Principali informazioni sull'insegnamento	
Denominazione dell'insegnamento	**Crittografia**
Corso di studio	Sicurezza Informatica
Anno Accademico	AA 2023/24
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/i	
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 ADA - https://elearning.di.uniba.it/
Sito web del docente	https://islab.di.uniba.it
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 di base relative alla Matematica Discreta (Strutture algebriche, algebra modulare, generatori, calcolo combinatorio), al calcolo delle probabilità, alla Statistica, alla Teoria dei Linguaggi formali, alla complessità computazionale e alle reti di calcolatori
Contenuti di insegnamento (Programma)	Introduzione alla Crittografia - Riservatezza, autenticazione, integrità, non ripudio - Concetto di segretezza - Cifratura e decifratura - Principio di Kerckhoffs - Chiave - Attacco bruteforce - Complessità computazionale e fattore tempo - Definizione di crittosistema - Sicurezza perfetta di Shannon Crittografia a chiave privata - Crittosistema a chiave privata - Condivisione della chiave e mancanza di non ripudiabilità - Cifrari a trasposizione - Permutazioni e permutazioni in espansione - Cifrario a trasposizione colonnare - Cifrario rail fence - Cifrario a griglia - Cifrari a sostituzione - Cifrario di Cesare - Cifrario di Vigenère - Chiavi deboli in un cifrario - Classificazione degli attacchi crittoanalitici - Analisi delle frequenze - Metodo Kasiski - Metodo Friedman - Cifrario di Vernam e sua segretezza perfetta - Confusione e Diffusione - Cifrari a blocchi e a flusso - Cifrari a flusso sincrono e cifrari a flusso autosincronizzanti - S-box e P-box - Modalità di funzionamento dei cifrari a blocchi: ECB, CBC, CFB, OFB, CTR - Struttura di un cifrario a blocchi - Reti di Feistel - Cifrario DES - Cifrario Triple DES - Attacco meet in the middle - Cifrario AES Crittografia a chiave pubblica - Three pass protocol - Crittosistema a cifratura asimmetrica - Chiave pubblica e chiave privata

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

	– Curve ellittiche – Curve ellittiche su campi finiti – Logaritmo discreto su curve ellittiche – Elliptic Curve Diffie-Hellman – Elliptic Curve Digital Signature Algorithm – Secp256k1 Generazione di numeri pseudorancomici – Casualità e pseudocasualità – Proprietà dei numeri pseudorandomici – Periodo dei generatori – Linear Congruent Generators – Generatori di Fibonacci ritardati – Generatori basati su cifrari a blocchi – ANSI X9.17 – Blum Blum Shub
Testi di riferimento	*William Stallings; Cryptography and Network security – Principles and practice Global edition – Seventh edition; Pearson* Dispense del docente 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* o Capacità di analisi individuale o Comprensione delle peculiarità di ciascun elemento o Capacità di valutazione critica rispetto alla situazione complessiva o Visione d'insieme *Abilità comunicative* o Esprimere in forma corretta e completa i concetti o Espressione delle conoscenze apprese tramite collegamenti con altre discipline o con applicazioni pratiche *Capacità di apprendere in modo autonomo* o Approfondimento individuale attraverso la ricerca 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. 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:* o Livello di completezza della conoscenza o Livello di correttezza della conoscenza o Livello di valutazione critica delle componenti crittografiche rispetto ai concetti chiave: chiavi e relativo spazio, riservatezza, integrità, disponibilità, non ripudio o Livello di valutazione rispetto alle debolezze attaccabili tramite crittoanalisi o Capacità di classificare correttamente un algoritmo o protocollo crittografico o Corretto uso dei formalismi e conoscenza delle peculiarità formali dell'algoritmo/protocollo *Conoscenza e capacità di comprensione applicate:* o Capacità di contestualizzazione rispetto al problema specifico o Individuazione della migliore soluzione per un problema sulla base delle disponibilità

Autonomia di giudizio:
- Capacità di giustificare le scelte
- Sostenere una tesi attraverso argomentazioni critiche, considerazioni
- Valutazione in prospettiva rispetto all'impatto di ciascuna scelta secondo i criteri di valutazione nell'ambito crittografico

Abilità comunicative:
- Completezza nell'esposizione
- Correttezza nell'esposizione
- Chiarezza nell'esposizione
- 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 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.di.uniba.it/

I programmi degli insegnamenti sono disponibili qui:
- https://programmi.di.uniba.it/

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 ADA. Al fine di stimolare la discussione sugli interrogativi posti durante il corso, le dispense vengono fornite dopo la lezione.