THE INTEGER FACTORIZATION PROBLEM IN CRYPTOGRAPHY

Giordano Santilli

Università degli Studi di Trento

Modern public-key cryptography is often based on hard-to-solve mathematical problems. One of the most important and famous number-theoretic problems employed in this field is the Integer Factorization Problem (IFP): given an integer it is hard to recover in polynomial time its factorization. After a brief introduction on the problem, I will present some public-key cryptosystems whose security relies on the IFP. During the last part of the talk I will describe several factorization methods, possibly hinting at some advanced algorithms like the General Number Field Sieve.