IL DIRETTORE DEL DIPARTIMENTO

Visto l'art. 7 comma 6 del Decreto Legislativo 30 marzo 2001 n. 165 e successive modifiche e integrazioni;

Visto il Regolamento per l'affidamento a terzi estranei all'Università di incarichi di carattere intellettuale emanato con Decreto Rettorale Reg. 0267760 del 23/04/2010;

Visto il Progetto "TOWARDS FULLY AUTOMATIC SEARCH OF CRYPTOGRAPHIC TRAILS";

Visto l'avviso di conferimento rivolto al personale interno pubblicato sul sito Web d'Ateneo prot. n. 0012600/25 del 27/03/2025 che è andato deserto;

Visto l'avviso di procedura comparativa ID 04/2025 Rep. 6756/2025 del 17/04/2025 per l'affidamento di un incarico di collaborazione di lavoro autonomo, della durata di 12 mesi e per un compenso di € 5.000,00 a *al lordo di ritenute fiscali, previdenziali ed assistenziali a carico del Collaboratore* (*oppure IVA e Cassa incluse*) a carico del Collaboratore, per attività di "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";

Considerato che l'importo lordo pari a 5.000,00, risulta congruo per l'attività in esso dedotta;

Verificata la disponibilità dei fondi posto a carico del progetto CTE_INT22AVISC_01 TOWARDS FULLY AUTOMATIC SEARCH OF CRYPTOGRAPHIC TRAILS;

Vista la determina di nomina della Commissione del 20/05/2025 rep. 8629/2025 del 22/05/2025;

Visto il verbale di selezione per *titoli o titoli e colloquio* del 05/06/2025 da cui risultano attribuiti ai candidati i seguenti punteggi:

COGNOME E NOME	PUNTI

Bellini Gabriele	80/100
Gallone Michela	60/100

DETERMINA

L'approvazione degli atti della procedura comparativa ID 04/2025 Rep. 6756/2025 del 17/04/2025;

L'autorizzazione alla stipula di un contratto occasionale al Dott. Bellini Gabriele e di un contratto occasionale alla dott.ssa Gallone Michela per attività di collaborazione nel progetto di ricerca "TOWARDS FULLY AUTOMATIC SEARCH OF CRYPTOGRAPHIC TRAILS"; finalizzata al raggiungimento dei 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".

Tale attività sarà da svolgersi nell'ambito del Progetto "TOWARDS FULLY AUTOMATIC SEARCH OF CRYPTOGRAPHIC TRAILS".

L' importo di ciascun contratto sarà di Euro 5.000,00 al lordo di ritenute fiscali, previdenziali ed assistenziali a carico del Collaboratore (*oppure IVA e Cassa incluse*) e avrà la durata di n. 12 mesi a favore del Dipartimento di informatica Giovanni degli Antoni.

Il corretto svolgimento dell'incarico sarà verificato dal Prof. Andrea Visconti;

Il costo di 5.000,00 euro di ciascuno dei due contratti graverà sul progetto CTE_INT22AVISC_01 numero di creazione 41226 denominato “TOWARDS FULLY AUTOMATIC SEARCH OF CRYPTOGRAPHIC TRAILS” del Dipartimento di informatica Giovanni degli Antoni.

Milano, 05 giugno 2025

Per IL DIRETTORE DEL DIPARTIMENTO
Il Vicedirettore Prof. Giuseppe Boccignone

Giuseppe
Boccignone
Universita' degli
Studi di Milano
05.06.2025 16:22:57
GMT+01:00