Per incarichi inferiori a 5.000 Euro

Codice selezione 1/2024

AVVISO PUBBLICO PER PROCEDURA DI DUE 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. 168/89;
Visto	l'art 7 comma 6 del Decreto Legislativo 30 marzo 2001, n. 165, e successive modificazioni;
Visto	l'articolo 81 comma 2 lettera b) 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 14/02/2024 prot. 0005473/24;
Considerato	che con avviso prot. N. 0004719/24 del 07/02/2024 il Direttore del Dipartimento di Informatica "Giovanni Degli Antoni" Prof. Danilo Bruschi ha emesso un avviso interno volto a reperire due professionalità per ricoprire gli incarichi di cui al presente avviso pubblico;
Verificato	che non è stato possibile reperire nessuna unità di personale interno per eseguire le prestazioni oggetto di tale avviso;

DETERMINA

È indetta una procedura di valutazione per il conferimento di due 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 CTE_INT21AVISC_01 - acronimo U-Gov 35718 e CTE_INT22AVISC_01 acronimo U-Gov no. creazione 41226.

Art. 1

La procedura di valutazione comparativa per titoli è intesa a selezionare due soggetti disponibili a stipulare un contratto di diritto privato per attività di supporto alla ricerca.

In particolare la/il collaboratrice/ore dovrà raggiungere i seguenti obbiettivi:
La/il collaboratrice/ore dovrà supportare il team ricerca svolgendo le seguenti attività:

- studio di caratteristiche e casi d'uso dei risolutori automatici utilizzati in ambito crittografico, mediante le principali librerie che li implementano;
- eseguire ricerche di trail crittografici in un framework generico;
- eseguire una fase di sperimentazione nella quale verranno ricercati trails crittografici, documentare/descrivere l'attività sperimentale svolta e i risultati ottenuti.

Svolgendo la seguente attività:

- La prima fase del progetto sarà dedicata allo studio (1) della letteratura dei risolutori automatici --- e.g. SAT, SMT, MILP, CP, etc.; (2) delle più importanti librerie utilizzate per implementare tali risolutori; (3) dei risultati pubblicati in letteratura in ambito crittografico.
- 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.
- 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.

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 mesi 12, prevede un corrispettivo complessivo di Euro 4.608,29 al lordo di ritenute fiscali, previdenziali ed assistenziali a carico del Collaboratrice/ore.

Art. 4

Requisiti necessari ai fini dell'ammissione:

Laurea Triennale in Informatica o Matematica, oppure analogo titolo accademico conseguito all'estero e riconosciuto equipollente al titolo italiano dalle competenti autorità accademiche.

Criteri di valutazione[1] :

- Conoscenze approfondite relative alle primitive crittografiche implementate all'interno di funzioni hash e cifrari simmetrici (fino a 20 punti)
- Comprovata esperienza nell'utilizzo dei risolutori automatici in ambito crittografico, per esempio SAT solvers, SMT solvers (fino a 12 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 20 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 12 punti)
- Capacità di lavorare in autonomia e in team (fino a 6 punti)

Le/i candidate/i devono inoltre godere dei diritti civili e politici; non devono aver riportato condanne penali, non devono essere destinatari 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 sottoposti 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 il Rettore, 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

[1] Si suggerisce di vedere l'art. 7 comma 6 della legge 165/01 e successive modificazioni e di indicare, se possibile, più lauree magistrali tra i requisiti

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 ritenuti idonei. 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 4 marzo 2024.**

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[2].

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 1/2024- 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 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

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

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)

Oppure è possibile inviare la domanda per posta elettronica ordinaria solo se il candidato non possiede l'indirizzo PEC di cui al punto a). 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 sarà nominata dopo la scadenza del presente avviso pubblico con determina del Direttore di Dipartimento.

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 dei vincitori, nonché la dichiarazione in merito ad altri incarichi saranno pubblicati sul sito web dell'Ateneo nella sezione "Amministrazione trasparente", "Consulenti e collaboratori".

Milano, 14 febbraio 2024

IL DIRETTORE

Danilo Mauro
Bruschi
Universita' degli
Studi di Milano
23.02.2024
12:45:54
GMT+01:00