**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" codice identificativo CTE_INT21AVISC_01 - acronimo U-Gov 35718 e CTE_INT22AVISC_01 acronimo U-Gov no. creazione 41226;

Visto l'avviso di conferimento rivolto al personale interno pubblicato sul sito Web d'Ateneo prot. n. 0004719/24 del 07/02/2024 che è andato deserto;

Visto l'avviso di procedura comparativa ID 1/2024 Rep. 2140/2024 del 27/02/2024 per l'affidamento di un incarico di collaborazione di lavoro autonomo, della durata di 12 mesi e per un compenso di € 4.608,29 *al lordo di ritenute fiscali, previdenziali ed assistenziali a carico del Collaboratore* (*oppure IVA e Cassa incluse*) a carico del Collaboratore, per attività di "attività di supporto alla ricerca 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";

Considerato che l'importo lordo pari a € 4.608,29 risulta congruo per l'attività in esso dedotta;

Verificata la disponibilità dei fondi posto a carico del progetto Towards fully automatic search of cryptographic trails" codice identificativo CTE_INT21AVISC_01 - acronimo U-Gov 35718 e CTE_INT22AVISC_01;

Vista la determina di nomina della Commissione del 11/03/2024 rep. 3122/2024;

Visto il verbale di selezione per *titoli o titoli e colloquio* del 19/04/2024 da cui risultano attribuiti ai candidati i seguenti punteggi:

| COGNOME E NOME | PUNTI |
|---|---|
| Gorla Federico | 68 |
| Oldani Mattia | 62 |
| Palmulli Luca | 63 |

**DETERMINA**

L'approvazione degli atti della procedura comparativa ID 1/2024 Rep. 2140/2024 del 27/02/2024;

L'autorizzazione alla stipula di due contratti, dei quali l'uno contratto occasionale, al Dott. Federico Carlo Gorla e l'altro occasionale, al Dott. Luca Palmulli

finalizzati al raggiungimento dei seguenti obiettivi:

- 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 ciascun collaboratore 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.

Tale attività sarà da svolgersi 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".

L' importo di ciascuno dei due contratti sarà di Euro € 4.608,29 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.

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

Il costo di Euro € 4.608,29 euro di ciascuno dei due contratti graverà sul progetto (acronimo U-GOV e numero di creazione) denominato CTE_INT21AVISC_01 - acronimo U-Gov 35718 e CTE_INT22AVISC_01 acronimo U-Gov no. creazione 41226" del Dipartimento di Informatica;

Milano, 29 aprile 2024

**IL DIRETTORE DEL DIPARTIMENTO**

**Prof Danilo Mauro Bruschi**

_____

Danilo Mauro Bruschi
Universita' degli Studi di Milano
29.04.2024 17:41:17
GMT+01:00