

Prot. 1619/2025

Pos. VII/16/ff

Roma, 31/10/2025

A tutti gli interessati

*Oggetto: Ricognizione interna per attivazione di incarico di collaborazione (mansioni esigibili da personale tecnico-amministrativo dell'Ateneo)*

Conformemente a quanto previsto dall'art. 7 del D. Lgs. 165/2001 il Dipartimento di Matematica e Fisica indice la presente ricognizione volta a verificare l'eventuale possibilità di utilizzare risorse interne dell'Ateneo per la seguente collaborazione.

Oggetto della prestazione:

Incarico di prestazione occasionale per attività di supporto tecnico-scientifico, finalizzate alla stesura e organizzazione di materiale tecnico sugli algoritmi di crittoanalisi applicati a sistemi di cifratura simmetrica, relativamente al progetto PNRR BAC SERICS Aqusdit, con particolare riferimento alle seguenti attività:

- **Analisi e sistematizzazione della letteratura tecnico-scientifica** relativa ai principali algoritmi di crittoanalisi utilizzati contro cifrari simmetrici, sia a blocchi (es. AES, DES) sia a flusso.
- **Redazione di schede tecniche e documentazione** sui principali metodi di attacco (es. attacchi differenziali, lineari, algebrici, boomerang, biclique, statistici), con particolare attenzione all'inquadramento teorico e all'efficacia pratica.
- **Sviluppo di esempi pratici e prototipi dimostrativi** mediante l'utilizzo dei seguenti strumenti software:
  - **Python** per scripting, simulazioni e automatizzazione di attacchi su cifrari simmetrici.
  - **SageMath** (con particolare riferimento alla libreria ClaaSP) per la modellazione simbolica e lo studio algebrico delle strutture interne dei cifrari.
  - **C++** per l'implementazione ad alte prestazioni di porzioni critiche di codice, in particolare per algoritmi di cifratura o crittoanalisi a basso live
- **Collaborazione alla preparazione di materiale tecnico**, tra cui:
  - documentazione interna al gruppo di ricerca;
  - supporto alla scrittura di dispense, appendici tecniche o fascicoli destinati alla divulgazione o alla pubblicazione.
- **Verifica della correttezza concettuale e computazionale** del materiale prodotto, con attenzione alla coerenza con i modelli crittografici di riferimento.

Il collaboratore dovrà possedere le seguenti caratteristiche curriculari:

- 1) Laurea Magistrale in Matematica o titolo di studio equiparato o equipollente;
- 2) comprovata competenza ed esperienza documentata nelle seguenti aree:
  - **Solida conoscenza della crittografia simmetrica**, incluse le strutture dei cifrari a blocchi e a flusso, i modi operativi, le funzioni di round e la generazione delle chiavi.
  - **Conoscenza approfondita delle principali tecniche di crittoanalisi**, con capacità di applicarle a casi studio concreti.
  - **Esperienza nell'uso dei linguaggi e ambienti richiesti**, in particolare:
    - **C++** per l'implementazione efficiente di algoritmi crittografici;
    - **Python** per scripting, simulazioni e automazione di test;

- **SageMath/Claasp** per l'analisi simbolica e la modellazione algebrica di cifrari.
- **Capacità di sintesi e redazione tecnica**, con produzione autonoma di documentazione rigorosa e leggibile.
- **Familiarità con strumenti di versionamento del codice** (es. Git) e buone pratiche di documentazione del software.

Il presente avviso è rivolto a tutto il personale in servizio presso l'Università Roma Tre. La prestazione avverrà durante l'orario di servizio e pertanto sarà a titolo gratuito.

I soggetti interessati sono pertanto invitati a segnalare eventuali disponibilità a svolgere la prestazione sopraindicata all'indirizzo Pec: [matematicafisica@ateneo.uniroma3.it](mailto:matematicafisica@ateneo.uniroma3.it) entro le ore 12:00 del quindicesimo giorno successivo alla data di pubblicazione della presente, allegando il proprio curriculum vitae firmato ed il parere favorevole del responsabile della struttura di appartenenza.

La valutazione di idoneità sarà basata sui titoli e sulle competenze possedute come descritte nel curriculum vitae e verrà effettuata da un'apposita commissione.

In assenza di riscontro si considererà tale silenzio quale indicazione della mancanza di personale idoneo a ricoprire l'incarico.

F.to      Il Direttore del Dipartimento  
Prof. Pietro Caputo

Il presente documento, firmato in originale, è conservato negli archivi del Dipartimento di Matematica e Fisica.