

Prot. 1620/2025

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 sulle tecniche di apprendimento automatico per l'analisi e la compromissione di sistemi crittografici simmetrici e, eventualmente, anche di schemi post-quantistici, relativamente al progetto PNRR BAC SERICS Aqusdit, con particolare riferimento alle seguenti attività:

- **Studio e sistematizzazione della letteratura** inerente l'uso del machine learning (supervisionato, non supervisionato e deep learning) applicato alla crittoanalisi di cifrari simmetrici, stream cipher, block cipher, lightweight crypto, e costrutti correlati.
- **Progettazione e sviluppo di dataset artificiali** per l'addestramento e la validazione di modelli ML volti a riconoscere schemi strutturali e vulnerabilità nei cifrari.
- **Sviluppo di modelli di apprendimento automatico** finalizzati a:
 - predire bit di chiave o pattern interni nei round dei cifrari;
 - riconoscere tracce residue nei ciphertext;
 - identificare correlazioni non evidenti nei dati criptati.
- **Utilizzo di ambienti software e librerie specifiche** per il machine learning applicato a contesti crittografici.
- **Supporto alla redazione di materiale tecnico**, tra cui schede descrittive dei modelli, risultati sperimentali, script e documentazione per l'utilizzo dei tool sviluppati.

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:
 - **Crittografia simmetrica e crittoanalisi**: conoscenza dei principali algoritmi a blocchi e a flusso, e delle tecniche base di attacco.
 - **Machine Learning**: comprensione dei concetti fondamentali (reti neurali, SVM, decision tree, CNN, RNN, ecc.) e capacità di progettare esperimenti di addestramento e testing.
 - **Esperienza con strumenti e librerie software**:
 - **Python** come linguaggio principale;
 - **Scikit-learn, TensorFlow o PyTorch** per la modellazione ML;
 - **NumPy, Pandas, Matplotlib** per la gestione dei dati e la visualizzazione dei risultati;
 - opzionalmente: **SageMath/CLaaSP** per componenti simboliche, o **C++** per implementazioni a basso livello.
 - **Abilità nella creazione e gestione di dataset artificiali**, anche tramite simulazioni crittografiche o generazione casuale controllata.

- **Capacità redazionale e scientifica**, necessaria per produrre documentazione tecnica chiara, rigorosa e riproducibile.
- **Conoscenza di base degli strumenti di versionamento** (es. Git) per la gestione collaborativa del codice.

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 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.