Logo Image not found or type unknown

PROGRAMMA DEL CORSO DI PRINCIPI E METODI DI CRITTOGRAFIA

SETTORE SCIENTIFICO

INF/01 (INFO-01/A)

CFU

6

SETTORE SCIENTIFICO DISCIPLINARE

/**/
INF/01

ANNO DI CORSO

/**/
I Anno

TIPOLOGIA DI ATTIVITÀ FORMATIVA

/**/

Base X
Caratterizzante q
Affine q
Altre attività q

NUMERO CREDITI

/**/
6 CFU

DOCENTE

/**/
Riccardo Treglia

MODALITÀ DI ISCRIZIONE E DI GESTIONE DEI RAPPORTI CON GLI STUDENTI

/**/
L’iscrizione ed i rapporti con gli studenti sono gestiti mediante la piattaforma informatica che permette l’iscrizione ai corsi, la fruizione delle lezioni, la partecipazione a forum e tutoraggi, il download del materiale didattico e la comunicazione con il docente. Un tutor assisterà gli studenti nello svolgimento di queste attività.

OBIETTIVI FORMATIVI SPECIFICI

/**/

L'obiettivo del corso è fornire agli studenti le conoscenze teoriche alla base dei principali algoritmi/protocolli crittografici impiegati in sicurezza informatica e rendere gli studenti in grado di applicare tali conoscenze nello sviluppo di sistemi software che offrano un determinato livello di sicurezza. Verrà evidenziato che la maggior parte degli attacchi informatici è rivolto alle vulnerabilità che si celano all’interno delle applicazioni software, che forniscono un facile percorso d’ingresso per compromettere i sistemi o lanciare attacchi informatici e malware. Saranno illustrate metodologie di progettazione e programmazione che garantiscano la sicurezza del codice. Saranno introdotti principi di gestione del rischio informatico e della sicurezza nei sistemi informativi alla luce degli adempimenti legislativi da rispettare.

RISULTATI DI APPRENDIMENTO SPECIFICI

/**/

Conoscenza e capacità di comprensione
Lo studente acquisirà la conoscenza delle fondamentali metodologie in materia di sicurezza informatica riconducibile ad una buona ingegnerizzazione del software, e sarà consapevole della necessità di applicarle per rispondere alla domanda di sicurezza e per ridurre i costi che comporta il trascurarle. Verrà illustrata l’analisi della sicurezza del software rivolta alla individuazione delle vulnerabilità.

Capacità di applicare conoscenza e comprensione
Lo studente acquisirà la capacità di valutare il codice software e le applicazioni al fine di identificare le vulnerabilità. Sarà in grado di implementare opportune attività che garantiscano la sicurezza nel corso di tutte le fasi del ciclo di vita del software, dalla analisi alla progettazione, sviluppo, test fino alla manutenzione.

Autonomia di giudizio
Lo studente sarà in grado di valutare le problematiche connesse alla sicurezza informatica in tutte le fasi del ciclo di sviluppo software nei vari ambiti di applicazione.
Abilità comunicative
L’esposizione del materiale didattico e l’ascolto delle lezioni consentiranno agli studenti di argomentare con un lessico preciso ed appropriato. Lo studente deve avere la capacità di spiegare, in maniera semplice, i concetti relativi alla analisi matematica.

Capacità di apprendimento
I concetti e gli istituti assimilati attraverso le videolezioni dovranno essere arricchiti e rielaborati dallo studente durante e al termine dell’intero percorso di studi. Lo studente deve essere in grado di aggiornarsi continuamente, tramite la consultazione di testi di analisi.

PROGRAMMA DIDATTICO

/**/

1 - LE BASI DELLA CRITTOGRAFIA

2 - CRITTOGRAFIA SIMMETRICA

3 - CRITTOGRAFIA ASIMMETRICA

4 - GLI ALGORITMI DI HASH

5 - PKI

6 - CERTIFICATI X509

7 - FIRMA DIGITALE

8 - RSA

9 - CURVE ELLITTICHE

10 - FIDO2

11 - PROTOCOLLI DI SCAMBIO CHIAVI11

12 - TLS

13 - ATTACCHI MITM

14 - CRITTOGRAFIA E BLOCKCHAIN

15 - CRITTOGRAFIA QUANTISTICA

16 - PASSWORD CRACKING

17 - INTRODUZIONE ALLA MALWARE ANALYSIS

18 - MALWARE STORICI E IL PROCESSO DI MALWARE ANALYSIS

19 - ANALISI STATICA

20 - ANALISI DINAMICA

21 - ANALISI AVANZATA

22 - ANALISI DELLE VULNERABILITA SFRUTTATE DAGLI MALWARE

23 - AMBIENTE DI LABORATORIO PER L’ANALISI MALWARE

24 - TOOL DI ANALISI DEL MALWARE

25 - ANALISI DEL NETWORK TRAFFIC

26 - TECNICHE DI EVASIONE DEL MALWARE

27 - ANALISI DI PARTICOLARI INFECTION CHAIN

28 - THREAT INTELLIGENCE

29 - INDICATORI DI COMPROMISSIONE E MODELLI DI THREAT INTELLIGENCE

30 - RILEVAMENTO DEL MALWARE E PREVENZIONE

31 - WINDOWS EVENTS E REGOLE DI RILEVAMENTO

32 - COMPUTER VIROLOGY

33 - MECCANISMI DI DIFESA

34 - I SISTEMI OPERATIVI MOBILI

35 - MALWARE ANALYSIS

36 - ANDROID MALWARE DISSECTION

TIPOLOGIE DI ATTIVITÀ DIDATTICHE PREVISTE E RELATIVE MODALITÀ DI SVOLGIMENTO

/**/

Ogni Macro-argomento è articolato in 15-17 videolezioni da 30 min. corredate da dispense, slide e test di apprendimento.
Per ogni insegnamento sono previste sino a 6 videolezioni (n.1 CFU) di didattica innovativa secondo modalità definite dal docente di riferimento.
Le videolezioni sono progettate in modo da fornire allo studente una solida base di competenze culturali, logiche e metodologiche atte a far acquisire capacità critiche necessarie ad esercitare il ragionamento matematico, anche in una prospettiva interdisciplinare, a vantaggio di una visione del diritto non meramente statica e razionale, bensì quale espressione della società e della sua incessante evoluzione.
Il modello didattico adottato prevede sia didattica erogativa (DE) sia didattica interattiva (DI):

- La didattica erogativa (DE) prevede l'erogazione in modalità asincrona delle videolezioni, delle dispense, dei test di autovalutazioni predisposti dai docenti titolari dell'insegnamento; la metodologia di insegnamento avviene in teledidattica.

- La didattica interattiva (DI) comprende il complesso degli interventi didattici interattivi, predisposti dal docente o dal tutor in piattaforma, utili a sviluppare l'apprendimento online con modalità attive e partecipative ed è basata sull'interazione dei discenti con i docenti, attraverso la partecipazione ad attività didattiche online.

  Sono previsti interventi brevi effettuati dai corsisti (ad esempio in ambienti di discussione o di collaborazione, in forum, blog, wiki), e-tivity strutturate (individuali o collaborative), sotto forma tipicamente di produzioni di elaborati o esercitazioni online e la partecipazione a web conference interattive.

  Nelle suddette attività convergono molteplici strumenti didattici, che agiscono in modo sinergico sul percorso di formazione ed apprendimento dello studente. La partecipazione attiva alle suddette attività ha come obiettivo quello di stimolare gli studenti lungo tutto il percorso didattico e garantisce loro la possibilità di ottenere una valutazione aggiuntiva che si sommerà alla valutazione dell'esame finale.

Per le attività di autoapprendimento sono previste 108 ore di studio individuale.
L'Ateneo prevede 7 h per ogni CFU articolate in 6 h di didattica erogativa (DE) e 1 h di didattica interattiva (DI).
Nel computo delle ore della DI sono escluse le interazioni a carattere orientativo sui programmi, sul cds, sull'uso della piattaforma e simili, che rientrano un semplice tutoraggio di orientamento. Sono altresì escluse le ore di tutorato didattico disciplinare, cioè la mera ripetizione di contenuti già proposti nella forma erogativa attraverso colloqui di

recupero o approfondimento one-to-one.

MODALITÀ E CRITERI DI VALUTAZIONE DELL'APPRENDIMENTO

/**/

La partecipazione alla didattica interattiva (DI) ha la finalità, tra le altre, di valutare lo studente durante l'apprendimento in itinere.
L'esame finale può essere sostenuto in forma scritta o in forma orale; lo studente può individuare, in autonomia, la modalità di svolgimento della prova, sempre rispettando la calendarizzazione predisposta dall'Ateneo.
L'esame orale consiste in un colloquio nel corso del quale il docente formula almeno tre domande.
L'esame scritto consiste nello svolgimento di un test a risposta multipla con 31 domande. Per ogni domanda lo studente deve scegliere una delle 4 possibili risposte. Solo una risposta è corretta.
Sia i quesiti in forma orale che i quesiti in forma scritta sono formulati per valutare il grado di comprensione delle nozioni teoriche e la capacità di sviluppare il ragionamento utilizzando le nozioni acquisite. I quesiti che richiedono l'elaborazione di un ragionamento consentiranno di valutare il livello di competenza e l'autonomia di giudizio maturati dallo studente.
Le abilità di comunicazione e la capacità di apprendimento saranno valutate attraverso le interazioni dirette tra docente e studente che avranno luogo durante la fruizione del corso (videoconferenze, e-tivity report, studio di casi elaborati) proposti dal docente o dal tutor.

CRITERI DI MISURAZIONE DELL'APPRENDIMENTO E ATTRIBUZIONE DEL VOTO FINALE

/**/

Sia lo svolgimento dell'elaborato, sia la presenza attiva durante le web conference prevedono un giudizio, da parte del docente, fino a un massimo di 2 punti. Lo studente può prendere parte ad entrambe le attività ma la votazione massima raggiungibile è sempre di 2 punti.
La valutazione proveniente dallo sviluppo dell'elaborato può essere pari a 0, 1 o 2 punti.
La valutazione derivante dalle web conference è strutturata tramite lo svolgimento, al termine della stessa, di un test finale a risposta multipla che può garantire da 0 a 1 punto.
È data facoltà allo studente di partecipare o meno alla didattica interattiva.
La valutazione finale ha lo scopo di misurare il raggiungimento degli obiettivi di apprendimento definiti alla base dell'insegnamento. Il giudizio riguarda l'intero percorso formativo del singolo insegnamento ed è di tipo sommativo.
Il voto finale dell'esame di profitto tiene conto del punteggio che lo studente può aver ottenuto partecipando correttamente alla didattica interattiva e deriva, quindi, dalla somma delle due valutazioni. Il voto derivante dalla didattica interattiva verrà sommato al voto dell'esame se quest'ultimo sarà pari o superiore a diciotto trentesimi.
Il voto finale è espresso in trentesimi. Il voto minimo utile al superamento della prova è di diciotto trentesimi.
Ciascun test dovrà essere composto da 31 domande, così da garantire la possibilità di conseguire la lode, in ottemperanza alle norme Europee sul Diploma Supplement. L'attribuzione della lode è concessa esclusivamente allo studente che ha risposto positivamente alle prime 30 domande.

ATTIVITÀ DI DIDATTICA EROGATIVA (DE)

/**/

- è 36 Videolezioni + 36 test di autovalutazione

Impegno totale stimato: 36 ore

ATTIVITÀ DI DIDATTICA INTERATTIVA (DI) ED E-TIVITY CON RELATIVO FEED-BACK AL SINGOLO STUDENTE DA PARTE DEL DOCENTE O DEL TUTOR

/**/

- è Redazione di un elaborato
- è Partecipazione a web conference
- è Svolgimento delle prove in itinere con feedback
- è Svolgimento della simulazione del test finale

Totale 6 ore

MATERIALE DIDATTICO UTILIZZATO

/**/

- è Videolezioni
- è Dispense predisposte dal docente e/o slide del docente
- è Testo di riferimento suggerito dal docente (facoltativo)

Il materiale didattico è sempre disponibile in piattaforma e consultabile dallo studente nei tempi e nelle modalità ad egli più affini.