IL DIRETTORE DEL DIPARTIMENTO /RESPONSABILE DELLA STRUTTURA

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 CTE_INT19AVISC_01;

Visto l'avviso di conferimento rivolto al personale interno pubblicato sul sito Web d'Ateneo prot. n. 0003605/22 del 02/02/2022 che è andato deserto;

Visto l'avviso di procedura comparativa ID 02/2022 Rep. 0015359/22 del 27/04/2022 per l'affidamento di due incarichi di collaborazione di lavoro autonomo, della durata di 12 mesi e per un compenso di ad € 5.000,00 per ciascun contratto (per contratto occasionale: lordo + 8,5% irap) oppure di € 6.150,00 (ipotesi contratti individuale) oppure di € 4.608,29 (ipotesi contratti professionali- IVA ed eventuale cassa escluse), *al lordo di ritenute fiscali, previdenziali ed assistenziali a carico del Collaboratore*, per "ATTIVITÀ DI SUPPORTO ALLA RICERCA NELL'AMBITO DEL PROGETTO ALGEBRAIC ANALYSIS OF HMAC-SHA-1";

Considerato che l'importo lordo pari ad € 5.000,00 per ciascun contratto (per contratto occasionale: lordo + 8,5% irap) oppure di € 6.150,00 (ipotesi contratti individuale) oppure di € 4.608,29 (ipotesi contratti professionali- IVA ed eventuale cassa escluse), risulta congruo per l'attività in esso dedotta;

Verificata la disponibilità dei fondi posto a carico del progetto CTE_INT19AVISC_01;

Vista la determina di nomina della Commissione del 13/05/2022 rep. 0017584/22 del 12/05/2022;

Visto il verbale di selezione per *titoli o titoli e colloquio* del 20/05/2022 da cui risultano attribuiti ai candidati i seguenti punteggi:

COGNOME E NOME	PUNTI
Casorerio Simone	70/100
Corrias Michele	61/100
Formenti Mattia	83/100
Garlet Marco	72/100
Lepori Pietro	60/100
Pelizzola Simone	83/100

DETERMINA

L'approvazione degli atti della procedura comparativa ID 02/2022 Rep. 0015359/22 del 27/04/2022;

L'autorizzazione alla stipula di un contratto occasionale con il sig. Simone Pelizzola e di un contratto occasionale con il dott. Mattia Formenti per attività di SUPPORTO ALLA RICERCA NELL'AMBITO DEL PROGETTO ALGEBRAIC ANALYSIS OF HMAC-SHA-1 finalizzata al raggiungimento dei seguenti obiettivi:

• comprendere caratteristiche e casi d'uso dei risolutori automatici utilizzati in ambito crittografico sfruttando 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 e descrivere l'attività sperimentale svolta e i risultati ottenuti.

Ciascun collaboratore supporterà il Responsabile Scientifico nelle seguenti attività:

- La prima fase del progetto sarà dedicata allo studio (1) della letteratura dei risolutori automatici --- e.g. SAT solver, SMT solver, risolutori basati su Constraint Programming (CP), etc.; (2) delle più importanti librerie utilizzate per implementare tali risolutori; (3) dei risultati pubblicati in letteratura in ambito crittografico. Inoltre, il collaboratore dovrà 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 identificare 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 input aventi diversa struttura (es. DES, SHA-1, XTEA, etc.) e descrivendo le attività svolte e i risultati ottenuti.Tale attività sarà da svolgersi nell'ambito del Progetto "Algebraic abalysis of HMAC-SHA-1".

L' importo di ciascuno dei due contratti sarà di Euro 5.000,00 al lordo di ritenute fiscali a carico del Collaboratore e avrà la durata di n. 12 mesi a favore del Dipartimento di Informatica "Giovanni degli Antoni";

Il corretto svolgimento di ciascun incarico sarà verificato dal Dr. Andrea Visconti;

Il costo di 5.425,00 euro per ciascun incarico graverà sul progetto **CTE_INT19AVISC_01 numero di creazione 32011** denominato Algebraic abalysis of HMAC-SHA-1 del Dipartimento di Informatica "Giovanni degli Antoni";

UNIVERSITÀ DEGLI STUDI DI MILANO

Milano, 24/05/2022

IL DIRETTORE DEL DIPARTIMENTO

Prof.ssa Silvana Castano

_____

CASTANO
SILVANA
Universita`
degli Studi di
Milano
25.05.2022
09:52:43
GMT+00:00