بتقنية RSA من أكثر الطرق انتشارا على الشبكة العنكبوتية في إطار أمن المعلومات و المبادلات الإلكترونية. تم ابتكار هذه التقنية في عام 1977 و لازالت تستعمل لحماية المواقع الإلكترونية و الحواسيب و التحقق من هويتها. فعند اتصالك بموقع البنك مثلا أو موقع البريد الالكتروني، يتم تشفير المعلومات التي يتم تبادلها بين حاسوبك و تلك المواقع باستعمال خوارزميات RSA. و ترجع شهرة RSA إلى صعوبة اختراقها.

نظريا، بالإمكان اختراق هذا النوع من التشفير عبر تجريب جميع الكلمات الممكنة، إلا أن هذه العملية تحتاج إلى جهاز حاسوب جد قوي و عشرين قرنا من الحساب !

هل تجد هذا الأمر مطمئنا؟ كلا فدوام الحال من المحال. فقد تمكن فريق من الباحثين من ابتكار طريقة لاختراق تشفير RSA عبر الإنصات لأصوات المعالج عندما يعمل الحاسوب على فك تشفير معلومات مشفرة بهذه الطريقة. و تتم عملية الاختراق بوضع هاتف محمول بجانب الحاسوب و التقاط الأصوات الخفيفة التي يصدرها المعالج عندما يقوم بفك الشفرة. يمكن استبدال الهاتف بجهاز ميكروفون. و قد ابتكر هذه الطريقة فريق من الباحثين من ضمنهم أحد مخترعي التشفير بخوارزمية RSA. و المدهش في الطريقة التي ابتكرها هذا الفريق أن مدة الاختراق لا تفوق ساعة من الزمن !

المصدر :

1