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

INFO-01/A

## ANNO DI CORSO

II Anno

## TIPOLOGIA DI ATTIVITÀ FORMATIVA

/**/
Base q

Caratterizzante X
Affine q
Altre attività q

## NUMERO DI 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

Modulo 1 – Introduzione e fondamenti matematici

Il corso si apre con una panoramica storica della crittografia, dalle origini classiche ai sistemi contemporanei, mettendo in evidenza il passaggio da metodi empirici a una disciplina scientifica basata su modelli formali di sicurezza. Seguono i richiami di matematica discreta necessari per la comprensione degli algoritmi crittografici: aritmetica modulare, teoria dei numeri, congruenze, inversi modulari, teorema di Eulero. Vengono introdotti i concetti di probabilità discreta e distribuzioni uniformi, con applicazioni dirette al calcolo della sicurezza e alla generazione di chiavi.

Modulo 2 – Crittografia simmetrica

Viene approfondita la struttura dei cifrari a chiave segreta, a partire dai modelli teorici (cifrario di Vernam, one-time pad, cifrari a flusso e a blocchi). Si presentano i principi di confusione e diffusione, il ciclo di Feistel, e gli algoritmi di riferimento: DES, 3DES e AES. Sono trattate le modalità operative (ECB, CBC, CTR) e le loro implicazioni sulla sicurezza. Le esercitazioni mirano a sviluppare la capacità di interpretare schemi di cifratura e riconoscere vulnerabilità note.

Modulo 3 – Crittografia asimmetrica

Si introduce la nozione di chiave pubblica e privata, analizzando i fondamenti matematici di RSA, Diffie–Hellman e dei sistemi basati su logaritmi discreti. Vengono discusse le proprietà di sicurezza, la gestione delle chiavi, gli attacchi noti e le condizioni di correttezza. Particolare attenzione è rivolta ai concetti di trapdoor function e hard problem, che costituiscono la base formale della sicurezza asimmetrica.

Modulo 4 – Funzioni hash, generatori pseudocasuali e autenticazione

Il modulo approfondisce le principali componenti di sicurezza dei sistemi informatici moderni, ponendo in relazione la generazione di casualità, l'integrità dei dati e i meccanismi di autenticazione. Si studiano le funzioni hash crittografiche (MD5, SHA-1, SHA-2, SHA-3) e le loro proprietà di resistenza all'inversione e alla collisione, evidenziandone l'uso in firme digitali, autenticazione e gestione delle password. Viene analizzata la generazione di numeri pseudocasuali, distinguendo tra casualità vera e pseudocasualità, e illustrando algoritmi come i Linear Congruential Generators e il Blum–Blum–Shub. Segue lo studio delle tecniche di autenticazione e integrità dei messaggi (MAC, HMAC) e dei principali schemi di firma digitale (RSA, DSA, ECDSA), fino alla trattazione dei certificati digitali e delle infrastrutture a chiave pubblica (PKI). Il modulo si conclude con un'introduzione alla gestione dei certificati X.509 e ai meccanismi di validazione delle identità digitali.

Modulo 5 – Applicazioni, protocolli e scenari avanzati

Il corso si conclude con una panoramica dei principali protocolli crittografici di rete (TLS, SSL, IPSec) e delle loro componenti di sicurezza. Sono discussi casi d'uso reali, esempi di fallimenti crittografici e principi di crypto-agility. Un approfondimento finale è dedicato alla legislazione, all'etica e alla gestione della sicurezza, con riferimento ai contesti di cybersecurity applicata e alle minacce emergenti, incluse le prospettive della crittografia post-quantistica.

## Modulo 6 – Interviste ed esperienze dal settore (attività integrativa trasversale)

### Elenco videolezioni

Ecco l'elenco numerato delle lezioni di Crittografia Avanzata e Sicurezza, pulito da ogni riferimento tecnico ai percorsi di sistema e codici:

Introduzione alla crittografia

Elementi di Probabilità discreta

One-Time Pad e la Sicurezza Perfetta

Generatori Pseudocasuali e Cifrari a Flusso

La Sicurezza dei Generatori Pseudocasuali

Cifrari a Blocchi

Attacchi su Cifrari a Blocchi: 3DES e AES

Modalità di funzionamento

Scambio di chiavi

Introduzione all'aritmetica modulare

Radici modulari e problemi difficili

Crittografia asimmetrica

RSA

Firme Digitali

PKI

Certificati X.509

Hash Functions

Curve ellittiche

Transport Layer Security (TLS)

Attacchi Man-in-the-Middle

Blockchain

Crittografia Quantistica

Password Cracking

Malware Analysis e Crittografia

Crittografia e PA

Zero Trust, Data Warehouse e Intelligenza Artificiale

Applicazione dei principi di sicurezza informatica presso l'Ospedale Pediatrico Bambino Gesù

Cybersicurezza e nuove fattispecie penali: la Legge 90/2024

## TIPOLOGIE DI ATTIVITÀ DIDATTICHE PREVISTE E RELATIVE MODALITÀ DI SVOLGIMENTO

/**/
L’insegnamento è articolato in videolezioni di circa 30 minuti corredate da dispense, slide e questionario di autovalutazione.

Per ogni insegnamento è prevista1 videolezione di didattica erogativa in modalità sincrona a contenuto innovativo ed interattivo, secondo modalità definite dal docente di riferimento,vi è altresì la possibilità di redazionedi un elaborato per insegnamento, differenziato in termini di difficoltà rispetto all’ampiezza dei CFU assegnati.

Il modello didattico 2025-2026, in ottemperanza al D.M. 1835 del 6 dicembre 2024, prevede di norma, per ogni CFU, un totale di almeno 7 ore di didattica. La didattica erogativa è perciò effettuata dall’Anno Accademico 2025/2026 per l’80% in modalità asincrona, articolata in un numero di videolezioni coerente ai CFU complessivi del singolo insegnamento, corredate da materiale didattico adeguato allo studio individuale e, per almeno il 20%, in modalità sincrona

La didattica erogativa asincrona prevede per ogni ora una videolezione registrata, una dispensa corredata da riferimenti bibliografici, note, tabelle, immagini, grafici ed un questionario di dieci domande di autovalutazione con quattro possibili risposte di cui solo una corretta e tre distrattori, oltre un file di riepilogo relativo agli obiettivi ed alla struttura in paragrafi della lezione, con l’aggiunta di alcune parole chiave. Nel dettaglio la videolezione corrisponde alla singola lezione teorica del docente.La didattica sincrona si compone di una web conferenze per CFU e di un elaborato per insegnamento, differenziato in termini di difficoltà rispetto all’ampiezza dei CFU assegnati.L’obiettivo della didattica erogativa in modalità sincrona è assicurare tutte quelle attività che tipicamente richiedono apprendimenti “in situazione” o rapporto “face to face”, quali laboratori, seminari, esperienze sul campo, tirocini, ecc., tenendo conto anche delle metodologie a carattere innovativo e volte a favorire l’interazione docente-studenti e tra studenti

Sono previsti:

interventi didattici rivolti da parte del docente/tutor all’intera classe (o a un suo sottogruppo), tipicamente sotto forma di dimostrazioni o spiegazioni aggiuntive (ad esempio dimostrazione o suggerimenti operativi su come si risolve un problema, esercizio esimilari); gli interventi brevi effettuati dai corsisti (ad esempio in ambienti di discussione o di collaborazione); le e-tivity strutturate (individuali o collaborative), sotto forma tipicamente di report, esercizio, studio di caso, problem solving, web quest,progetto,produzionediartefatto(ovariantiassimilabili),effettuati dai corsisti, con relativo feed-back; le forme tipiche di valutazione formativa, con il carattere di questionari o test initinere; le esperienze di apprendimento in situazione realizzabili attraverso ambienti di simulazione, oppure attraverso la virtualizzazione di laboratori didattici.
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.

Nel computo delle ore della didattica erogativa sono escluse le interazioni a carattere orientativo sui programmi, sul Corso di Studio, sull’uso della piattaforma e simili, che rientrano nei servizi di tutoraggio per l’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 erogativa 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 la verifica 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 per verificare la capacità di apprendimento ovvero il livello di apprendimento raggiunto dallo studente. 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 studenti che avranno luogo durante la fruizione del corso proposte dal docente o dal tutor.

## CRITERI DI MISURAZIONE DELL'APPRENDIMENTO E ATTRIBUZIONE DEL VOTO FINALE

/**/
La didattica sincrona garantisce una premialità massima di 2 punti che si somma al voto dell'esame finale, suddivisa in 1 punto per la didattica erogativa sincrona (Webconference) ed 1 punto didattica erogativa sincrona (Elaborato). La premialità massima per le Webconference è di un punto sul voto di esame. Ogni studente può partecipare a tutte le Webconference erogate.  Per ciascuna di esse, il superamento del test finale di apprendimento –che richiede almeno quattro risposte corrette su cinque domande relative al tema trattato – consente di ottenere un punteggio pari a 0,5. Una volta raggiunto un punteggio totale di 1, allo studente viene riconosciuta la premialità. La redazione dell'elaborato consente una premialità pari ad 1 punto sul voto dell'esame, se considerato sufficiente. Saranno rese disponibili due tracce di elaborati.

È data facoltà allo studente di partecipare alla didattica erogativa sincrona.

La valutazione finale ha lo scopo di misurare il grado di comprensione delle nozioni teoriche e la capacità di sviluppare il ragionamento utilizzando le nozioni acquisite per verificare la capacità di apprendimento ovvero il livello di apprendimento raggiunto dallo studente. 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 ottenuto nella verifica di profitto al quale si sommano le premialità che lo studente può aver ottenuto partecipando alla didattica erogativa sincrona e deriva, quindi, dalla somma delle due valutazioni. Il voto derivante dalla didattica sincrona 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 ed anche all'ultima domanda.

## ATTIVITÀ DI DIDATTICA EROGATIVA ASINCRONA

Di norma massimo l’80% delle lezioni è svolto in modalità asincrona.

## ATTIVITÀ DI DIDATTICA EROGATIVA SINCRONA CON RELATIVO FEED-BACK AL SINGOLO STUDENTE DA PARTE DEL DOCENTE O DEL TUTOR

Almeno il 20% delle lezioni è svolto in modalità sincrona e possono prevedere:

èPartecipazione web conference

èRedazione di un elaborato

èSvolgimento delle prove in itinere con feedback

èSvolgimento della simulazione del test finale

## MATERIALE DIDATTICO UTILIZZATO

èVideolezioni

èDispense predisposte dal docente e/o slide del docente

èQuestionario di autovalutazione

èMateriali predisposti per le lezioni sincrone

èTesto 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.

## OBIETTIVI

/**/
Il corso Principi e Metodi di Crittografia ha l’obiettivo di introdurre i fondamenti teorici e pratici della crittografia moderna. Gli studenti apprendono il funzionamento delle principali primitive crittografiche, dai cifrari simmetrici e asimmetrici alle funzioni hash e ai protocolli di autenticazione. Il corso sviluppa la capacità di analizzare e valutare la sicurezza degli algoritmi in base a modelli formali e probabilistici. Particolare attenzione è dedicata all’uso corretto degli strumenti crittografici e alla comprensione delle loro applicazioni reali nella sicurezza dei sistemi informatici.