## Principali informazioni sull'insegnamento

| | |
|---|---|
| Denominazione dell'insegnamento | **Crittografia** |
| Corso di studio | Sicurezza Informatica |
| Anno Accademico | AA 2024/25 |
| Crediti formativi universitari (CFU) / European Credit Transfer and Accumulation System (ECTS) | 6 CFU |
| Settore Scientifico Disciplinare | INF/01 |
| Lingua di erogazione | Italiano |
| Anno di corso | Primo |
| Periodo di erogazione | 1^ semestre, le date esatte sono riportate nel manifesto/regolamento |
| Obbligo di frequenza | La frequenza è fortemente raccomandata |
| Sito web del corso di studio | https://www.uniba.it/it/ricerca/dipartimenti/informatica/didattica/corsi-di-laurea/sicurezza-informatica/laurea-magistrale-in-informatica |

## Docente

| | |
|---|---|
| Nome e cognome | Stefano Galantucci |
| Indirizzo mail | stefano.galantucci@uniba.it |
| Telefono | NA |
| Sede | Dipartimento di Informatica - Sede di Taranto, Via Alcide De Gasperi |
| Sede virtuale | Piattaforma E-Learning - https://elearning.uniba.it/ |
| Sito web del docente | https://islab.di.uniba.it/team/stefano-galantucci/ |
| Ricevimento (giorni, orari e modalità, es. su appuntamento) | Mercoledì ore 14:00 su appuntamento |

## Syllabus

| | |
|---|---|
| **Obiettivi formativi** | Acquisizione delle competenze crittografiche, raggiungimento della piena consapevolezza e capacità di distinzione tra algoritmo e protocollo crittografico, dei singoli algoritmi e protocolli, delle loro proprietà, peculiarità, debolezze e delle modalità di applicazione. Valutazione di ciascun elemento nei termini di riservatezza, |

| | |
|---|---|
| | autenticazione delle parti, integrità e non ripudio. Ottenimento della massima competenza e conoscenza dei limiti della crittografia e delle sue debolezze intrinseche. Acquisizione delle capacità di determinare i limiti e le debolezze di ciascun algoritmo attraverso una conoscenza basilare della crittanalisi e dei concetti legati allo spazio delle chiavi. |
| **Prerequisiti** | Conoscenze relative a:<br>– Matematica Discreta (in particolare: numeri primi, strutture algebriche, algebra modulare, generatori, calcolo combinatorio)<br>– Analisi matematica (in particolare: funzioni, successioni, curve, polinomi, interpolazione polinomiale)<br>– Calcolo delle probabilità<br>– Teoria dei linguaggi formali<br>– Teoria della complessità computazionale<br>– Reti di calcolatori |
| **Contenuti di insegnamento (Programma)** | Introduzione alla Crittografia<br>– Riservatezza, autenticazione, integrità, non ripudio<br>– Concetto di segretezza<br>– Cifratura e decifratura<br>– Principio di Kerckhoffs<br>– Chiave<br>– Attacco bruteforce<br>– Complessità computazionale e fattore tempo<br>– Definizione di crittosistema<br>– Sicurezza perfetta di Shannon<br><br>Crittografia a chiave privata<br>– Crittosistema a chiave privata<br>– Condivisione della chiave e mancanza di non ripudiabilità<br>– Cifrari a trasposizione<br>– Permutazioni e permutazioni in espansione<br>– Cifrario a trasposizione colonnare<br>– Cifrario rail fence<br>– Cifrario a griglia<br>– Cifrari a sostituzione<br>– Cifrario di Cesare<br>– Cifrario di Vigenère<br>– Chiavi deboli in un cifrario<br>– Classificazione degli attacchi crittoanalitici<br>– Analisi delle frequenze<br>– Metodo Kasiski<br>– Metodo Friedman<br>– Cifrario di Vernam e sua segretezza perfetta<br>– Many time pad<br>– Confusione e Diffusione<br>– Cifrari a blocchi e a flusso<br>– Cifrari a flusso sincrono e cifrari a flusso autosincronizzanti<br>– S-box e P-box<br>– Modalità di funzionamento dei cifrari a blocchi: ECB, CBC, CFB, OFB, CTR<br>– Struttura di un cifrario a blocchi<br>– Reti di Feistel<br>– Cifrario DES<br>– Cifrario Triple DES<br>– Attacco meet in the middle<br>– Cifrario AES<br><br>Crittografia a chiave pubblica<br>– Three pass protocol<br>– Crittosistema a cifratura asimmetrica |

| | |
|---|---|
| | - Chiave pubblica e chiave privata<br>- Crittografia asimmetrica per la riservatezza<br>- Crittografia asimmetrica per l'autenticazione del mittente<br>- Crittografia asimmetrica per riservatezza e autenticazione del mittente<br>- Tempi e complessità computazionale<br>- Problema della fattorizzazione degli interi molto grandi<br>- Algoritmo RSA<br>- Elaborazione a blocchi dell'RSA<br>- Implementazione dell'esponenziazione modulare in RSA<br>- Timing attacks<br>- Crittografia omomorfica<br>- Attacco chosen ciphertext ad RSA<br>- Optimal Asymmetric Encryption Padding<br><br>Autenticazione dei messaggi e funzioni hash<br>- Funzioni hash<br>- Uniformità semplice<br>- Applicazioni delle funzioni hash<br>- Funzioni hash crittografiche<br>- Collisioni<br>- Paradosso del compleanno<br>- Attacco del compleanno<br>- Rainbow table<br>- Metodo del sale<br>- Costruzione di Merkle-Damgård<br>- MD5<br>- Famiglia SHA<br>- MAC<br>- Classi di falsificazione<br>- CBC-MAC<br>- OMAC/CMAC<br>- HMAC<br><br>Protocolli crittografici, gestione e distribuzione delle chiavi<br>- Definizione di protocollo crittografico<br>- Protocolli di secret sharing<br>- Shamir's Secret Sharing<br>- Attacco eavesdropping e attacco man in the middle<br>- Resistenza del Three pass protocol<br>- Problema del logaritmo discreto<br>- Protocollo di scambio delle chiavi Diffie-Hellman<br>- Algoritmo di cifratura ElGamal<br>- Firme digitali<br>- Firma digitale di ElGalam<br>- Firma digitale di Schnorr<br>- Firma digitale RSA<br>- Digital Signature Algorithm<br>- Collision attack su firma digitale<br>- Firma cieca<br>- Gestione e distribuzione delle chiavi<br>- Key Distribution Center<br>- Public announcement, Publicly available directory, Public Key Authority<br>- Certificati<br>- X.509<br>- Public Key Infrastructure<br>- Catene di certificati e cross-certification<br><br>Crittografia basata su curve ellittiche<br>- Curve ellittiche<br>- Curve ellittiche su campi finiti<br>- Logaritmo discreto su curve ellittiche |

| | |
|---|---|
| | - Elliptic Curve Diffie-Hellman<br>- Elliptic Curve Digital Signature Algorithm<br>- Secp256k1<br><br>Generazione di numeri pseudorancomici<br>- Casualità e pseudocasualità<br>- Proprietà dei numeri pseudorandomici<br>- Periodo dei generatori<br>- Linear Congruent Generators<br>- Generatori di Fibonacci ritardati<br>- Generatori basati su cifrari a blocchi<br>- ANSI X9.17<br>- Blum Blum Shub |
| **Testi di riferimento** | *William Stallings; Cryptography and Network security – Principles and practice Global edition – Seventh edition; Pearson*<br><br>Dispense del docente<br><br>Gli studenti che lo desiderano possono ottenere i testi in prestito dalla Biblioteca. Può convenire verificarne la disponibilità mediante il Sistema Bibliotecario di Ateneo https://opac.uniba.it/easyweb/w8018/index.php e contattare la biblioteca per concordare il prestito. |
| **Note ai testi di riferimento** | - |
| **Organizzazione della didattica** | |

| **Ore** | | | |
|---|---|---|---|
| Totali | Didattica frontale | Pratica (laboratorio, progetto, esercitazione, altro) | Studio individuale |
| 150 ore | 32 ore | 30 ore | 88 ore |
| **CFU/ETCS** | | | |
| 6 CFU | 4 CFU | 2 CFU | |

| | |
|---|---|
| **Metodi didattici** | |
| | Il corso viene erogato mediante lezioni frontali, nelle quali si analizzano teoricamente e praticamente i concetti legati al programma del corso. Vengono svolte esercitazioni pratiche, guidate dal docente, di applicazione dei concetti analizzati durante la didattica frontale. Le lezioni si svolgono in presenza. |
| **Risultati di apprendimento previsti** | |

| | |
|---|---|
| **Conoscenza e capacità di comprensione** | Lo studente acquisirà le competenze tali per la comprensione degli algoritmi e protocolli crittografici, dei problemi aperti relativi alla crittografia. Conoscerà il funzionamento nel dettaglio dei maggiori algoritmi e protocolli crittografici. |
| **Conoscenza e capacità di comprensione applicate** | Lo studente sarà in grado di applicare gli algoritmi crittografici presentati durante il corso, individuando quale tipologia di algoritmo o protocollo va applicata e quale implementazione specifica . |
| **Competenze trasversali** | *Autonomia di giudizio*<br>- Capacità di analisi individuale<br>- Comprensione delle peculiarità di ciascun elemento<br>- Capacità di valutazione critica rispetto alla situazione complessiva<br>- Visione d'insieme<br><br>*Abilità comunicative*<br>- Esprimere in forma corretta e completa i concetti<br>- Espressione delle conoscenze apprese tramite collegamenti con altre discipline o con applicazioni pratiche<br><br>*Capacità di apprendere in modo autonomo*<br>- Approfondimento individuale attraverso la ricerca<br>- Approfondimento di tematiche inerenti alla Crittografia |

| **Valutazione** | |
|---|---|
| **Modalità di verifica dell'apprendimento** | L'esame si svolge mediante una prova orale nella quale si analizza la competenza dello studente rispetto agli argomenti trattati.<br>Per gli studenti che lo desiderano, è possibile concordare con il docente la redazione di un approfondimento, espresso in forma scritta. Tale approfondimento sarà oggetto di valutazione integrativa e verrà presentato durante parte della prova orale. |
| Criteri di valutazione | *Conoscenza e capacità di comprensione:*<br>- Livello di completezza della conoscenza<br>- Livello di correttezza della conoscenza<br>- Livello di valutazione critica delle componenti crittografiche rispetto ai concetti chiave: chiavi e relativo spazio, riservatezza, integrità, disponibilità, non ripudio<br>- Livello di valutazione rispetto alle debolezze attaccabili tramite crittoanalisi<br>- Capacità di classificare correttamente un algoritmo o protocollo crittografico<br>- Corretto uso dei formalismi e conoscenza delle peculiarità formali dell'algoritmo/protocollo<br><br>*Conoscenza e capacità di comprensione applicate:*<br>- Capacità di contestualizzazione rispetto al problema specifico<br>- Individuazione della migliore soluzione per un problema sulla base delle disponibilità<br><br>*Autonomia di giudizio*:<br>- Capacità di giustificare le scelte<br>- Sostenere una tesi attraverso argomentazioni critiche, considerazioni<br>- Valutazione in prospettiva rispetto all'impatto di ciascuna scelta secondo i criteri di valutazione nell'ambito crittografico<br><br>*Abilità comunicative:*<br>- Completezza nell'esposizione<br>- Correttezza nell'esposizione<br>- Chiarezza nell'esposizione<br>- Efficacia nell'esposizione |

*Capacità di apprendere:*
- Livello di autonomia raggiunto
- Capacità di approfondimento

Comprensione del proprio livello di conoscenza

**Criteri di misurazione dell'apprendimento e di attribuzione del voto finale**

| Voto | Descrittori |
|---|---|
| < 18 insufficiente | Conoscenze frammentarie e superficiali dei contenuti, errori nell'applicare i concetti, descrizione carente. |
| 18 - 20 | Conoscenze dei contenuti sufficienti ma generali, descrizione semplice, incertezze nell'applicazione di concetti teorici. |
| 21 - 23 | Conoscenze dei contenuti appropriate ma non approfondite, capacità di applicare i concetti teorici, capacità di presentare i contenuti in modo semplice. |
| 24 - 25 | Conoscenze dei contenuti appropriate ed ampie, discreta capacità di applicazione delle conoscenze, capacità di presentare i contenuti in modo articolato. |
| 26 - 27 | Conoscenze dei contenuti precise e complete, buona capacità di applicare le conoscenze, capacità di analisi, descrizione chiara e corretta. |
| 28 - 29 | Conoscenze dei contenuti ampie, complete ed approfondite, buona applicazione dei contenuti, buona capacità di analisi e di sintesi, descrizione sicura e corretta. |
| 30<br>30 e lode | Conoscenze dei contenuti molto ampie, complete ed approfondite, capacità ben consolidata di applicare i contenuti, ottima capacità di analisi, di sintesi e di collegamenti interdisciplinari, padronanza di descrizione. |

## Altro

Si suggerisce agli studenti di affidarsi esclusivamente alle informazioni/comunicazioni fornite sui siti ufficiali del Dipartimento di Informatica, ovvero sui gruppi social solo se costituiti e amministrati esclusivamente dai docenti dei relativi insegnamenti:

- https://www.uniba.it/it/ricerca/dipartimenti/informatica/didattica/corsi-di-laurea/corsi-di-laurea
- https://www.uniba.it/it/ricerca/dipartimenti/informatica
- https://elearning.uniba.it/

I programmi degli insegnamenti sono disponibili qui:
- https://elearning.uniba.it/course/index.php?categoryid=455

Le informazioni che tutti gli studenti dovrebbero conoscere sono scritte nei Regolamenti didattici e manifesti degli studi disponibili nel sito:
- https://www.uniba.it/it/ricerca/dipartimenti/informatica/didattica/corsi-di-laurea/corsi-di-laurea

Si suggerisce agli studenti di diffidare delle informazioni e dei materiali circolanti su siti o gruppi social non ufficiali, poiché spesso sono risultati non affidabili, non corretti o incompleti. Per ogni dubbio, chiedere un incontro al docente secondo le modalità previste per il ricevimento.

L'accesso alle dispense del docente avviene mediante iscrizione alla pagina del corso su piattaforma di E-Learning. Al fine di stimolare la discussione sugli interrogativi posti durante il corso, le dispense vengono fornite dopo la lezione.