DE CIFRIS

Massimiliano Sala - Acting Director

LA DE CIFRIS INCONTRA ROMA 04/10/2018

Massimiliano Sala?

Università degli Studi di Trento

- Professore Ordinario di Algebra (**Crittografia**)
- Direttore del **CryptoLabTN**
  Laboratorio di Matematica Industriale e **Crittografia**

Associazione Crittografia De Componendis Cifris

- Acting Director

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

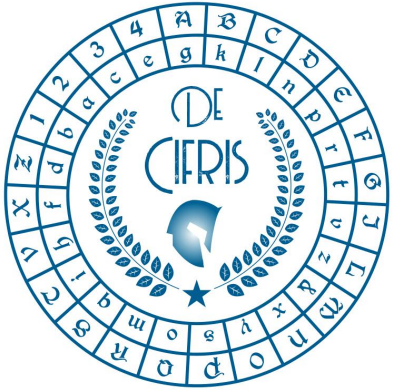
Al momento circa **500** membri:

1. accademia

   21 sedi universitarie/centri di ricerca
2. aziende

   140 iscritti
3. studenti

   un centinaio (tutta Italia)

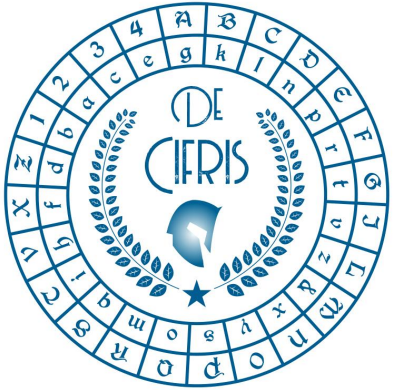


De Cifris: Cosa vogliamo

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**



De Componendis Cifris

COSA FACCIAMO??

De Cifris: Convegni

1. Preparatori: ottobre 2017 e gennaio 2018

2. Eventi tematici: febbraio 2018
   postquantum a ITASEC18
   (collaborazione con i colleghi **Cyber!!**)

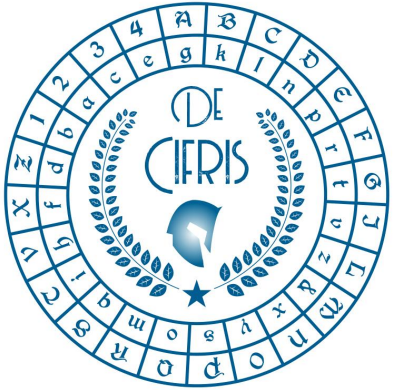
3. Eventi territoriali: Salerno maggio 2018,
   Milano settembre 2018, Roma ottobre 2018

De Cifris: divulgazione

1. Mailing list

2. Il libro delle 100 tesi:
   pubblichiamo riassunti di <u>100 tesi</u>
   di **Crittografia** degli ultimi 10 anni

3. Piccoli eventi locali



De Cifris: ricerca e progetti

1. Bandi pubblici:
   costituzione di tre gruppi per PRIN 2017

2. Richieste/proposte:
   come Associazione abbiamo ricevuto un paio di **richieste** da parte di enti/grandi aziende e stiamo predisponendo le nostre **proposte**

De Componendis Cifris

COSA OFFRIAMO??

De Cifris: per gli Studenti

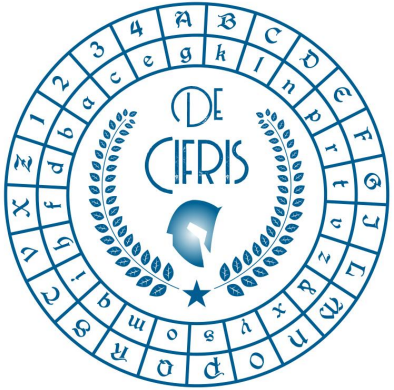
1. Informazione:
   corsi, percorsi, tesi

2. Borse di studio:
   per seguire percorsi di studio specifici

3. Piccoli finanziamenti di ricerca:
   ad esempio per seguire un convegno estero

De Cifris: per i Ricercatori

1. Informazione
2. Coinvolgimento in bandi/proposte/progetti
3. Pubblicazioni scientifiche



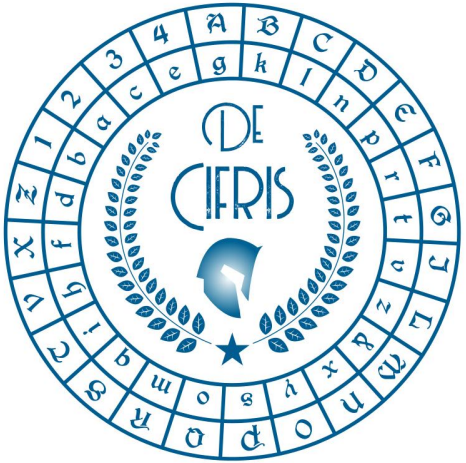
De Cifris: per le Aziende

1. Formazione qualificata
2. Coinvolgimento in bandi/proposte/progetti
3. Mappatura delle competenze

De Cifris: per la Pubblica Amministrazione

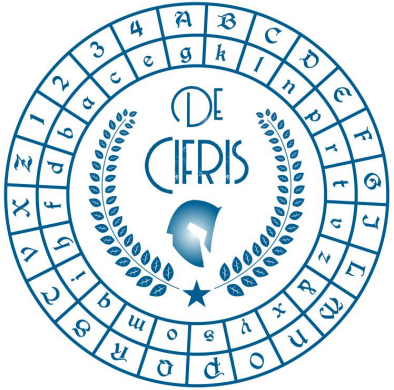
1. Formazione qualificata
2. Mappatura delle competenze
3. Ricerca **nazionale** di alto livello e **affidabile**

De Componendis Cifris



NEXT

CifrisChain



1. Gruppo tematico su BLOCKCHAIN
   oltre 50 iscritti

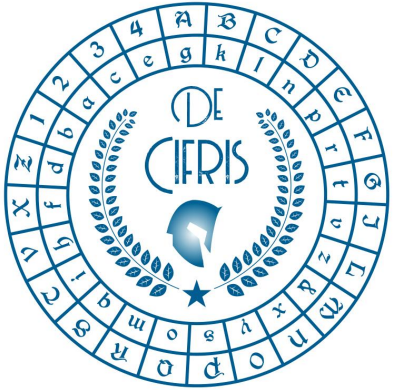
2. Coordinato da Ivan Visconti (UNISA)

3. Primo workshop specifico il **17 dicembre 2018** (Roma)

CryptoWars 2018

1. Gara di *Crittografia* a squadre, aperta a tutti gli studenti delle Università

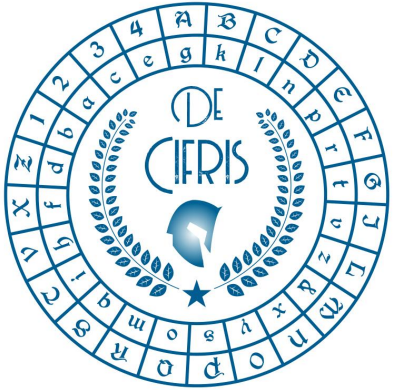
2. Coordinata da Andrea Visconti (UNIMI)



3. Dura una settimana: **la prossima** dal 15 al 21 ottobre!
   www.decifris.it/cryptowars2018.html

Nuovi gruppi tematici

Nel 2019 attiveremo:



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

2. **CifrisPQuantum**
   per lavorare sulla PostQuantum Encryption

Conclusioni: **Polybius**

*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