DE CIFRIS

Massimiliano Sala - Acting Director

De Cifris incontra Torino 14/10/2019

Massimiliano Sala?

- **Università degli Studi di Trento**
  Professore Ordinario di Algebra (**Crittografia**)
  Direttore del Laboratorio di Mat. Ind. e **Crittografia**
- **Iniziativa nazionale De Componendis Cifris**
  Acting Director
- **Fondazione Quadrans**
  Presidente del **Crypto Board**

De Componendis Cifris

www.decifris.it

La crittografia: un alone di mistero?

Sin dalla notte dei tempi, la **Crittografia** è stata usata per proteggere segreti militari e diplomatici.

Ma nessuno avrebbe potuto immaginare il numero **incredibile** di applicazioni che ha avuto negli ultimi decenni:

la firma digitale - gli acquisti online - il cloud cifrato -

la privacy nelle chat sugli smartphone - le **crittovalute**

Leon Battista Alberti : la scienza crittografica

Leon Battista Alberti (1404-1472) ha un'impostazione radicalmente **diversa** rispetto a quella **oscura** dei suoi predecessori. Pur lavorando per il Papato, scrive il

De Componendis Cifris (1466)

che è arrivato fino a noi è che viene considerato da molti la prima **importante** opera crittografica.

De Cifris: Chi siamo

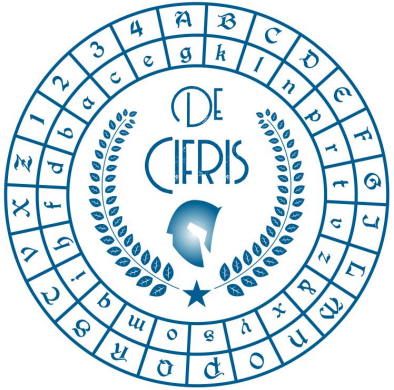
Al momento circa **800** membri:

1. accademia

   27 sedi universitarie/centri di ricerca
2. aziende

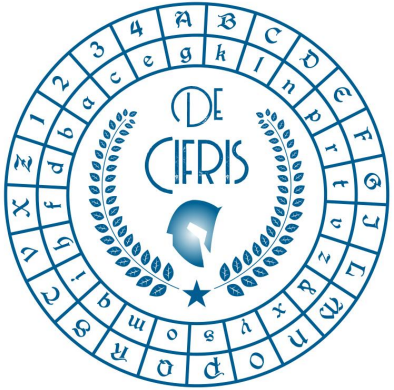
   250 iscritti
3. studenti

   oltre 300 (tutta Italia)



De Cifris: Organizzazione

Michele Elia (POLITO) Acting President
Massimiliano Sala Acting Director
Elisa Cermignani Assistente alla Dir/Pres



Comitato

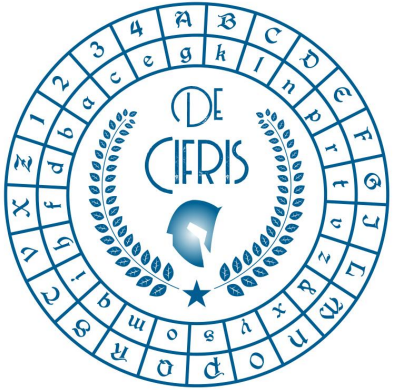
Marco Baldi (UNIVPM) - Massimo Giulietti (UNIPG)
Roberto La Scala (UNIBA) - Marco Pedicini (Roma3)
Andrea Visconti (UNIMI) - Ivan Visconti (UNISA)

De Cifris: Cosa vogliamo

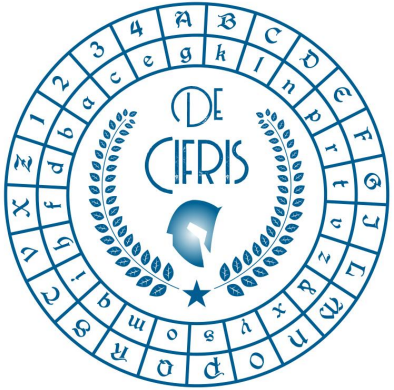
1. diffondere e divulgare
   la **Crittografia** è **affascinante**

2. ideare cifrari e sviluppare algoritmi
   la **Crittografia** è **utile**

3. aggregare la comunità crittografica
   la **Crittografia** è **partecipativa**



Piano nazionale per la protezione cibernetica e la sicurezza informatica (31/05/2017)



Il piano prevede un **Centro nazionale di crittografia**,

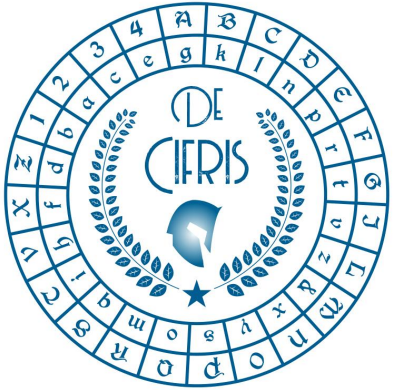
1. progettazione di **cifrari**
2. realizzazione di un **algoritmo nazionale**
3. realizzazione di una **blockchain nazionale**
4. esecuzione di valutazioni di **sicurezza**

De Componendis Cifris

COSA FACCIAMO??

De Cifris: Convegni (I)

1. Preparatori:
   a. Roma (CNEL) ottobre 2017
   b. streaming gennaio 2018



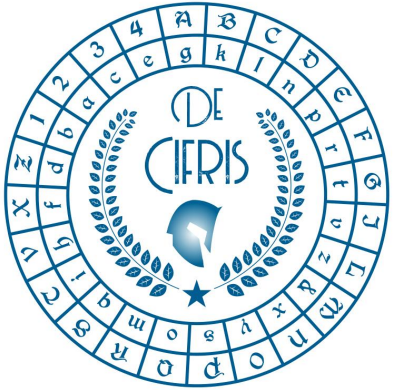
2. Eventi territoriali:

   2018 : Salerno -- Milano -- Roma

   2019 : Torino (oggi) -- Perugia (dopodomani)

De Cifris: Convegni (II)

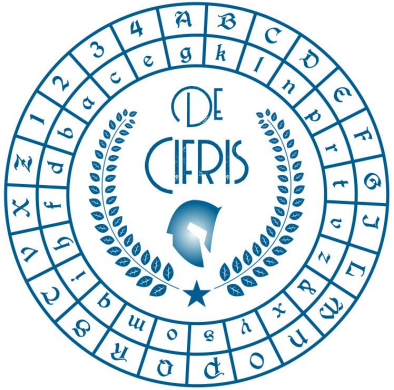
Eventi tematici:



- **2018**
  a. postquantum (presso ITASEC18)
  b. CifrisChain (blockchain)

- **2019**
  a. Crittografia (con AFCEA)
  b. PQCifris (postquantum, maggio 2019)
  c. CifrisChain (blockchain, maggio 2019)

CifrisChain



1. Gruppo tematico su BLOCKCHAIN
   oltre 80 iscritti

2. Coordinato da Ivan Visconti (UNISA)

3. Secondo workshop **maggio 2019** (Roma-**Consob**)

PQCifris

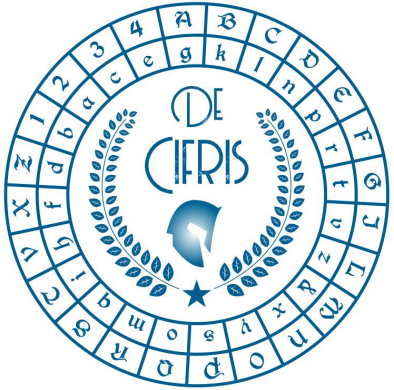
1. Gruppo tematico su POSTQUANTUM
   oltre 40 iscritti

2. Coordinato da Marco Baldi (UNIVPM)

3. Primo workshop maggio **2019**

Altri gruppi tematici

Potremmo attivare altri gruppi tematici:



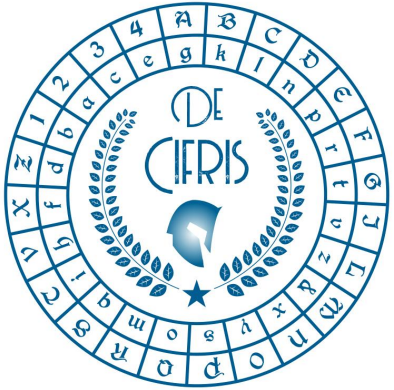
1. **CifrisCloud**
   per lavorare sulla Cloud Encryption

2. **QuantumCifris**
   per lavorare sulla Crittografia Quantistica

De Cifris: divulgazione (I)

1. Mailing list

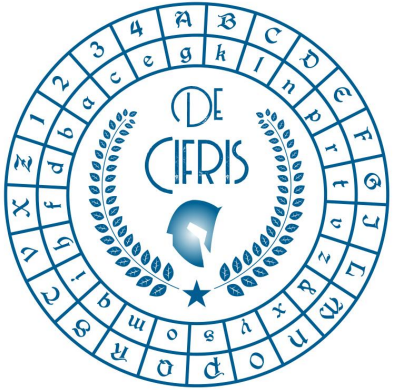
2. Il libro delle 100 tesi:
   riassunti di 100 tesi di **Crittografia**



3. Gare di crittografie/hackaton:
   a. **Cryptowars2018**
   b. **Hackaton** a settembre 2019 su **crittovalute**
   c. **Cryptowars2019** (settimana prossima)

De Cifris: divulgazione (II)

Cicli di seminari gestiti da gruppi locali (2019)



1. **De Cifris Athesis** (Trento)
2. **De Cifris Augustae Taurinorum** (Torino)
3. **De Cifris Schola Latina** (Roma-L'Aquila)

4. De Cifris Mediolanum ??

De Componendis Cifris

COSA OFFRIAMO??

De Cifris: per gli Studenti

1. Informazione:
   corsi, percorsi, tesi

2. Mondo del lavoro:
   stage e tirocini -- Massimo Giulietti UNIPG

3. Borse di studio:
   per seguire percorsi di studio specifici
   (borse Advisory Board -> Marco Pedicini UNIRM3)

De Cifris: per i Ricercatori

1. Informazione
2. Coinvolgimento in bandi/proposte/progetti
3. Pubblicazioni scientifiche
   (Collectio Cifris - 2020)

De Cifris: per le Aziende

1. Formazione qualificata
   (Advisory Board -> Marco Pedicini)

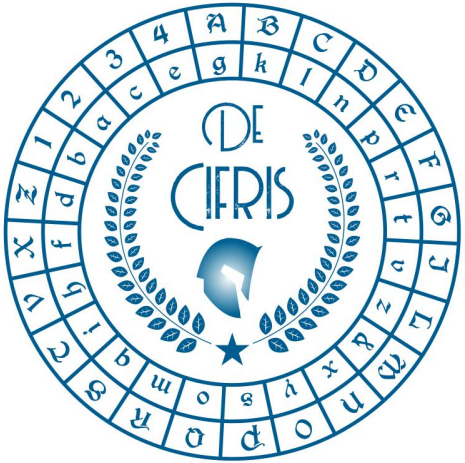
2. Coinvolgimento in bandi/proposte/progetti

3. Mappatura delle competenze
   (tirocinanti)

De Cifris: per la Pubblica Amministrazione

1. Formazione qualificata
2. Mappatura delle competenze
3. Ricerca **nazionale** di alto livello e **affidabile**

De Componendis Cifris



NEXT ?

Conclusioni

Polybius (circa 145 a.C.)

*The order of battle used by the Roman army is very difficult to break through, since it allows **every man** to fight both **individually** and **collectively**.*

*It is impossible to agree beforehand about things of which one **cannot be aware** before they happen.*

De Componendis Cifris

www.decifris.it