



Per incarichi superiori a 5.000 Euro

Codice selezione ID 2402

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"

LA DIRIGENTE DELLA DIREZIONE TRATTAMENTI ECONOMICI E LAVORO AUTONOMO

- 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'art. 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 delibera del 9 aprile 2025 prot. 0015271/25 del 15/4/2025 del Dipartimento di Informatica;
- Considerato che in data 24 marzo 2025 con avviso interno prot. n. 0011285 del 20/03/2025 il Direttore del Dipartimento di Informatica, Prof. Danilo Bruschi ha avviato un'indagine preventiva rivolta al personale interno al fine di reperire una professionalità per ricoprire l'incarico 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 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;
- Vista la delega del Direttore Generale del 23/10/2024, rep. n. 17421/2024, con il quale è stata conferita formale delega di funzioni dal Direttore Generale alla Dott.ssa Anna Canavese, nella sua qualità di Dirigente di II^a fascia della Direzione Trattamenti Economici e Lavoro Autonomo, relative alla gestione delle procedure concorsuali e dei rapporti di collaborazione dei lavoratori assimilati, proprie del Settore Lavoro Autonomo - Ufficio Incarichi e Collaborazioni Esterne dell'Università degli Studi di Milano;

DETERMINA

È indetta una procedura di valutazione per il conferimento di un incarico di collaborazione a favore del Dipartimento di Informatica per attività di supporto alla ricerca, da svolgersi sotto la guida della Prof. Andrea Visconti nell'ambito del Progetto "Towards fully automatic search of



cryptographic trails” - c. i. U-Gov CTE_INT22AVISC_01 n. creaz. 41226 e CTE_INT23AVISC_01 n. creaz. 47443.

Art. 1

La procedura di valutazione comparativa, per titoli è intesa a selezionare un soggetto disponibile a stipulare un contratto di diritto privato per attività di supporto alla ricerca.

In particolare la/il collaboratrice/ore dovrà 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.

La/Il collaboratrice/ore supporterà il Responsabile Scientifico nelle seguenti 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;
- 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, identificando trails crittografici (lineari e differenziali) su un particolare “esempio giocattolo” e/o identificare i limiti relativi alla lunghezza dei trails;
- la terza ed ultima fase del progetto sarà dedicata alle attività di supporto di verifica del *framework* sviluppato durante la seconda fase, testando primitive o cifrari aventi una diversa struttura (es. DES, XTEA, SHA-1, etc.) e documentando/descrivendo le attività svolte, ivi compresi i risultati ottenuti anche in *paper* scientifici.

Art. 2

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

Art. 3

La collaborazione, della durata di 24 mesi, prevede un corrispettivo complessivo di € 59.000,00 al lordo di ritenute fiscali, previdenziali ed assistenziali a carico della/del Collaboratrice/ore.



Art. 4

Requisiti necessari ai fini dell'ammissione:

Laurea Magistrale 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):

- Dottorato o Laurea Magistrale 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 (fino a 20 punti);
- conoscenze approfondite relative alle primitive crittografiche implementate all'interno di funzioni hash e cifrari simmetrici (fino a 15 punti);
- comprovata esperienza nell'utilizzo dei risolutori automatici in ambito crittografico, per esempio SAT solvers, SMT solvers (fino a 10 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 (scritto e parlato) (fino a 10 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 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 richiesti nell'art. 4 e per colloquio che si svolgerà in data che sarà comunicata successivamente.



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 26/05/2025**.

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 valutabili¹.

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 ID 2402 - Dipartimento di Informatica**). 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 Candidata/il candidato 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.

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 il candidato non possieda l'indirizzo PEC. Si precisa che l'invio della

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



domanda mediante posta elettronica ordinaria deve includere la richiesta di esplicita conferma di ricezione da parte della/del destinataria/o 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 della Dirigente della Direzione Trattamenti Economici e Lavoro Autonomo.

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 D.lgs. n.196/2003 (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 di Ateneo. Si informa inoltre che secondo quanto previsto dal D.lgs. n. 33/2013 in materia di trasparenza, i curricula delle/dei vincitrici/ori, nonché la dichiarazione in merito ad altri incarichi saranno pubblicati sul sito web di Ateneo nella sezione "Amministrazione trasparente" - "Consulenti e collaboratori" e sul sito web del Governo - Dipartimento della Funzione Pubblica nella sezione "Anagrafe delle Prestazioni".

Art. 11

La Responsabile del procedimento di selezione è la Dott.ssa Anna Tavano - *e-mail*: anna.tavano@unimi.it . Per informazioni gli interessati potranno rivolgersi all'Ufficio Incarichi e Collaborazioni Esterne, *e-mail*: lavoroautonomo@unimi.it .

Milano, data della firma

LA DIRIGENTE
Anna Luisa Canavese