UNIVERSITÀ DEGLI STUDI DI MILANO

Per incarichi inferiori a 5.000 Euro

Codice selezione 04/2025

AVVISO PUBBLICO PER PROCEDURA DI INCARICHI DI COLLABORAZIONE *PER ATTIVITÀ DI* SUPPORTO ALLA RICERCA NELL'AMBITO DEL PROGETTO "TOWARDS FULLY AUTOMATIC SEARCH OF CRYPTOGRAPHIC TRAILS"

IL DIRETTORE

Vista	la Legge n. 168/1989;
Visto	l'art. 7 comma 6 del Decreto Legislativo 30 marzo 2001, n. 165, e ss.mm.ii.;
Visto	l'articolo 81 comma 2 del "Regolamento d'Ateneo per l'Amministrazione, la Finanza e la Contabilità" dell'Università degli Studi di Milano;
Visto	il "Regolamento per l'affidamento a terzi estranei all'Università di incarichi di carattere intellettuale";
Vista	la determina del Direttore del Dipartimento del 14 aprile 2025 protocollo no. 0015067 del 14 aprile 2025;
Considerato	che in data 27 marzo 2025 con avviso prot. n. 0012600 del 27 marzo 2025 il Direttore del Dipartimento di Informatica "Giovanni Degli Antoni" Prof. Danilo Mauro Bruschi ha emesso un avviso interno volto a reperire una/più professionalità per ricoprire l'incarico/gli incarichi di cui al presente avviso pubblico;
Verificato	che non è stato possibile reperire nessuna unità di personale interno per eseguire la prestazione oggetto di tale avviso;
Vista	l'autorizzazione presentata dalla/dal Responsabile della struttura per l'emissione dell'Avviso pubblico volto al conferimento a soggetti esterni all'Ateneo di incarichi di collaborazione a norma del Regolamento;

DETERMINA

È indetta una procedura di valutazione per il conferimento di n.2 incarichi di collaborazione a favore del Dipartimento di Informatica "Giovanni Degli Antoni" per l'attività di supporto alla ricerca, da svolgersi sotto la guida del Prof.Andrea Visconti nell'ambito del Progetto "Towards fully automatic search of cryptographic trails" – codice identificativo U-Gov CTE_INT21AVISC_01 e n. di creazione U-Gov 35718

Art. 1

La procedura di valutazione comparativa, per titoli, è intesa a selezionare n.2 soggetti disponibili a stipulare un contratto di diritto privato per attività di supporto alla ricerca.
In particolare le/i collaboratrici/ori dovranno raggiungere i seguenti obiettivi**:**

- comprendere le caratteristiche dei cifrari simmetrici, asimmetrici, delle funzioni hash e delle loro implementazioni.
- analizzare implementazioni e ottimizzazioni pubblicate in letteratura, comprenderne il funzionamento e utilizzare tali ottimizzazioni in fase di testing proponendo un'analisi critica di reali casi d'uso;
- eseguire una fase di sperimentazione nella quale verranno ricercati errati utilizzi di queste librerie o implementazioni improprie;
- documentare opportunamente l'attività sperimentale svolta e i risultati ottenuti.

Svolgendo la seguente attività:

- La prima fase del progetto sarà dedicata allo studio (1) della letteratura di cifrari e chiavi crittografiche; (2) di importanti librerie e implementazioni utilizzate negli attuali software open source; (3) delle debolezze pubblicate in letteratura. Inoltre, il collaboratore inizierà a prendere familiarità con gli strumenti da utilizzare.
- La seconda fase del progetto sarà dedicata allo sviluppo di un framework generico (in un opportuno linguaggio di programmazione, es. python, e utilizzando determinate librerie, es. Sagemath) in cui l'input (es. primitive crittografiche, permutazioni crittografiche, etc.), dato in pasto a diversi risolutori, viene automaticamente elaborato. L'obiettivo di questa seconda fase è quello di imparare a utilizzare in maniera disinvolta i risolutori automatici, identificando trails crittografici su particolari "esempi giocattolo" identificati durante le fasi di sviluppo del progetto.
- Inoltre, è richiesta la partecipazione del collaboratore ad un incontro settimanale di aggiornamento, in orario lavorativo, concordato sia con l'ente finanziatore del progetto, sia con il Responsabile Scientifico dello stesso.

Art. 2

La collaborazione sarà espletata personalmente dal/dai soggetto/i selezionato/i, in piena autonomia, senza vincoli di subordinazione, in via non esclusiva.

Art. 3

La collaborazione, della durata di 12 mesi, prevede un corrispettivo complessivo di Euro 5.000,00 al lordo di ritenute fiscali, previdenziali ed assistenziali a carico della/del Collaboratrice/ore.

Art. 4

Requisiti necessari ai fini dell'ammissione:

Laurea Triennale in Informatica o Matematica o Fisica, oppure analogo titolo accademico conseguito all'estero e riconosciuto equipollente al titolo italiano dalle competenti autorità accademiche, o comprovata specializzazione nell'ambito dell'incarico descritto

Criteri di valutazione (punteggio totale pari a 100):

- Conoscenze approfondite relative alle primitive crittografiche implementate all'interno di funzioni hash e cifrari simmetrici (fino a 25 punti)
- Comprovata esperienza nell'utilizzo dei risolutori automatici in ambito crittografico, per esempio SAT solvers, SMT solvers (fino a 15 punti)
- Comprovata esperienza pregressa in progetti crittografici (almeno 6 mesi) e/o in lavori di tesi di carattere sperimentale/teorico in ambito crittografico e/o in competizioni crittografiche internazionali/nazionali (fino a 15 punti)
- Conoscenza dell'algebra, in particolare dei campi finiti, e delle basi di Groebner (fino a 15 punti)
- Conoscenza dei linguaggi di programmazione, python in particolare (fino a 15 punti)
- Buona conoscenza della lingua inglese scritta e parlata (fino a 10 punti)
- Capacità di lavorare in autonomia e in team (fino a 5 punti)

Le/i candidate/i devono inoltre godere dei diritti civili e politici; non devono aver riportato condanne penali, non devono essere destinatarie/i di provvedimenti che riguardano l'applicazione di misure di prevenzione, di decisioni civili e di provvedimenti amministrativi iscritti nel casellario giudiziale, non devono altresì essere a conoscenza di essere sottoposte/i a procedimenti penali. Non possono partecipare alla presente selezione coloro che abbiano un grado di parentela o di affinità, fino al quarto grado compreso, con una/un professoressa/ore appartenente al dipartimento o alla struttura proponente ovvero con la Rettrice, il Direttore Generale o un/a componente del Consiglio di Amministrazione dell'Ateneo nonché, in

riferimento alle attività di studio o consulenza, i soggetti già lavoratori privati o pubblici collocati in quiescenza.

Art. 5

La selezione viene effettuata sulla base della valutazione dei curricula vitae e dei requisiti nell'art. 4. Il punteggio è espresso in centesimi e le/i candidate/i che non avranno conseguito almeno 60 punti non saranno ritenute/i idonee/i. Non si dà corso ad una graduatoria di merito.

Art. 6

La presentazione della domanda di partecipazione alla selezione di cui al presente avviso ha valenza di piena accettazione delle condizioni in esso riportate, di piena consapevolezza della natura autonoma del rapporto lavorativo.

Art. 7

La domanda di partecipazione dovrà essere presentata entro e non oltre **le ore 12** del giorno 9 maggio 2025.

Alla domanda, debitamente firmata, dovranno essere allegati dichiarazione dei titoli di studio posseduti, curriculum vitae in formato europeo e quant'altro si ritenga utile in riferimento ai titoli valutabili[1].

La domanda di partecipazione dovrà pervenire attraverso una delle seguenti modalità:

a) **Mediante PEC**

In formato PDF all'indirizzo di posta elettronica certificata (PEC) unimi@postecert.it (citando nell'oggetto della mail: **Domanda di partecipazione incarico di lavoro autonomo – Codice di Selezione 04/2025 - Dipartimento di Informatica "Giovanni degli Antoni").** L'invio dovrà essere effettuato esclusivamente da altro indirizzo PEC.

Si invita ad allegare al messaggio di posta elettronica certificata la domanda debitamente sottoscritta comprensiva dei relativi allegati e copia di un documento di identità valido in formato PDF.

Si precisa che la posta elettronica certificata non consente la trasmissione degli allegati che abbiano una dimensione pari o superiore a 30 Megabyte. La/il candidata/o che debba trasmettere allegati che complessivamente superino tale limite, dovrà trasmettere con una prima e-mail la domanda precisando che gli allegati o parte di essi saranno trasmessi con successive e-mail da inviare entro il termine per la presentazione delle domande e sempre tramite PEC.

[1] La modulistica è disponibile in calce alla pagina di pubblicazione del bando di riferimento.

Si precisa che ai sensi dell'art. 6 del D.P.R. n. 68 dell'11/02/2005, la validità della trasmissione della domanda tramite Posta elettronica certificata è attestata dalla ricevuta di accettazione e dalla ricevuta di avvenuta consegna fornite dal gestore di posta elettronica al momento dell'invio.

b) Mediante Posta Elettronica ordinaria (PEO) secondo le stesse modalità riportate nel punto a) e solo nel caso in cui la/il candidata/o non possieda l'indirizzo PEC. Si precisa che l'invio della domanda mediante posta elettronica ordinaria deve includere la richiesta di esplicita conferma di ricezione da parte del destinatario che sarà archiviata come ricevuta di consegna ed esibita a richiesta dell'Ateneo. La conferma deve essere richiesta all'indirizzo e-mail *amministrazione@di.unimi.it* .

Art. 8

La Commissione di valutazione comparativa delle/i candidate/i sarà nominata dopo la scadenza del presente avviso pubblico con determina del Direttore del Dipartimento di Informatica Giovanni degli Antoni.

Art. 9

Alla/al candidata/o dichiarata/o vincitrice/ore sarà fatto sottoscrivere un contratto di collaborazione, salvo revoca o non approvazione del finanziamento alla base del progetto di cui sopra.

Art. 10

Ai sensi del Decreto Legislativo n.196 del 2003 (Codice in materia di protezione dei dati personali) e sue successive modifiche e integrazioni, nonché del Regolamento UE 679/2016 (Regolamento Generale sulla Protezione dei dati, o più brevemente, RGPD) e dell'art. 7 del Regolamento d'Ateneo in materia di protezione dei dati personali, l'Università si impegna a rispettare la riservatezza delle informazioni fornite dalla/ dal collaboratrice/ore: tutti i dati conferiti saranno trattati solo per finalità connesse e strumentali alla gestione della collaborazione, nel rispetto delle disposizioni vigenti. L'informativa completa è disponibile alla seguente pagina del sito web d'Ateneo. Si informa inoltre che secondo quanto previsto dal D.lgs. 14/03/2013 n. 33 in materia di trasparenza, i curricula delle/dei vincitrici/ori, nonché la dichiarazione in merito ad altri incarichi saranno pubblicati sul sito web dell'Ateneo nella sezione "Amministrazione trasparente", "Consulenti e collaboratori" e sul sito web del Governo – Dipartimento della Funzione Pubblica nella sezione "Anagrafe delle Prestazioni".

UNIVERSITÀ DEGLI STUDI DI MILANO

Milano, 17 aprile 2025

IL DIRETTORE DEL DIPARTIMENTO

Prof. Danilo Mauro Bruschi

Danilo Mauro
Bruschi
Universita' degli
Studi di Milano
17.04.2025 14:14:27
GMT+02:00