



COMUNICATO 48

Comunicare sicuri con la crittografia quantistica

Artur Ekert è uno dei pionieri della crittografia quantistica: il nuovo sistema per codificare messaggi e renderli definitivamente sicuri non è più un miraggio, e al giorno d'oggi, con la giusta disponibilità economica, è possibile acquistare da un paio di ditte specializzate tutto il necessario per metterla in pratica. Ma la strada per arrivare fino a questo punto non è stata semplice, e il fisico polacco l'ha ripercorsa ieri in occasione del suo intervento al Festival della Scienza di Genova dal titolo ***Cifre, quanti e computer***.

«Oggi parlerò dell'affascinante rapporto fra la crittografia e la quantistica – spiega **Ekert** - ma non scenderò nei dettagli tecnici: voglio solo dare un'idea di come sia possibile scambiare informazioni fra due persone con la sicurezza di non essere intercettati». Protagonisti della storia sono i personaggi buoni Bob e Alice, e una biblica Eva pronta ad ascoltare le conversazioni private dei primi due. «Occorre fare un passo indietro – prosegue **Ekert** – e raccontare come l'avvento della scrittura abbia accompagnato l'evoluzione dell'uomo moderno; dai primi geroglifici egiziani si è passati all'alfabeto fenicio: un fatto fondamentale per la crittografia. Ancora oggi è estremamente delicato crittografare messaggi scritti in lingue, come il cinese, basate su ideogrammi anziché su lettere». Esistono due pilastri su cui si basa la crittografia tradizionale: la **permutazione** e la **sostituzione**. La prima nasce intorno al 400 a.C. e consiste semplicemente nel sostituire la posizione dei caratteri. A Giulio Cesare, invece, viene attribuito il primo utilizzo della seconda, che consiste nello spostamento delle lettere dell'alfabeto di un numero concordato di posti.

«Esiste però una percentuale di utilizzo delle singole lettere, ed è statisticamente possibile cercare di risalire al messaggio originale: tutte le lingue indoeuropee sono caratterizzate dall'utilizzo della *e*. Certo esistono messaggi particolari come i *lipogram*, che prevedono sistematicamente di non usare una lettera. **Georges Perec** scrisse un testo di 8.500 parole senza *e*, mentre **Gottlob Burmann** detestava a tal punto la *r* che parlò per 17 anni senza mai utilizzarla».

Dal congegno meccanico di Leon Battista Alberti (due dischi concentrici) alla celebre Enigma del novecento, passando per la macchina di Babbage, tutti i sistemi ideati per rendere sicure le comunicazioni sono stati sistematicamente violati. Al giorno d'oggi ci sono due possibilità, ma nel giro di qualche decennio resterà solo la crittografia quantistica.

“Attualmente si usano sistemi basati su due **chiavi, pubblica e privata**, correlate fra loro: la sicurezza è data dalla limitata capacità computativa a disposizione per riuscire a scoprire la chiave personale; **ma con strumenti adeguati sarebbe possibile violare anche questo sistema**”. Ecco la soluzione della crittografia quantistica: grazie alle proprietà quantistiche dei fotoni, permette di smascherare immediatamente un'eventuale Eva in ascolto, garantendo ad Alice e Bob la possibilità di adottare opportune contromisure.

Genova, 6 novembre 2006