Evento conoscitivo De Cifris
22 Gennaio 2018

Nadir Murru

Università di Torino, Dipartimento di Matematica G. Peano

Chi siamo

- Dott. Stefano Barbero – Università di Torino
- Prof. Danilo Bazzanella – Politecnico di Torino
- Prof. Umberto Cerruti – Università di Torino
- Dott. Nadir Murru – Università di Torino
- Prof. Lea Terracini – Università di Torino

Attività didattica

- Insegnamento *Codici Correttori e Crittografia*, Università di Torino, Corso di Laurea Triennale in Matematica
- Insegnamento *Algebra computazionale*, Università di Torino, Corso di Laurea Magistrale in Matematica
- Insegnamento *Introduzione alla crittografia*, Politecnico di Torino, Corso di Dottorato in Matematica Pura e Applicata
- Tesi di laurea triennale e magistrale

Attività/Competenze di ricerca

- **Frazioni continue**
  - Attacchi a RSA (Wiener), generazione di sequenze pseudocasuali
  - Frazioni continue multidimensionali (non ancora sfruttate in crittografia)
- **Successioni lineari ricorrenti**
  - LUC cryptosystem
  - Codici correttori (Stakhov 2006)

Attività/Competenze di ricerca

- **Polinomi di permutazione su campi finiti**
  - Schema di Dickson
  - Funzioni razionali di Rédei
- **Successioni di punti su curve**
  - Coniche (in particolare iperbole di Pell)
  - Schemi stile RSA
  - Pairing e isogenie

Attività/Competenze di ricerca

- Distribuzione di numeri primi
- Soft computing (reti neurali artificiali, algoritmi genetici, automi cellulari e logica fuzzy)
- Analisi di sengali (filtro di Kalman)