



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 GENERALE

- Vista la Legge n. 168/89;
- Visto l'art. 7 comma 6 del D.Lgs. 165/2001 e ss.mm.ii.;
- Visto l'art. 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";
- Visto il provvedimento d'urgenza del 04/11/2021 del Direttore del Dipartimento di Informatica "Giovanni degli Antoni";
- Considerato che con avviso prot. n. 0035215/21 del 13/10/2021 il Direttore del Dipartimento di Informatica "Giovanni degli Antoni", Prof.ssa Silvana Castano, ha emesso un avviso interno volto a 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;

DETERMINA

È indetta una procedura di valutazione per il conferimento di un incarico di collaborazione a favore del Dipartimento di Informatica "Giovanni degli Antoni" per attività *di supporto alla ricerca*, da svolgersi sotto la guida del Dott. Andrea Visconti nell'ambito del Progetto "Towards fully automatic search of cryptographic trails" codice U-Gov CTE_INT21AVISC_01.

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 il collaboratore dovrà raggiungere i seguenti obiettivi:



- Comprendere le principali proprietà e casi d'uso dei risolutori automatici utilizzati in ambito crittografico, studiando le principali librerie che li implementano;
- Comprensione e applicazione di tali risolutori per la ricerca di *trail* crittografici in un *framework* generico;
- Fase di sperimentazione, nella quale verranno ricercati *trails* crittografici mediante dispositivi *High Performance Computing*.

Svolgendo la seguente attività:

Il collaboratore interverrà a supporto nelle varie attività del progetto, nello specifico:

- La prima fase del progetto sarà dedicata allo studio dello stato dell'arte e 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. funzioni hash, cifrari a blocchi, cifrari a flusso, permutazioni crittografiche, etc.), dato in pasto a diversi risolutori (SAT, SMT, MILP, CP, etc.), viene automaticamente elaborato. L'obiettivo di questa prima fase è quello di identificare un *trail* crittografico (lineare e differenziale) su un particolare "esempio giocattolo", e/o identificare limiti relativi alla lunghezza dei *trails*.
- La seconda fase del progetto sarà dedicata alla verifica del *framework* precedentemente sviluppato, testando input aventi diversa struttura e diverso design (es. DES, SHA-1, XTEA, etc.).

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 13 mesi, prevede un corrispettivo complessivo di Euro 22.750,00 (IVA ed eventuale cassa escluse) al lordo di ritenute fiscali, previdenziali ed assistenziali a carico del Collaboratore.

Art. 4

Requisiti necessari ai fini dell'ammissione:

- Laurea Magistrale in Informatica o Matematica 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:

- Laurea Magistrale in Informatica o Matematica 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 (20 punti)
- Conoscenze crittografiche approfondite relative alle funzioni *hash* e ai cifrari simmetrici (15 punti)
- Comprovata esperienza nell'utilizzo di risolutori automatici in ambito crittografico (20 punti)
- Comprovata esperienza pregressa (almeno 12 mesi) in progetti crittografici (20 punti)
- Conoscenza dei linguaggi di programmazione, *python* in particolare (10 punti)
- Buona conoscenza della lingua inglese (scritto e parlato) (10 punti)
- Capacità di lavorare in autonomia e in team (5 punti)

I candidati 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 un professore 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

La selezione viene effettuata sulla base della valutazione dei curricula vitae e dei requisiti richiesti nell'art 4. Il punteggio è espresso in centesimi e i candidati 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 10/01/2022.

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 1831 - 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. 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)

Considerate le disposizioni normative in materia di contenimento e gestione dell'emergenza epidemiologica da COVID-19, 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 mail amministrazione@di.unimi.it.

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



UNIVERSITÀ DEGLI STUDI DI MILANO

Art. 8

La Commissione sarà nominata dopo la scadenza del presente avviso pubblico con determina del Direttore Generale.

Art. 9

Al candidato dichiarato vincitore 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 dal collaboratore: 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".

IL DIRETTORE GENERALE

Roberto Conte