

*All'Università di Camerino si sta sperimentando un nuovo sistema indecifrabile*

## **Comunicazioni criptate e inviolabili**

**Una prima prova pratica esterna all'Ateneo verrà effettuata a gennaio**

**CAMERINO** – Creare un sistema di comunicazione tra due soggetti in grado di risultare assolutamente indecifrabile a terzi potrebbe non essere più fantascienza.

All'Università di Camerino, infatti, è giunto nella fase sperimentale il progetto di "crittografia quantistica efficiente in condizioni non ottimali" che permetterà, appunto, di condividere chiavi segrete basandosi su principi fisici e non più su quelli matematici.

Un concetto difficile da spiegare, ma che potrebbe presto trovare applicazione nel vivere comune e segnare una svolta. Tutto è partito nel 2003, con un progetto del dipartimento di Fisica dell'Università di Camerino e l'allestimento di un laboratorio di ottica quantistica. "Si tratta di un progetto partito tre anni fa con fondi del Miure di cui è responsabile il professor Tombesi – ha spiegato il professor Gianni di Giuseppe del

dipartimento di fisica dell'Università di Camerino – La novità è che il sistema messo a punto qui si basa su principi della fisica e, quindi, sicurissimi. Molte delle applicazioni che prevedono uno scambio di dati e di cui si fa largo uso oggi, basti pensare ai bancomat o semplicemente agli acquisti in rete, sono fondati su complessi calcoli matematici. Si tratta di calcoli difficilissimi da risolvere, ma non impossibili, almeno a livello concettuale. Questo nuovo sistema, invece, è completamente inviolabile". In sostanza, saranno generate chiavi segrete per decifrare o cifrare messaggi. Chi si scambierà questi messaggi, dunque, potrà contare sull'assoluta certezza che tali chiavi non potranno mai essere conosciute da altri, soprattutto perché utilizzabili una sola volta.

E la dimostrazione non tarderà ad arrivare. E' prevista per gennaio, infatti, una

prima "prova all'esterno" dei risultati ottenuti dagli studiosi di Unicam. Presso il rettorato ed una delle sedi della Banca Popolare di Ancona saranno installate due apparecchiature sviluppate proprio nell'ambito del progetto e che si scambieranno tra loro le chiavi segrete per cifrare e decifrare messaggi. "Sono chiavi generate secondo leggi fisiche – ha spiegato il professor Tombesi, responsabile del progetto di crittografia quantistica – Ogni chiave potrà essere utilizzata una sola volta e, quindi, non c'è nessuna possibilità che altri soggetti, oltre i due che si scambiano il messaggio, riescano a decifrarlo. Comunque, quella di gennaio sarà solo una dimostrazione all'esterno, perché nei nostri laboratori tutto è già stato ampiamente testato". Tantissime, almeno stando alle premesse, le applicazioni che il nuovo sistema potrà trovare nel vivere quotidiano.