il Consiglio Nazionale delle Ricerche

Istituto per le applicazioni del Calcolo "M. Picone"

in collaborazione con l'Associazione Culturale "Confine Mondo"

Tranquilli, crittografiamo

LA MATEMATICA E GLI ALGORITMI PER LA SICUREZZA INFORMATICA

Stage digitale 27 febbraio – 24 aprile 2021

Con questo stage faremo un viaggetto attraverso **Euclide**, **Fermat**, **Eulero** e **Galois** per arrivare fino alle Fiandre alla scoperta di "**Rijndael**", l'algoritmo standard di cifratura simmetrica (**Advanced Encryption Standard**). Per strada scopriremo che il massimo comune divisore, i numeri primi e i polinomi non sono necessariamente strumenti di tortura ma anche formidabili alleati per tenere al sicuro i nostri dati (comprese chat turpiloquenti in cui si dice peste e corna di un corso come questo). Se saremo stati bravi, dopo aver addomesticato Python, potremmo addirittura crittare gli improperi contro i docenti del corso: paradossalmente sarebbe un successo.

Docenti:

Nicola Apollonio, IAC-CNR, Fabrizio d'Amore, Università di Roma "La Sapienza", Paolo G. Franciosa, Università di Roma "La Sapienza".

27 FEBBRAIO H 15-18
Sicurezza informatica: un aperitivo

28 FEBBRAIO H 15-18
Le basi: Aritmetica e crittografia

6 MARZO H 15-18
Esercizi e approfondimenti

13 MARZO H 15-18
I ferri del mestiere, coding I - Python variabili, assegnazione, espressione, if

20 MARZO H 15-18
I ferri del mestiere, coding II - Python liste, cicli, funzioni, I/O

27 MARZO H 15-18
"Amici e nemici" algoritmi e complessità computazionale primalità, regola di Horner

10 APRILE H 15-18
Ricorsione: (amici) MCD, sorting

17 APRILE H 15-18
Quasi ad AES, Advanced encription system identità di Bézout, l'algoritmo AES: primitive

24 APRILE H 15-18
Ad AES - crittate!

Consiglio Nazionale delle Ricerche

Associazione Confine Mondo

PER INFORMAZIONI ED ISCRIZIONI SCRIVERE A info@confinemondo.com