VareseNews

La matematica minaccia la sicurezza in Internet?

Pubblicato: Lunedì 4 Novembre 2002

È una di quelle scoperte che rivoluzioneranno il concetto di sicurezza nella Rete e che rappresentano un altro tassello nelle conquiste matematiche. Manindra Agrawal, matematico indiano ed insigne professor dell'Istituto di Tecnologia di Kanpur, ha risolto il problema di trovare in tempi accettabili un numero primo, cioè quel numero divisibile solo per se stesso o per uno (2,3,5,17 ecc, ecc). Era un problema che assillava i matematici di mezzo mondo e ora assillerà i navigatori di tutto il mondo. Già perché la difficoltà ad individuare i numeri primi di certe dimensioni era l'ostacolo principale che gli hacker dovevano affrontare per superare i sistemi di crittografia, che oggi rendono più sicure le comunicazioni nella Rete. I programmi di crittografia utilizzano, infatti, due grandi numeri primi moltiplicati tra di loro, difficili da identificare in tempi brevi. Il metodo individuato dal professor Agrawal velocizzerebbe questa identificazione e di conseguenza minaccerebbe la sicurezza delle transazioni in Internet. Il condizionale è d'obbligo perché la scoperta non scioglie un altro nodo importante: ovvero l'identificazione del moltiplicatore, anche se il passo sarà breve.

Una scoperta di grande valore, insomma. Tale era infatti la difficoltà di individuare grandi numeri primi, che chi (come è accaduto al giovane studioso canadese Michael Cameron , scopritore, il 14 novembre dello scorso anno, del 39mo numero primo di Mersenne*) vi fosse riuscito era sicuro di ritagliarsi una citazione nella storia della matematica. Il numero individuato dal ventenne Cameron possiede la bellezza di 4.053.946 cifre e per scriverlo occorrerebbero 2000 pagine scritte fittamente lasciando pochissimo spazio tra una cifra e l'altra.

***I numeri primi di Mersenne prendono il nome da padre Marin Mersenne (1588-1648), insigne studioso francese e amico dei grandi matematici del tempo, tra cui Descartes e Fermat.**

Redazione VareseNews
redazione@varesenews.it