La *De Cifris* incontra Milano

Università degli Studi di Milano - Bicocca

11 Settembre 2018, Aula Massa, Edificio U6, quarto piano

http://www.decifris.it

Per ragioni organizzative, è richiesta l'iscrizione utilizzando questo link

L'incontro si propone di offrire una panoramica sulle attività di ricerca in Lombardia, riguardanti la Crittografia e le sue applicazioni. Sarà inoltre l'occasione per presentare l'Associazione Nazionale "*De Componendis Cifris*" che organizza l'evento.
L'iniziativa *De Cifris* di aggregazione delle competenze di Crittografia vuole stimolare la collaborazione in ambito crittografico, coinvolgendo sia le numerose eccellenze accademiche, che sono tuttora presenti in Italia, sia il mondo delle Aziende che operano nel settore.

Programma

10:30 – 10:50 Registrazione partecipanti

10:50 – 11:50 Sessione I
- 10.50 **Prof. Danilo Porro** – Università di Milano-Bicocca
  Pro-Rettore alla Valorizzazione della Ricerca
- 11.10 **Prof. Massimiliano Sala** – Università di Trento
  Acting Director dell'Associazione "De Componendis Cifris"
- 11.30 **Dott. Paolo Ciocca** – Consob
  Commissario della Commissione Nazionale per le Società e la Borsa

11:50 – 12:15 Break

12:15 – 13:00 Sessione II
- 12.15 **Prof. Alberto Leporati** – Università di Milano-Bicocca
  Blockchains, and the search for Cryptographic Boolean Functions
- 12.30 **Prof.ssa Francesca Dalla Volta** – Università di Milano-Bicocca
  Some Mathematical Topics in Symmetric Ciphers
- 12.45 **Dott. Tommaso Pellizzari, Dott. Simone Pintus** – Unicredit
  Blockchain Technology – Opportunità e rischi

13:00 – 13:45 Lunch break

13:45 – 15:00 Sessione III
- 13.45 **Dott. Andrea Visconti** – Università degli Studi di Milano
  Blockchain, White-box and High-speed Cryptography
- 14.00 **Dott. Ottavio Giulio Rizzo** – Università degli Studi di Milano
  Logaritmo discreto: perché è difficile attaccarlo?
- 14.15 **Prof. Gerardo Pelosi** – Politecnico di Milano
  Praticamente resistente: realizzare crittografia protetta da attacchi side-channel
- 14.30 **Dott. Alessandro Barenghi** – Politecnico di Milano
  Crittografia nell'era del calcolo quantistico: direzioni nella progettazione e realizzazione di crittosistemi
- 14.45 **Dott. Paolo Amato** – Micron Technology Inc.
  The Challenges of Memory and Storage Security

15:00 – 15:30 Coffee Break

15:30 – 16:45 Sessione IV
- 15.30 **Dott. Andrea Barri** – SAP
  Un caso d'uso: l'Intelligent Blockchain per le imprese visionarie
- 15:45 **Dott. Massimo Iaccarino** – Eurizon Asset Management
  Come utilizzare un DLT Private nei processi di riconciliazione di portafogli
- 16:00 **Dott. Hannes Eder** – Google Zurich
  High Availability in the Internal Google Key Management System (KMS)
- 16.15 **Dott.ssa Silvia Mella** – ST Microelectronics
  Security Challenges in the IoT
- 16.30 **Dott. Luigi Pugnetti** – Symbolic
  Network Security a 360°

16:45 – 17:30 Questions & Answers, Closing Remarks, Networking

Eventuali richieste possono essere inviate a: segreteria@decifris.it