De Cifris incontra Roma

Giornata di Studio sulla Crittografia

4 Ottobre 2018

Università Roma Tre

Aula Magna del Rettorato

Via Ostiense 159

Il giorno 4 ottobre 2018 si terrà a Roma il workshop organizzato dal Dipartimento di Matematica e Fisica dell'Università Roma Tre con il patrocinio della costituenda associazione nazionale di crittografia De Componendis Cifris.

Questo incontro è il terzo di una serie di eventi locali e si propone di offrire una panoramica sulle attività di ricerca a Roma e nel centro Italia, riguardanti la Crittografia e le sue applicazioni.

Sarà inoltre l'occasione per presentare l'Associazione Nazionale "De Componendis Cifris".

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.

10:30 – 11:00 *Registrazione partecipanti*

Sessione I

11:00 **Prof. Paolo Atzeni** – Università Roma Tre
Prorettore con delega per la didattica

11:15 **Prof. Massimiliano Sala** – De Componendis Cifris
Acting Director

11:30 **Dott.ssa Ebe Bultrini** – Banca d'Italia
Capo Dipartimento di Informatica

11:45 **Dott.ssa Nunzia Ciardi** – Polizia Postale
Direttore

12:00 – 12:15 *Coffee Break*

Sessione II

12:15 **Prof. Marco Pedicini** – Università Roma Tre
Cosa la crittografia può fare per la privacy nell'ambito dei big data

12:30 **Prof. Daniele Venturi** – Università di Roma La Sapienza
Codici non malleabili e applicazioni

12:45 **Dott. Marco Liverani** – NSR
Firma digitale: quanta complessità dietro ad un'operazione semplice

13:00 – 13:45 *Lunch*

Sessione III

13:45 **Paolo Menesatti** – CREA **Davide Del Vecchio** – Microsoft
Un esempio di applicazione blockchain per la tracciabilità elettronica del legno lungo tutta la sua filiera di trasformazione

14:00 **Dott. Daniele Campli e Prof.ssa Dajana Cassioli** – Università degli Studi dell'Aquila
NRoWE: a fair non-repudiation protocol harnessing extractable witness encryption

14:15 **Dott. Roberto Civino** – Università degli Studi dell'Aquila
Some group theoretical aspects of block cipher security

14:30 **Ing. Fabrizio Renzi** – IBM Italia **Dott.ssa Cecilia Boschini** – IBM Research, Zurich
The (post-quantum) future of data privacy

14:45 **Prof.ssa Marina Monsurrò** – RNTA – Università Europea di Roma
Una panoramica sulle attività della RNTA: promozione e diffusione della teoria dei numeri e della crittografia nei paesi in via di sviluppo

15:00 – 15:30 *Coffe Break*

Sessione IV

15:30 **Prof. Massimo Giulietti** – Università degli Studi di Perugia
Curve algebriche in crittografia

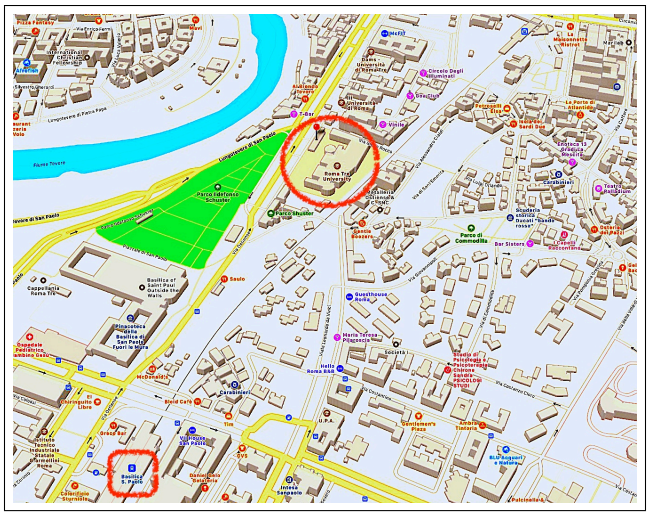
15:45 **Prof. Filippo Mignosi** – Università degli Studi dell'Aquila
La crittografia nella didattica dei corsi di teoria della complessità

16:00 **Ing. Sergio Civino** – Studio di Ingegneria Civino
Lo specialista d'informatica forense e l'hackeraggio etico

16:15 **Pasquale Racca e Claudio Rosati** – Armundia
Armundia e le ipotesi di impiego della blockchain nel mercato dell'intermediazione assicurativa e dell'advisory finanziario

16:30 **Sandro Fontana** – GT50
Problemi pratici nell'uso della blockchain nella notarizzazione documentale

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



Metro Linea B – San Paolo

Dipartimento di Matematica e Fisica
Università Roma Tre

Dipartimento di Informatica
Università degli Studi di Roma La Sapienza

Dipartimento di Matematica e Informatica
Università degli Studi di Perugia

De Componendis Cifris

Dipartimento di Ingegneria e Scienze dell'Informazione e Matematica
Università degli Studi dell'Aquila

Comitato Organizzatore:

Questo evento è stato coordinato a livello nazionale dall'*Acting Director* della De Componendis Cifris e a livello locale dal Comitato De Cifris, che è rappresentato da:

- **Prof. Riccardo Aragona** dell'Università dell'Aquila - Dipartimento di Ingegneria e Scienze dell'Informazione e Matematica
- **Prof. Marco Carli** dell'Università Roma Tre - Dipartimento di Ingegneria
- **Prof. Norberto Gavioli** dell'Università dell'Aquila - Dipartimento di Ingegneria e Scienze dell'Informazione e Matematica
- **Prof. Francesca Merola** dell'Università Roma Tre - Dipartimento di Matematica e Fisica
- **Prof. Francesco Pappalardi** dell'Università Roma Tre - Dipartimento di Matematica e Fisica
- **Prof. Marco Pedicini** (Chair) dell'Università Roma Tre - Dipartimento di Matematica e Fisica
- **Prof. Daniele Venturi** dell'Università di Roma La Sapienza - Dipartimento di Informatica