UNIVERSITÀ DEGLI STUDI DI ENNA "KORE"

Facoltà di Ingegneria e Architettura
Anno Accademico 2022/2023
Corso di studi in Ingegneria Informatica, classe di laurea L8

Insegnamento	Sicurezza Informatica
CFU	9
Settore Scientifico Disciplinare	ING-INF/05
Metodologia didattica	Lezioni Frontali
Nr. ore di aula	54
Nr. ore di studio autonomo	171
Nr. ore di laboratorio	0
Mutuazione	NO
Annualità	II Anno
Periodo di svolgimento	II Semestre

Docente	E-mail	Ruolo[i]	SSD docente
Vincenzo Conti	vincenzo.conti@unikore.it	PA	ING-INF/05

Propedeuticità	Nessuna
Sede delle lezioni	Facoltà di Ingegneria e Architettura

Moduli

N.	Nome del modulo	Docente	Durata in ore

Orario delle lezioni

L'orario delle lezioni sarà pubblicato sulla pagina web del sito Unikore:
https://gestioneaule.unikore.it/agendaweb_unikore/index.php?view=easycourse&_lang=it

Obiettivi formativi

Studio e analisi delle minacce delle vulnerabilità e del rischio associato ai sistemi informatici al fine di proteggerli da possibili attacchi (interni o esterni) che potrebbero provocare danni diretti o indiretti di impatto superiore ad una determinata soglia di tollerabilità.

Contenuti del Programma

N.	ARGOMENTO	TIPOLOGIA	DURATA
1	Concetti sulla Sicurezza Informatica: Attacchi, Servizi, Meccanismi	Frontale	3h
2	Studio e Implementazione della Cifratura Simmetrica Classica e Criptoanalisi	Frontale	10h
3	Introduzione Cifratura Simmetrica Moderna: Cifrari a Blocchi	Frontale	2h
4	Concetti di base sulla Teoria dei Numeri e sui Campi Finiti	Frontale	2h
5	Studio e Implementazione degli Algoritmi di Crittografia: DES, Double DES, Triple DES, BLOWFISAH, AES	Frontale	12h
6	Modi di Funzionamento dei Cifrari a Blocchi	Frontale	2h

7	Generatori di Numeri Pseudo-Casuali e Cifrari a Flusso	Frontale	4h
8	Introduzione Cifratura Asimmetrica: Chiave Pubblica e Chiave Privata	Frontale	1h
9	Studio e Implementazione degli Algoritmi RSA e a Curva Ellittica	Frontale	10h
10	Protocollo Scambio Chiave di Sessione: Diffie-Hellaman	Frontale	2h
11	Protocollo Scambio Chiave Pubblica e Certificati	Frontale	2h
12	Cenni sull'Autenticazione Utente Sicura: Sistemi Biometrici	Frontale	2h
13	Cenni sui Software Maliziosi	Frontale	2h

Risultati di apprendimento (descrittori di Dublino)

I risultati di apprendimento attesi sono definiti secondo i parametri europei descritti dai cinque descrittori di Dublino.

1. **Conoscenza e capacità di comprensione (knowledge and understanding)**: Lo studente alla fine del corso acquisirà una buona conoscenza delle principali tecniche e algoritmi di crittografia per la cifratura/decifratura dei messaggi, di autenticazione e protezione dei sistemi informatici. Sarà in grado di analizzare e comprendere il codice sorgente dei principali algoritmi utilizzati per la protezione dei sistemi informatici.
2. **Capacità di applicare conoscenza e comprensione (applying knowledge and understanding)**: Lo studente sarà in grado di valutare le caratteristiche, i vantaggi e le limitazioni dei principali sistemi analizzati. Sarà in grado di progettare, analizzare e valutare le soluzioni software a problemi di sicurezza di media complessità. Sarà anche in grado di sviluppare le soluzioni software, valutandone la qualità in termini di semplicità, efficacia ed efficienza.
3. **Autonomia di giudizio (making judgements)**: Lo studente sarà in grado sia di effettuare l'analisi di un problema di sicurezza che di progettare, a partire da precise specifiche, una opportuna soluzione software. Sarà in grado di valutarne la qualità di una soluzione software in termini di semplicità, leggibilità, efficienza e possibilità di riutilizzo. L'autonomia di giudizio verrà valutata esaminando le soluzioni proposte dagli studenti a problemi di sicurezza di media complessità. Lo studente verrà incoraggiato inizialmente a trovare e valutare autonomamente soluzioni ai problemi posti, al fine di potere comprendere la qualità e l'utilità delle soluzioni proposte successivamente dal docente.
4. **Abilità comunicative (communication skills)**: Lo studente acquisirà la capacità di comunicare ed esprimere problematiche inerenti all'oggetto del corso. Sarà in grado di sostenere conversazioni su tematiche relative alla sicurezza informatica e all'implementazioni software di algoritmi al fine di contrastare tale tematica. Sarà in grado di utilizzare un linguaggio semplice e chiaro per la descrizione dei processi di analisi e di sintesi di soluzioni di sicurezza a problemi di media complessità. Il carattere interattivo delle lezioni dovrà permettere il miglioramento delle abilità comunicative dello studente.
5. **Capacità d'apprendimento (learning skills)**: Lo studente dovrà sviluppare la capacità di apprendere i processi di analisi e di sintesi relativi alla codifica di algoritmi di cifratura/decifratura e autenticazione di media complessità e alla relativa implementazione di librerie e strumenti software. Il grado di apprendimento sarà valutato non in base alla capacità di memorizzare concetti specifici ma in base alla capacità di ricostruire ex novo, partendo dal minor numero possibile di idee generali di base, le migliori soluzioni software.

Testi per lo studio della disciplina

Testo di riferimento:

- Crittografia – William Stallings – Pearson Editore

Slide del corso

Testo per eventuali approfondimenti:

- Sicurezza dei computer e delle Reti – William Stallings – Pearson Editore

Modalità di accertamento delle competenze

L'obiettivo della prova d'esame consiste nel verificare il livello di raggiungimento delle conoscenze,

competenze e abilità in accordo con i descrittori di Dublino. Il voto sarà dato in trentesimi e varierà da 18/30 a 30/30 con lode. L'accertamento delle competenze si basa su un esame espletato in un'unica giornata solamente tramite una prova orale basata sull'esposizione degli argomenti trattati durante il corso.
Il voto sarà espresso, secondo il seguente schema di valutazione:

- Ottimo (30-30 e lode): Ottima conoscenza e comprensione degli argomenti trattati. Ottima capacità di applicare le conoscenze acquisite per risolvere i problemi di sicurezza proposti. Eccellenti capacità espositive.
- Molto buono (26-29): Buona conoscenza e comprensione degli argomenti trattati. Buona capacità di applicare le conoscenze acquisite per risolvere i problemi di sicurezza proposti. Ottime capacità espositive.
- Buono (24-25): Buona conoscenza e comprensione degli argomenti trattati. Discreta capacità di applicare le conoscenze acquisite per risolvere i problemi di sicurezza proposti. Buone capacità espositive.
- Discreto (21-23): Discreta conoscenza e comprensione degli argomenti trattati. Limitata capacità di applicare le conoscenze acquisite per risolvere i problemi di sicurezza proposti. Discrete capacità espositive.
- Sufficiente (18-20): Conoscenza minima degli argomenti trattati e limitata capacità di applicare le conoscenze acquisite per risolvere i problemi di sicurezza proposti. Sufficienti capacità espositive.
- Insufficiente: Manca di una conoscenza accettabile degli argomenti trattati e non dimostra una sufficiente capacità di applicare le conoscenze acquisite per risolvere i problemi di sicurezza proposti. Scarsa capacità espositiva.

Date di esame

Le date di esami saranno pubblicate sulla pagina web del sito Unikore:
https://gestioneaule.unikore.it/agendaweb_unikore/index.php?view=easytest&_lang=it

Modalità e orario di ricevimento

Gli orari di ricevimento saranno pubblicati sulla pagina personale del docente:
https://unikore.it/cdl/ingegneria-informatica/persone-e-regolamenti/vincenzo-conti/

[i] PO (professore ordinario), PA (professore associato), RTD (ricercatore a tempo determinato), RU (Ricercatore a tempo indeterminato), DC (Docente a contratto).