Ministero delle Imprese e del Made in Italy

DIPARTIMENTO PER IL DIGITALE, LA CONNETTIVITÀ E LE NUOVE TECNOLOGIE
DIREZIONE GENERALE PER IL DIGITALE E LE TELECOMUNICAZIONI -
ISTITUTO SUPERIORE DELLE COMUNICAZIONI E DELLE TECNOLOGIE DELL'INFORMAZIONE
DIVISIONE I
SCUOLA SUPERIORE DI SPECIALIZZAZIONE IN TELECOMUNICAZIONI

PROGRAMMA

Anno accademico 2026/2027

Corso di **TELEFONIA E TELEGRAFIA**

Modulo di **NETWORK PROGRAMMABILITY**

Ore previste: **30**

OBIETTIVI DEL CORSO

Il modulo mira ad introdurre le tecnologie e le tecniche abilitanti alla creazione di una rete programmabile, sia sui piani di gestione e controllo che sul piano dei dati. Inoltre, viene fornita una panoramica dei casi d'uso più rilevanti che beneficiano della (o che sono abilitati dalla) disponibilità delle reti programmabili.

PROGRAMMA

- Richiami di networking
  - architettura di rete
  - metriche prestazionali
  - modello ISO/OSI
- Network Automation
  - NETCONF e RESTCONF
  - Data Modeling Languages e YANG
  - esempi applicativi
- Control Plane Programmability
  - Software Defined Networking
  - Openflow
  - esempi applicativi
- Network Softwarization
  - ETSI use cases
  - Network Function Virtualization
  - NFV placement
  - Service Function Chaining e Network Service Header
  - SRv6
- Data Plane Programmability
  - Programmable Devices
  - P4 Language
  - esempi applicativi

Modulo di	**SICUREZZA NELLE COMUNICAZIONI**
Ore previste:	**20**

OBIETTIVI DEL CORSO	*Il modulo mira a fornire gli elementi concettuali e tecnici di base per la comprensione dello stato dell'arte nelle comunicazioni sicure, a definire la terminologia tecnica relativamente agli elementi introduttivi di crittografia e protocolli di comunicazione sicuri ed a fornire elementi di base sulla valutazione della sicurezza di algoritmi e protocolli.*
PROGRAMMA	• Introduzione alla sicurezza nelle comunicazioni • Introduzione alla crittografia • Primitive crittografiche: cifratura e autenticazione di messaggio a chiave simmetrica • Cifratura e autenticazione di messaggio a chiave pubblica (RSA). Cenno alla crittografia basata sulle curve ellittiche. • Cenni sulla crittografia Post-Quantum. • Autenticazione: autenticazione di identità, autenticazione su base indirizzo, terze parti, deleghe, token di sicurezza, identity providers. • Protocolli crittografici: caratteristiche principali e attacchi, protocolli di autenticazione: sfida-risposta, Needham-Schroeder, protocolli di autenticazione e scambio chiavi (instaurazione di un canale sicuro): Diffie-Hellman autenticato. • Password: definizioni, attacchi, inizializzazione e gestione, protocolli di autenticazione su base password: Lamport hash, EKE, SRP. • IPSec e IKE

Modulo di	**CODIFICA E AFFIDABILITÀ**
Ore previste:	**20**

OBIETTIVI DEL CORSO	*Il modulo si prefigge di riassumere le basi di telecomunicazioni e l'acquisizione degli elementi base della protezione dell'informazione e impatto a livello di sistema.*
PROGRAMMA	• Scenari Evolutivi delle TLC Sistemi di accesso cablato e wireless Sistemi cellulari e comunicazioni a corto raggio (NFC, Bluetooth) Radio Cognitiva • Il problema della codifica di sorgente Sorgenti discrete stazionarie senza memoria Compressione ottima secondo Huffman Sorgenti discrete e stazionarie con memoria Sorgenti di Markov • Il problema della codifica di canale e la contrapposizione tra affidabilità e velocità trasmissiva Codifica a Blocchi Decodifica MV Decodificatore a Sindrome • Codifica convoluzionale. Utilizzo del meccanismo di memoria Algoritmo di Viterbi in modalità Hard e Soft. Interleaving

	• Meccanismo ARQ per la protezione da errori. Protocolli Stop and Wait, Go Back m, selective repeat Modulazioni numeriche. Modulazioni PAM e QAM • Modulazione OFDM nella versione analogica e digitale Schemi di accesso a suddivisione di canale. TDMA, FDMA e CDMA Schemi di accesso a contesa: Slotted Aloha e CSMA nelle versioni Collision Detection e Collision Avoidance

Corso di	**RADIOTELEGRAFIA E RADIOTELEFONIA**
Modulo di	**ANALISI DEL FUNZIONAMENTO DEI MODERNI SISTEMI RADIOMOBILI**
Ore previste:	**30**

OBIETTIVI DEL CORSO	*Obiettivo del modulo è quello di fornire una descrizione dei concetti generali e delle metodologie alla base dell'analisi del funzionamento dei moderni sistemi radiomobili. Nella presentazione degli argomenti trattati si focalizza l'attenzione sui problemi generali riguardanti la realizzazione di un moderno sistema radiomobile. Per ciascuno dei problemi analizzati sono descritte le relative soluzioni implementate nei sistemi 4G, 5G e nei futuri sistemi 6G. I principali argomenti presentati nel corso riguardano: 1. l'analisi delle architetture delle moderne reti radiomobili; 2. il problema di ottimizzazione del throughput mediante tecniche di caching e di edge cloud computing; 3. l'organizzazione delle moderne reti radiomobili con particolare riferimento ai sistemi 4G LTE e 5G.*

PROGRAMMA	• Concetti generali sui sistemi radiomobili e visione di alto livello. Organizzazione cellulare della sezione di accesso. Concetto di cluster e tecniche di settorizzazione. Parametri che qualificano le prestazioni di un sistema radiomobile
	• Gestione della mobilità e funzionalità di handover. I servizi radiomobili e loro evoluzione. Distinzione tra servizi portanti e teleservizi. Importanza dei nuovi servizi basati sulla trasmissione dati. La classificazione ITU dei servizi introdotta per il 5G
	• I moderni sistemi radiomobili: concetti generali. Evoluzione della rete di accesso radio orientata al miglioramento della efficienza spettrale di sistema. Problema della latenza nei sistemi radiomobili. Architetture di rete di accesso a salto singolo o salto multiplo, reti mesh e loro impieghi nelle moderne reti di accesso radio
	  ○ La formula della capacità di Shannon e sue implicazioni nel progetto delle moderne reti di accesso via radio. Uso efficiente dello spettro radio. Concetto di spectrum sharing per le reti di nuova generazione
	  ○ Le reti di accesso di tipo eterogeneo. Dispiegamento di una rete eterogenea. I capacity boosters. Micro, pico e femtocelle. Tecniche per la gestione della interferenza: ICIC, eICIC e note sul COMP
	• MIMO. Concetti Generali. Tipologie di MIMO: SU-MIMO, MU-MIMO e Massive MIMO
	• Evoluzione delle architetture delle reti radiomobili: dalla RAN passando per la Cloud RAN fino alla OpenRAN
	• Concetti di: QoS, QoE e TCP Throughput (Formula di Matis). Uso di piattaforme di QoE per il miglioramento delle prestazioni nelle moderne reti di Telecomunicazione. Lo Edge Cloud Computing e il Multi Access Edge Computing
	• Evoluzione dei sistemi radiomobili. Dal 2G al 4G passando per il 2.5G e il 3G
	• Il sistema 4G LTE
	  ○ Architettura generale ed entità funzionali: eNB ed EPC. Separazione delle funzionalità del piano di controllo (MME, PCRF, P-GW etc.) e di utente e sue implicazioni (S-GW, P-GW)

	○ Architettura protocollare del LTE: piano di controllo e piano di utente. Concetto di EPS bearer. Descrizione di dettaglio delle funzionalità di alcuni strati protocollari del sistema LTE ○ Interfaccia radio del LTE: OFDM e SC-FDMA. Cenni sulla tecnica OFDM. Assegnazione delle risorse nel LTE: il physical resource block (PRB) e il resource block (RB). Valutazione del data rate ottenibile sulla interfaccia radio LTE • Brevi cenni sul 5G: percorso di standardizzazione e stato attuale dello sviluppo. Architettura di rete 5G ed elementi che realizzano i piani di utente e di controllo. Confronto architettura di rete 4G e 5G e innovazioni introdotte nel 5G. Descrizione di dettaglio della interfaccia radio del 5G: lo Scalable-OFDM e numerologia

Modulo di	**LTE, LTE AVANZATO E 5G**
Ore previste:	**10**
OBIETTIVI DEL CORSO	*Obiettivo del modulo è quello di fornire una presentazione dei sistemi radiomobili di 4ª e 5ª generazione, di descrivere le tecniche realizzate per ottenere elevato data rate e connettività di molti dispositivi contemporaneamente e le tecniche per ottenere una bassa latenza.*
PROGRAMMA	• LTE (completamento) ○ Tecnica Orthogonal Frequency Division Multiplexing (OFDM) ○ Accesso multiplo e Strato fisico LTE parte 1 (physical resource block, organizzazione della trama) ○ Strato fisico LTE parte 2 (canali fisici/trasporto, procedure di trasmissione dati) ○ Strati MAC, RLC e PDCP ○ Strato RRC e cenni sul NAS ○ Esempio di procedura Initial Attach • LTE ADVANCED ○ Tecnica MIMO ○ Carrier Aggregation ○ Small Cell ○ Dual Connectivity • Introduzione al 5G ○ Use case del 5G e visione architetturale ○ Tecnologie principali del 5G ○ Architettura: dual connectivity, Network slicing, radio cloud edge computing ○ Strato fisico 5G (new radio e numerology), innovazioni sull'interfaccia radio 5G (minislot, self-contained frame, canali di controllo

Corso di	**COMMUTAZIONE E SEGNALAZIONE**

Modulo di	**CONFIGURAZIONE E GESTIONE RETI TCP/IP**
Ore previste:	**30**

OBIETTIVI DEL CORSO	*L'obiettivo formativo del modulo è quello di fornire allo studente le conoscenze teoriche e pratiche (basate su Linux) di networking TCP/IP che gli permettano di gestire e progettare ambienti d'ufficio centralizzati o distribuiti (smart working).*
PROGRAMMA	• Richiami TCP/IP, indirizzamento e forwarding • Configurazione sperimentale ed analisi di reti IP su Linux in ambiente GNS3 • Teoria e laboratorio dei servizi di Network Address Translation (DNAT, SNAT) e DHCP • Teoria e laboratorio dei servizi di DNS • Teoria e laboratorio dei servizi di Proxy (forward, reverse) • Richiami Sicurezza TLS • Teoria e laboratorio di Virtual Private Networks basate su TLS

Modulo di	**FONDAMENTI RETI IP**
Ore previste:	**20**

OBIETTIVI DEL CORSO	*Il corso ha l'obiettivo di insegnare il funzionamento delle reti IP analizzando il comportamento nei principali livelli OSI, dallo strato fisico a quello di trasporto. In particolare, si analizzeranno le reti Ethernet, i processi di routing, la gestione della qualità dell'informazione sino alla valutazione delle prestazioni. Il corso verrà inquadrato nell'ambito delle ultime metodologie delle reti basate sui paradigmi SDN e NFV a supporto delle reti 5G*

PROGRAMMA	• Introduzione alle reti IP
	  ○ Dalle reti NGN alle reti 5G
	  ○ Criteri SDN e NFV
	  ○ Il modello OSI
	• OSI Layer 1
	  ○ Dal PDH a SDH
	  ○ OTN
	• OSI Layer2
	  ○ 802.3
	  ○ Reti Ethernet, GbE
	  ○ Switch, Spanning Tree
	  ○ Virtual LAN
	• OSI Layer3
	  ○ Protocollo IP, struttura del pacchetto
	  ○ ICMP
	  ○ Ping e traceroot
	• Indirizzamento e routing
	  ○ NAT, DHCP, supernatting

- Cenni BGP e EGP
- OSI Layer 4
  - TCP e UDP
- TCP
  - Controllo d'errore, fast retransmit
  - Controllo di flusso e congestione
  - Principali TCP (Tahoe, Rino, New Rino, Cubic)
- IP mobile
- Cenni IPv6
- Prestazioni reti IP
  - Cenni Intserv e Diffserv
  - QoS, throughput
  - Misura QoS, multisessione
- Cenni di servizi su IP (SIP, IMS, VoLTE)
- Dal routing distribuito a quello centralizzato
  - Reti SDN-NFV
  - La rete core 5G
- Cenni di intelligenza artificiale nelle reti
  - Modelli 3GPP, O-RAN, ETSI

Corso di	**ENERGETICA E PROBLEMI DI TERMODINAMICA**

Modulo di	**ENERGETICA**
Ore previste:	**20**

OBIETTIVI DEL CORSO	*Il modulo si prefigge l'obiettivo di presentare il quadro attuale del settore energetico nazionale ed internazionale con l'individuazione a livello nazionale del quadro normativo, dei meccanismi di regolazione ed incentivazione previsti nel settore delle energie rinnovabili e dell'efficienza energetica.*
PROGRAMMA	• Il quadro normativo • Le diagnosi energetiche • Data center • I meccanismi di incentivazione • Il meccanismo dei titoli di efficienza energetica • Il conto termico • Casi studio e applicazioni pratiche • Impianti a fonti rinnovabili • Interventi di efficientamento energetico • Bilancio di sostenibilità • Analisi delle emissioni dei gas climalteranti • Footprint Scope 1, Scope 2, Scope 3

Corso di	**IMPIANTI DI TLC**

Modulo di	**SISTEMI E RETI WIRED**
Ore previste:	**20**

OBIETTIVI DEL CORSO	*Il corso ha l'obiettivo di insegnare il funzionamento completo delle reti in fibra ottica con cenni a quelle in doppino telefonico. In particolare, il corso partirà dai sistemi ottici, con cenni sul trasmettitore e sul ricevitore, e si analizzeranno le prestazioni dei sistemi (sia IM-DD che coerenti, singolo canale e WDM).* *Particolare attenzione verrà data alle reti di accesso ottiche (FTTx, PON) e alla loro integrazione con le reti 5G. Cenni sul funzionamento dei sistemi su lunga distanza e sottomarini.* *Verranno quindi mostrate le nuove frontiere delle comunicazioni e delle elaborazioni ottiche basate sugli aspetti quantistici. Verranno quindi illustrati i concetti base della meccanica quantistica, il funzionamento alla base dei calcolatori quantistici. Verranno invece approfondite le comunicazioni quantistiche con particolare attenzione agli aspetti della sicurezza quantistica con la tecnica Quantum Key Distribution.* *Verranno inoltre accennate le tecniche Post Quantum CriptographY.*

PROGRAMMA	• Introduzione ai sistemi ottici.
	  ○ Shannon
	  ○ Reti ottiche
	• Sistemi IM-DD
	  ○ Rumore Shot e termico
	  ○ Calcolo probabilità di errore, fattore Q
	  ○ Amplificatore ottico e limite quantico
	• Cenni sistemi coerenti
	  ○ FSK, PSK, ASK
	  ○ M-QAM
	  ○ OFDM
	• Sistemi Sub-Carrier Multiplexing
	  ○ CATV
	• Sistemi Free Space Optics (FSO)
	  O Accesso e satelliti
	• Sistemi xDSL
	  ○ Cenni ai sistemi in doppino telefonico
	• Reti di accesso
	  ○ FTTx
	  ○ PON, EPON, GPON, WDM-POB
	  ○ Costi rete di accesso
	  ○ Reti ottiche per 5G (Backhauling, FrontHauling)
	• Reti di Edge e core
	  ○ OXC, OADM
	• Sicurezza reti ottiche
	  ○ Attacchi in reti ottiche
	• Comunicazioni e sicurezza quantistica
	  ○ Concetti base sulle comunicazioni quantistiche

	○ Computer quantistico ○ Crittografia quantistica ○ Quantum Key Distribution (QKD) ○ Esempi di reti QKD nel mondo ○ Crittografia Post-Quantum

Corso di	LEGISLAZIONE ED ECONOMIA

Modulo di	**DIRITTO E POLITICHE DEL CYBERSPAZIO PER LA SICUREZZA NAZIONALE**
Ore previste:	**15**

OBIETTIVI DEL CORSO	*L'obiettivo è quello di fornire ai partecipanti una overview completa delle principali normative europee e nazionali in materia di cybersecurity.*
PROGRAMMA	• La Direttiva NIS 2 ▪ Dalla Direttiva NIS alla Direttiva NIS 2 ▪ La Direttiva NIS 2 e le richieste del legislatore europeo ▪ Il D.lgs. 138/2024 e gli obblighi di *compliance* discendenti dal Decreto di recepimento della Direttiva NIS 2 in Italia • Il Cybersecurity Act e il Cyber Resilience Act ▪ Il quadro europeo di certificazione della cybersicurezza ▪ Il (futuro) quadro giuridico sui requisiti essenziali di cybersicurezza per l'immissione sul mercato di prodotti con elementi digitali ▪ L'interazione tra le due normative • La Direttiva CER ▪ La resilienza dei soggetti critici nella fornitura dei servizi essenziali ▪ La Direttiva UE 2022/2557 e gli obblighi imposti a livello europeo ▪ Il D.lgs. 134/2024 di recepimento in Italia della Direttiva CER e gli obblighi di *compliance* • Il Perimetro di Sicurezza Nazionale Cibernetica (PSNC) ▪ Gli obiettivi del legislatore italiano ▪ L'impianto normativo a tutela della sicurezza nazionale ▪ I principali obblighi di *compliance* • La Legge 90/2024 sulla Cybersicurezza ▪ Il ruolo e le richieste normative alle Pubbliche Amministrazioni ▪ Il ruolo e le richieste normative per i soggetti ricompresi nel Perimetro di Sicurezza Nazionale Cibernetica, per quelli sottoposti alla Direttiva NIS e per quelli Tel.Co. ▪ L'impatto sui contratti pubblici di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici

Modulo di	**LIBERALIZZAZIONE ED ECONOMIA DELLE TLC**
Ore previste:	**10**

OBIETTIVI DEL CORSO	*Il modulo si prefigge l'obiettivo di ripercorrere gli eventi storici, da un punto di vista normativo e degli effetti di questi sul mercato, che hanno portato alla liberalizzazione delle TLC, dal monopolio di fine anni '80 al libero mercato dei giorni nostri, con particolare attenzione al Codice delle Comunicazioni Elettroniche del 2003 e delle sue successive modifiche.* *Vengono inoltre forniti elementi di valutazione di progetti (business planning) e di analisi di bilanci privatistici con particolare riferimento al mondo delle TLC, analizzando casi ed applicazioni reali.*

PROGRAMMA	• Dal monopolio alla concorrenza: storia della liberalizzazione delle TLC in Italia
	  ○ Le fasi della liberalizzazione, dalla fine degli anni '80 ad oggi
	  ○ Il Codice delle Comunicazioni Elettroniche
	  ○ Il listino di interconnessione ed il mercato concorrenziale: evoluzione e regolamentazione
	• Tecniche di stesura di un business plan
	  ○ Metodologie ed obiettivi
	  ○ Principali indicatori (VAN, TIR, PBT, PF)
	  ○ Applicazione alle TLC: banda larga ed ultralarga
	• Analisi di un bilancio privatistico
	  ○ Struttura di un bilancio, stato patrimoniale, conto economico, flussi di cassa
	  ○ Indicatori di bilancio
	  ○ Applicazione alle TLC: analisi di un bilancio reale di un Operatore
	  ○ Confronto tra indicatori, applicazioni a casi reali

Modulo di	**LEGISLAZIONE IN MATERIA DI SICUREZZA DELLE RETI DI TELECOMUNICAZIONE IN TECNOLOGIA 5G**
Ore previste:	**10**

OBIETTIVI DEL CORSO	*Il modulo si prefigge l'obiettivo di fornire un quadro generale della normativa europea e italiana in materia di sicurezza delle reti in tecnologia 5G.*

PROGRAMMA	• Cenni sulle caratteristiche reti in tecnologia 5G
	• Art. 1-bis del DL 21/2012: Poteri speciali inerenti le reti di telecomunicazione elettronica a banda larga con tecnologia 5G
	• Raccomandazione (UE) 2019/534 – Sicurezza cyber delle reti 5G
	  ○ Risk assessment europeo sulle reti 5G
	  ○ Toolbox di misure di sicurezza per le reti 5G
	• Il ruolo del Centro di Valutazione e Certificazione Nazionale nella sicurezza delle reti 5G
	• Comunicazione congiunta del Parlamento Europeo e del Consiglio del 16 dicembre 2020: la strategia di cybersicurezza dell'UE per il decennio digitale

	• Art. 14 della Legge 28 giugno 2024, n. 90 e Decreto Del Presidente Del Consiglio Dei Ministri 30 aprile 2025 "*Disciplina dei contratti di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici e della sicurezza nazionale*".

Modulo di	**CODICE EUROPEO DELLE COMUNICAZIONI ELETTRONICHE – Contenuti normativi**
Ore previste:	**5**
OBIETTIVI DEL CORSO	*Il programma intende offrire un quadro aggiornato della disciplina delle comunicazioni elettroniche, tenendo conto delle principali novità conseguenti all'evoluzione del quadro europeo di riferimento e alla relativa attuazione interna*
PROGRAMMA	• La disciplina europea delle comunicazioni elettroniche • L'ambito nazionale: l'adeguamento alla disciplina comunitaria ○ Tipologie di provvedimenti autorizzatori e nuove procedure autorizzatorie, alla luce degli innovativi principi di efficienza, effettività ed equa ripartizione dello spazio elettromagnetico e degli istituti di semplificazione procedimentale)

Modulo di	**CODICE EUROPEO DELLE COMUNICAZIONI ELETTRONICHE – Regolazione e tutela nei servizi di comunicazione elettronica: sanzioni amministrative e protezione dei minori nel contesto digitale**
Ore previste:	**10**
OBIETTIVI DEL CORSO	*Fornire un quadro aggiornato delle sanzioni amministrative in materia di comunicazioni elettroniche alla luce delle modifiche introdotte dal D.lgs. 207/2021 e dal D.lgs. 48/2024.* *Approfondire i profili normativi e operativi connessi alla tutela dei minori online, in particolare nella prevenzione e contrasto della pedopornografia, del bullismo e del cyberbullismo.*
PROGRAMMA	• Il nuovo assetto regolatorio delle comunicazioni elettroniche in Italia • Le novità in materia di sanzioni amministrative: poteri, procedimenti, criteri di proporzionalità • Il ruolo e le funzioni del MIMIT • Tutela dei minori online: normativa nazionale e internazionale • Responsabilità e strumenti di contrasto a bullismo e cyberbullismo • Approfondimenti su casi concreti, simulazioni e scenari operativi

Modulo di	**L'EVOLUZIONE DEL SISTEMA RADIO TELEVISIVO ITALIANO: ASPETTI NORMATIVI E TECNICI**
Ore previste	**5**

OBIETTIVI DEL CORSO	*L'obiettivo del modulo è quello di fornire una panoramica dell'attuale stato del sistema radio televisivo italiano, ripercorrendo, sia dal punto di vista normativo che dal punto di vista tecnico, la storia dell'evoluzione del comparto con particolare riferimento ai diversi processi di transizione che, a partire dai primi anni '90, hanno determinato il definitivo passaggio dal sistema analogico a quello digitale, per quanto attiene al comparto televisivo, ed hanno avviato il processo di digitalizzazione del comparto radiofonico.*

PROGRAMMA	• Il settore televisivo nazionale e locale
	  ○ Stato del sistema fino agli anni '90
	  ○ Il sistema dagli anni '90 ai primi anni 2000
	  ○ Inquadramento normativo
	• La transizione alla televisione digitale terrestre (lo switch-off)
	  ○ Motivi e storia della transizione
	  ○ Inquadramento normativo
	• L'evoluzione del sistema televisivo
	  ○ Le reti mobili e la liberazione della banda a 700 MHz
	  ○ La realizzazione del Piano Nazionale di Assegnazione delle Frequenze (PNAF)
	  ○ Inquadramento normativo
	• Il settore radiofonico nazionale e locale
	  ○ Evoluzione del sistema
	  ○ Il processo di digitalizzazione (il DAB)
	  ○ Inquadramento normativo

Corso di	**PRINCIPI DI INFORMATICA APPLICATA ALLE TLC**

Modulo di	**INTRODUZIONE ALLA CYBER SECURITY DEI SISTEMI OT**
Ore previste	**20**

OBIETTIVI DEL CORSO	*Il modulo si prefigge l'obiettivo di fornire ai discenti una panoramica delle principali problematiche in tema di cyber security con particolare riferimento alle Operational Technologies (OT) ed ai sistemi di Intelligenza Artificiale*

PROGRAMMA	• Cosa è la cyber security
	  ○ Definizioni e obiettivi
	  ○ Motivazioni e Trend
	  ○ Principali modalità di attacco
	  ○ Disamina delle minacce: cyber crime, spionaggio, APT, cyberwar
	  ○ Intelligenza Artificiale e Cybersecurity: bias, allucinazioni e tecniche di prompt injection
	• Introduzione alle Operational Technologies.
	  ○ Principi di funzionamento, architetture, protocolli e prodotti
	  ○ Peculiarità dei sistemi OT
	  ○ Analisi delle problematiche cyber per sistemi OT ed illustrazione di casi esemplificativi di attacco cyber
	• Contromisure
	  ○ Elementi di valutazione del rischio (CVE, CVSS)
	  ○ Principi di cyber security
	  ○ Il paradigma Zero Trust
	  ○ L'utilizzo delle tecniche OSINT
	  ○ Cenni sulle direttive CER (D.lgs. 134/24) e NIS2(D.lgs. 138/24)

Modulo di	**ATTACCHI CRITTOGRAFICI E BLOCKCHAIN**
Ore previste	**30**

OBIETTIVI DEL CORSO	*Il modulo ha l'obiettivo di coprire tre macro-argomenti: i)* ***crittografia applicata****, con specifica attenzione alle modalità di applicazione degli algoritmi crittografici ed agli errori da evitare nell'integrazione della crittografia nei sistemi; ii)* ***protocolli per la sicurezza delle comunicazioni****, con approfondimento specifico sul protocollo TLS e sui relativi attacchi, ma studiato come esempio concreto di progetto di un "generico" protocollo, e iii)* ***introduzione alle blockchain****.*
PROGRAMMA	• Motivazioni ed esempi di errori comuni in sicurezza • Esempio di errore #1: uso errato dell'assunzione di one-time-pad in un contesto di autenticazione mutua con RFID • Richiami su PAP e CHAP (autenticazione Challenge-Response) • Esempio di errore #2: problemi dall'uso di CHAP per autenticazione mutua (attacchi di reflection/intertwining) e "soluzione finale" • Confronto CHAP vs PAP al variare dei modelli di attacco, e considerazioni su sicurezza "relativa" (esempio di errore #3)

- Richiami su protezione delle password mediante hash; perché con CHAP non è possibile farlo; tecnica di mitigazione basata su “salt”; differenze con “salt” integrato nei database delle password
- Ancora sui modelli di attacco: perché non usare SHA-256 nei file di password (cenni a bcrypt)
- Richiami su stream cipher. Definizione di sicurezza semantica (IND-CPA). Il concetto di Initialization Vector
- Esempio di errore #4: il caso WEP: attacco alla confidenzialità a causa di IV completamente sottodimensionato (cenni anche a debolezze RC4 ed attacco Fluhrer-Mantin-Shamir)
- Esempio di errore #4: il caso WEP: attacco all’integrità e problema di linearità del CRC
- Esempio di errore #4: il caso WEP: Autenticazione in WEP e doppio errore: i) attacco all’autenticazione stessa con esempio di impersonation attack, e ii) uso dell’autenticazione WEP per produrre coppie IV->keystream valide ed attaccare cifratura
- Cenni a evoluzione di Wi-FI security post-WEP
- Introduzione a TLS: handshake e record phases; processo di trasformazione dei dati in trasmissione e discussione
- Richiami su Message Authentication Codes: protezione ad attacchi MITM, protezione ad attacchi SPOOFING, NON protezione a replay attack; concetto di Nonce, le tre forme di nonce (seq, random, timestamp) e discussione di pro e contro per ciascuna categoria
- MAC con Hash: perché il problema NON è banale. Cosa succede con costruzione H(msg, segreto) (precomputation attack); cosa succede con costruzione H(segreto, msg) (message expansion attack)
- HMAC: cenni alla costruzione, uso di HMAC
- Ripasso su crittografia a Blocchi: ECB, come rendere ECB semanticamente sicuro. La costruzione CBC
- Il problema della combinazione MAC ed encrypt: le tre possibilità e perché la soluzione MAC and ENC usata in SSH è clamorosamente errata (definizione di sicurezza e sua confutazione con game IND-CPA)
- Richiami su padding TLS
- Risposte del server SSLv3 e TLS1.0 a messaggio errato: decryption_failed vs bad_record_MAC: Padding Oracle Attack. Perché è difficile da mitigare: Canvel side channel 2003
- Parentesi su side channel attack, e cenni ad evoluzioni successive dell’attacco Padding Oracle: Lucky 13, Lucky ms, etc e conclusione con Citazione di Marlinspike (Cryptographer’s doom)
- Il problema dell’IV predicibile in CBC: teoria e pratica (BEAST attack, con introduzione al concetto di Chosen Boundary Attack e linearità dell’attacco con dimensione dei token di autenticazione – demo youtube)
- Problemi emergenti con combinazione di compressione e cifratura: CRIME attack (idee di base)
- TLS Handshake: introduzione, obiettivi, richiami su crittografia asimmetrica (RSA key transport e Diffie-Hellman key agreement)
- Il problema dei downgrade attack e dei bid-down attack (con esempi 5G)
- Negoziazione in TLS ed attacco downgrade alla versione. Mitigazione con RSA transport; soluzione definitiva con finished message. Generalizzazione ed applicazione della stessa tecnica difensiva ad altri sistemi
- Gestione delle chiavi in TLS. Extract & Expand: motivazione, esempi, applicazione specifica al caso TLS, PRF e la nuova funzione HKDF (cenni)

	• Approfondimento sulla sicurezza di RSA key transport. RSA e Chosen Ciphertext Attack; malleability di RSA • RSA padding PKCS1v1.5: perché (malleability e CPA), dettagli • Bleichenbacker Oracle: dove nasce, cosa comporta, vulnerabilità nelle versioni TLS precedenti a 1.0, patch protocollari e relativi limiti • La saga dell'oracolo di Bleichenbacker dal 1998 al 2019. Perché è veramente difficile mitigare l'attacco. Dettagli sugli attacchi DROWN e ROBOT, e discussione errori di configurazione (es. riuso chiavi) e di implementazione (cenni a protocol fuzzying). Conclusioni (è uno dei tre motivi per cui RSA è stata tolta da TLS1.3) • Il problema dell'integrità di sessione. Perché non è risolto da HMAC. Soluzione TLS: close-notify • Renegotiation attack in TLS: quale errore è stato fatto nella standardizzazione, e come è stato sfruttato • Renegotiation attack in pratica: perché un apparentemente innocuo Plaintext preample injection attack può invece avere effetti disastrosi in adeguati scenari applicativi. Esempi semplificati ma ispirati all'attacco di Kurmus a twitter • Cenni a TLSv1.3, con particolare approfondimento sul concetto di Perfect Forward Secrecy e la sua importanza attuale. Perché solo Ephemeral DH permette PFS. PFS con pre-shared key: come si ottiene. Cenni a PFS in applicazioni di messaggistica (signal double ratchet). • Altri asset di TLS1.3 (cenni veloci): 3way handshake, 0-rtt, restrizione ai soli cipher AEAD, etc. • Mass surveillance in TLS e problematiche emergenti con la PKI (problema dei certificati Fake e scenari di attacco) • La soluzione Certificate Transparency / Extended Validation • Dettagli tecnici su Merkle Tree / Cron Tree ed applicazione a Certificate Transparency • Introduzione alle Blockchain. Definizione, giustificazione, perché l'organizzazione a blocchi di Certificate Transparency non è una blockchain • Differenze tra permissionless vs permissioned • Architettura e struttura dati di una blockchain; come gestire l'identità per utenti anonimi: self-certifying identities • Consenso: concetto generale, il caso permissioned; perché è difficile nel caso permissionless, consenso implicito nella soluzione bitcoin. Il problema degli attacchi sibilla e cenni a proof-of-work e proof-of-stake; il problema del 51%: attacchi offspring ed implicazioni geo-politiche • Scripting nelle blockchain: cenni

Modulo di	**SICUREZZA INFORMATICA E PREVENZIONE DEGLI ATTACCHI**
Ore previste:	**10**

OBIETTIVI DEL CORSO	*Il modulo si prefigge l'obiettivo di fornire elementi di base di sicurezza informatica al fine di aumentare la consapevolezza dei principali rischi e migliorare la conoscenza delle relative contromisure da adottare in termini tecnici e comportamentali.* *Vengono descritti i principali vettori di attacco, tra i quali viene dato ampio spazio al phishing ed alle relative metodologie di social engineering, lo sfruttamento di vulnerabilità e l'utilizzo di malware, fornendo parallelamente tutti gli elementi tecnici e, soprattutto, comportamentali, per evitare di diventare vittime di crimini informatici mettendo in pericolo i propri dati, sia come cittadini che come lavoratori all'interno di una organizzazione.*

PROGRAMMA	• Introduzione: definizione e panoramica dei rischi e degli attacchi informatici
	• Phishing
	  ○ Rischi e contromisure
	  ○ Social engineering e spear phishing
	  ○ Tecniche di protezione: analisi dell'header, SPF, DKIM, DMARC
	• Malware
	  ○ Tecniche di attacco attraverso malware: classificazione del malware
	  ○ Analisi del malware: statica e dinamica, analisi di casi reali
	  ○ Botnet: struttura, analisi e tecniche di attacco; attacchi DDoS
	• Vulnerabilità
	  ○ Definizioni, CVE e CVSS
	  ○ SQL Injection, tecniche di attacco e contromisure
	  ○ Data breach: rischi e mitigazione
	  ○ XSS (Cross Site Scripting): tecniche di attacco e contromisure
	• Crittografia e protezione dei dati
	  ○ Cenni di crittografia simmetrica ed asimmetrica
	  ○ Funzioni hash
	  ○ Cenni di steganografia

Modulo di	**SISTEMI BIOMETRICI**
Ore previste:	**15**

OBIETTIVI DEL CORSO	*Il modulo si propone l'obiettivo di fornire gli strumenti per comprendere ed analizzare i sistemi biometrici che utilizzino sia una sola caratteristica biometrica (sistemi uni-modali) che più caratteristiche biometriche (sistemi multi-modali). Inoltre, i sistemi biometrici sono analizzati dal punto di vista della sicurezza e della privacy.*
PROGRAMMA	• **Fondamenti di Biometria**: Identità e biometria. Introduzione ai sistemi biometrici. Applicazioni • **Identificatori biometrici morfologici:** impronte digitali, volti (2D e 3D), geometria della mano, palmo della mano, strutture venose, iride, termogrammi, etc.) e comportamentali (firma, voce, modalità di digitazione, andatura, movimento delle labbra, etc.)

	• **Verifica e valutazione delle prestazioni del sistema:** FAR, FRR. FTE, FTA, curve ROC, DET, CMC, usabilità, scalabilità • **Sistemi biometrici multimodali** • **Sicurezza nei sistemi biometrici** • **•Vulnerabilità e contromisure nei sistemi biometrici** • **Privacy nei sistemi biometrici** • **"Privacy Enhancing Technologies" (PET)**
Modulo di	**HARDWARE SECURITY**
Ore previste:	**25**
OBIETTIVI DEL CORSO	*Il corso introduce i principi della sicurezza hardware lungo l'intero ciclo di vita dei sistemi digitali: progettazione, fabbricazione, test, integrazione e impiego operativo. L'obiettivo è collegare il concetto di hardware come root of trust alle minacce derivanti da filiere globali, vulnerabilità fisiche e microarchitetturali, meccanismi di test e variabilità di processo. Sono utili conoscenze di base di elettronica digitale, algebra booleana e architettura dei calcolatori. Il corso richiama i concetti essenziali di crittografia, progettazione VLSI, manufacturing test, affidabilità e progettazione fault tolerant necessari per seguire i moduli specialistici.*

PROGRAMMA	• **Introduction and background notions**
	  ○ **Dependability e sicurezza.** Quality, reliability e security; hardware come root of trust; minacce, vulnerabilità, attacchi, riservatezza, integrità e disponibilità.
	  ○ **Filiera e fiducia.** Modelli verticali e orizzontali dell'industria VLSI; IP di terze parti; system integration; foundry non fidate; contraffazione, overproduction, riciclo, cloning, IP e IC piracy.
	  ○ **Richiami di crittografia.** Cifratura simmetrica e asimmetrica; crittoanalisi; cifrari a blocchi e a flusso; concetti e funzionamento essenziale di DES e RSA.
	  ○ **VLSI, test e affidabilità.** Flusso di progettazione e fabbricazione; livelli e principi del test; scan design; yield; relazione fault-error-failure; stima dell'affidabilità; ridondanza hardware, temporale e informativa.
	• **Trust Issues e Hardware Trojan**
	  ○ **Definizioni e modelli.** Differenza tra bug e modifica malevola; backdoor e time bomb; avversari e minacce nelle fasi di specifica, progettazione, fabbricazione e test.
	  ○ **Tassonomia.** Livello di astrazione, fase di inserimento, meccanismo di attivazione, payload e posizione fisica del Trojan.
	  ○ **Esempi e benchmark.** Trojan attivati internamente o da eventi rari; perdita di informazioni tramite canali covert e overt; benchmark Trust-Hub.
	  ○ **FPGA.** Architettura di base, flusso di progettazione e inserimento di Hardware Trojan; meccanismi di attivazione e payload in dispositivi riconfigurabili.
	• **Vulnerability Issues e tecniche di attacco**
	  ○ **Side-channel attacks.** Tassonomia degli attacchi invasivi e non invasivi, attivi e passivi; modello dell'attaccante; misura e interpretazione delle informazioni fisiche.

	○ **Power ed electromagnetic analysis.** Simple Power Analysis, Differential Power Analysis ed Electromagnetic Analysis; esempi su DES e RSA; setup sperimentali e piattaforme di analisi. ○ **Fault-injection e timing.** Glitch di tensione o clock, perturbazioni elettromagnetiche e laser; modelli di guasto; attacchi temporali contro implementazioni crittografiche. ○ **Vulnerabilità microarchitetturali.** Attacchi all'esecuzione transiente, inclusi Spectre e Meltdown, e tecniche di tipo Flush+Reload. ○ **Test-oriented attacks**. Abuso delle infrastrutture di scan e debug; scan-chain attack finalizzato all'estrazione di chiavi in implementazioni AES. • **Countermeasures** ○ **Asset e modelli di attacco.** Identificazione degli asset da proteggere e costruzione di modelli coerenti con fase del ciclo di vita, capacità dell'avversario e canali osservabili. ○ **Trust a livello IP e IC.** Verifica formale, property e model checking, coverage analysis; rilevamento post-silicon mediante test logico e funzionale, side-channel e analisi del ritardo; metodo MERO. ○ **Design for Hardware Trust.** Rimozione o aumento della probabilità di eventi rari, runtime monitoring, design obfuscation e Built-In Self-Authentication. ○ **Contromisure per SCA.** Masking, hiding, bilanciamento, logiche Dual Rail Precharge e VSC; contromisure microarchitetturali contro timing e transient-execution attacks. ○ **Contromisure per FIA e test.** Prevenzione fisica e temporale, rilevamento degli errori, protezione del package e difesa di scan chain, JTAG e infrastrutture BIST. • **Hardware Security Primitives** ○ **Variabilità e identità fisica.** Variabilità sistematica e casuale dei processi CMOS come base per primitive difficili da clonare. ○ **Physically Unclonable Functions.** Arbiter PUF, Ring Oscillator PUF e SRAM PUF; strong e weak PUF; challenge-response pairs, identificazione e generazione di chiavi. ○ **Metriche e affidabilità.** Unicità, uniformità, repeatability, stabilità e gestione degli helper data. ○ **True Random Number Generators**. Sorgenti fisiche di entropia, jitter di clock, requisiti di qualità, architetture TRNG e tecniche di post-processing.

Modulo di	**MODELLI DECISIONALI E INTELLIGENZA ARTIFICIALE**
Ore previste:	**20**
OBIETTIVI DEL CORSO	*Lo scopo del modulo è quello di introdurre gli studenti all'uso di strumenti analitici per affrontare problemi decisionali. Gli strumenti includono la definizione di modelli matematici prescrittivi, modelli descrittivi di simulazione e di intelligenza artificiale e l'uso di algoritmi per individuare una buona soluzione del problema in esame. Sarà data anche enfasi all'applicazione di tali strumenti nel settore TLC.*
PROGRAMMA	I. Introduzione alla decision analytics

	• Decision analytics: definizione e differenza tra metodi descrittivi, predittivi e prescrittivi • Vantaggi dell'utilizzo delle tecniche di decision analytics nell'ambito delle telecomunicazioni • Esposizione di casi applicativi rilevanti nel settore TLC II. Metodologie di decision analytics II.a Machine learning e reti neurali • Machine learning: definizioni; paradigmi di apprendimento supervisionato e non supervisionato • Modelli di clustering • Modelli di classificazione: le reti neurali artificiali, alberi e foreste II.b Modellistica per la prescriptive analytics • Definizione del problema e raccolta dei dati • Costruzione e validazione del modello • Utilizzo dei modelli per la pianificazione e l'ottimizzazione delle decisioni • Modelli prescrittivi e ottimizzazione: ruolo, caratteristiche, classificazione e metodologie principali II.c Metodi e modelli di simulazione • Classificazione delle tecniche di simulazione • Modelli di sistemi di servizio e simulazione • Simulazione ad eventi discreti: caratteristiche ed applicazioni III. Applicazioni di metodi e modelli di decision analytics nel settore delle telecomunicazioni e casi di studio di processi decisionali in ambito strategico, tattico e operativo: • Progetto e pianificazione di reti e di capacità • Gestione delle risorse, del traffico e dell'esperienza del cliente • Analisi e miglioramento di processi aziendali

Corso di	SERVIZI, RETI E TERMINALI DI TLC

Modulo di	SCIENZE SOCIALI, PIATTAFORME E INTERFACCE
Ore previste:	20

OBIETTIVI DEL CORSO	*Il modulo si prefigge l'obiettivo di proporre il contributo delle scienze sociali (e, in particolare, sociologia della comunicazione e internet studies) all'analisi e all'interpretazione dei fenomeni legati all'utilizzo delle piattaforme e degli ambienti digitali.*

PROGRAMMA	• Rapporto tecnologia/cultura/società
	  ○ Mutual shaping tecnologia/società
	• Gli algoritmi dei social media e di Google – dal punto di vista dello scienziato sociale
	  ○ Immaginari algoritmici
	• I processi di convergenza
	• I modelli: network society e platform society
	• Struttura e dinamiche dei network (dal punto di vista dello scienziato sociale)
	• Social media e social network site
	• Gli utenti dei sistemi digitali
	  ○ "Nascita degli utenti" (e della HCI)
	  ○ Evoluzione della riflessione sugli utenti
	  ○ Un focus: il concetto di "utente modello"
	  ○ Anziani e ICT: tra ageism e "unexpected users"
	• Interfacce
	User experience
	Human centered design

Modulo di	USABILITÀ DEL WEB
Ore previste:	10

OBIETTIVI DEL CORSO	*Il modulo didattico è strutturato per trasferire conoscenze e competenze specialistiche sugli aspetti dell'usabilità e dell'UX. La didattica si completa poi, con una parte dedicata ai servizi digitali nel web, con cenni sul rapporto tra accessibilità e usabilità e sui metodi e gli strumenti per valutarli. La sezione teorica per l'acquisizione delle conoscenze è integrata ed arricchita da una serie di esperienze pratiche, svolte grazie all'ausilio del Laboratorio della Qualità dei servizi digitali – DGTel*

PROGRAMMA	• Usabilità del web
	  ○ L'usabilità e l'UX
	  ○ Il protocollo eGLU
	  ○ Introduzione alla QoE sul web
	• Esercitazione e pratiche di laboratorio

Modulo di	**ACCESSIBILITÀ DEL WEB**
Ore previste:	**15**

OBIETTIVI DEL CORSO	*Il modulo è strutturato per trasferire conoscenze e competenze specialistiche sugli aspetti legati ai requisiti di qualità e all'accessibilità dei contenuti e dei servizi digitali nel web, con particolare riguardo ai metodi e agli strumenti per valutarli. La sezione teorica per l'acquisizione delle conoscenze scientifiche e normative è integrata ed arricchita con una serie di esperienze pratiche, svolte grazie all'ausilio dei laboratori della DGTEL-ISCTI.*

PROGRAMMA	• Introduzione all'accessibilità
	  ○ Concetti generali
	  ○ Disabilità e tecnologie assistive
	  ○ Dislessia e buone pratiche di progettazione
	• Normativa e standard di riferimento
	  ○ EN 301 549 e linee guida W3C WCAG 2.1
	  ○ Legge n. 4/2004 e s.m.i.
	• Introduzione alle tecnologie del web
	  ○ HTML
	  ○ CSS
	• Requisiti tecnici
	  ○ Criteri di successo
	  ○ Tecniche di accessibilità
	• Verifiche di accessibilità
	  ○ Metodologia
	  ○ Strumenti di valutazione
	• Attività e pratiche di laboratorio
	  ○ Esecuzione delle verifiche di accessibilità in esercitazione di gruppo
	  ○ Analisi dei risultati e redazione del rapporto di prova

Corso di	TECNOLOGIE ELETTRONICHE E TECNICHE CIRCUITALI

Modulo di	**SISTEMI DI COMUNICAZIONE IN FIBRA OTTICA**
Ore previste:	**20**

OBIETTIVI DEL CORSO	*Il modulo si propone l'obiettivo di fornire le conoscenze principali relative ai sistemi di comunicazione in fibra ottica. Obiettivi del corso sono l'analisi delle prestazioni di tali sistemi sia in configurazione punto-punto sia nell'ambito delle reti ottiche (rete di trasporto e rete d'accesso). Sono forniti gli strumenti di base per la progettazione di tali sistemi.*

PROGRAMMA	• FIBRE OTTICHE
	  ○ Fibre ottiche: analisi mediante l'ottica geometrica; fibre ottiche multimodali, apertura numerica, dispersione modale
	  ○ Fibre ottiche singolo-modo: analisi mediante l'ottica fisica; modo fondamentale, cut-off, attenuazione
	  ○ Dispersione cromatica: dispersione del materiale, dispersione di guida
	  ○ Tipi di fibra ottica singolo-modo: SM (G.652), DS (G.653), NZDF (G.655)
	  ○ Propagazione in fibra ottica in regime lineare
	  ○ Fenomeni non-lineari: effetto Kerr (SPM, FWM, XPM)
	  ○ Propagazione in fibra ottica in regime non-lineare (solitoni)
	  ○ Fenomeni di scattering in fibra ottica: effetto Brillouin, effetto Raman
	• SORGENTI OTTICHE
	  ○ Interazione luce-materia
	  ○ Laser a semiconduttore
	• COMPONENTI IN OTTICA INTEGRATA
	  ○ Effetto elettro-ottico lineare (effetto Pockels)
	  ○ Modulatori elettro-ottici di ampiezza e di fase (LiNbO3)
	• RICEVITORI OTTICI
	  ○ Fotodiodi: PIN, APD, efficienza quantica, responsività, rumore di rivelazione (shot-noise)
	  ○ Struttura del ricevitore ottico a rivelazione diretta (DD): amplificatore di front-end (amplificatore a transimpedenza, amplificatore ad alta impedenza)
	  ○ Sensibilità del ricevitore. Limite quantico della rivelazione ottica
	  ○ Prestazioni del ricevitore ottico: rumore termico, rapporto segnale-rumore (SNR), probabilità d'errore di bit (BER)

Modulo di	**COMPETENZE DI OPTOELETTRONICA**
Ore previste:	**20**

OBIETTIVI DEL CORSO	*Il modulo si prefigge l'obiettivo di fornire una panoramica completa dei dispositivi optoelettronici alla base dei sistemi di comunicazione ottica.*

PROGRAMMA	• Introduzione alle reti ottiche
	  ○ Dispositivi e funzioni 1R, 2R 3R
	  ○ Proprietà ed utilizzo delle fibre ottiche
	• Proprietà dei semiconduttori
	  ○ L'archetipo dei dispositivi optoelettronici a stato solido: la giunzione p-n
	  ○ Classificazione principali dispositivi optoelettronici
	  ○ Concetti di base sui materiali semiconduttori. Fondamenti del trasporto di carica. Proprietà ottiche dei semiconduttori. Cenni su giunzioni p-n e diodi p-i-n. Eterostrutture: proprietà di base ed applicazioni
	• Dispositivi optoelettronici fondamentali
	  ○ Fotorivelatori
	  ○ Assorbimento intrinseco ed efficienza quantica. Fotorivelatori a diodo p-i-n. Fotorivelatori a valanga (APD). Fotorivelatori ad eterogiunzione. Sistemi ed applicazioni: Free Space Optics, Visible Light Communications
	• Dispositivi optoelettronici fondamentali
	  ○ LED
	  ○ LASER multimodali (Fabry-Perot)
	  ○ Assorbimento, emissione spontanea ed emissione stimolata. Guadagno ottico. Emissione spontanea. Spettro della radiazione di ricombinazione. Efficienza quantica. Modulazione della radiazione ottica. Principi di funzionamento di LED. Applicazioni dei LED
	  ○ LASER: Emissione stimolata. Principi dell'azione laser. Proprietà della radiazione laser. Guadagno ottico in semiconduttori. Rate equations per Laser a semiconduttori
	• Dispositivi optoelettronici avanzati
	  ○ Amplificatori ottici (SOA, EDFA, Raman)
	  ○ Sistemi ottici per l'elaborazione ottica dell'informazione
	  ○ Case study (esercitazione di laboratorio): il caso della conversione di lunghezza d'onda per i sistemi WDM mediante effetti ottici non lineari negli amplificatori a semiconduttore
	  ○ Esempi di sistemi di comunicazione ottica. Sistemi WDM, architetture di routing ottico, conversione di lunghezza d'onda mediante dispositivi ottici non lineari, esercitazione di laboratorio su amplificazione ottica, modulazione, conversione di lunghezza d'onda mediante XGM
	• Dispositivi optoelettronici avanzati
	  ○ LASER monocromatici avanzati (DFB, DBR)
	  ○ Dispositivi per la modulazione esterna (Niobato di Litio, modulatori ad elettroassorbimento)
	  ○ Tipi di modulatori, architetture e principi di funzionamento

Modulo di	**CYBERSECURITY DELLE INFRASTRUTTURE DIGITALI CRITICHE: CAVI SOTTOMARINI E DATA CENTER**
Ore previste:	**10**

OBIETTIVI DEL CORSO	*Il modulo si propone di fornire competenze operative e strategiche per proteggere le infrastrutture digitali critiche, con focus su minacce, normative e contromisure relative a cavi sottomarini e data center.*
PROGRAMMA	• **Modulo 1 – Sicurezza cyber dei cavi sottomarini (5h)** ○ Introduzione alla rilevanza strategica dei cavi sottomarini nel cyberspazio globale. Ruolo critico delle landing station, tratta sottomarina, dorsali intercontinentali. ○ Minacce cyber documentate: attori statali (APT29, APT31), attacchi a componenti di rete, compromissione firmware e supply chain. ○ Analisi tecnica delle vulnerabilità nei sistemi OT e SCADA connessi ai cavi: accessi remoti, interfacce esposte, exploit CVE reali. ○ Tecnologie di monitoraggio e detection: AI, analisi di pattern comportamentali, sensoristica lungo la tratta fisica, allarmi precoci. ○ Sistemi di difesa attiva: segmentazione della rete, gestione delle credenziali, approcci zero-trust, sicurezza by design. ○ - Normativa di riferimento: NIS2, Cable Security Toolbox, linee guida ENISA e policy europee per la protezione delle infrastrutture digitali sottomarine. ○ Simulazione guidata: risposta coordinata a un attacco cyber su una landing station. Coinvolgimento di CERT, gestori e operatori di rete. • **Modulo 2 – Data center e AI (5h)** ○ Introduzione ai data center moderni: cloud distribuito, edge computing, sistemi AI-native e architetture critiche ○ Minacce reali: attacchi ransomware, compromissioni hardware, blackout indotti, casi studio noti (OVH, Equinix, Google) ○ Sicurezza dei sistemi AI: poisoning, inferenze malevole, jailbreak dei modelli, vulnerabilità nei dataset ○ Difesa avanzata: tecniche zero-trust, MLOps sicuro, controllo degli accessi e dei flussi AI, audit automatici ○ Requisiti normativi: AI Act, NIS2, GDPR e regole per l'operatività di data center critici ad alta affidabilità ○ Certificazioni, audit e compliance: framework ISO/IEC, gestione del rischio e resilienza operativa ○ Caso pratico: simulazione di attacco AI-driven a un data center nazionale, con analisi dei flussi decisionali e risposta integrata (IT, OT, legale)

Corso di	**UTILIZZAZIONE E ALLOCAZIONE DELLO SPETTRO RADIO**

Modulo di	**PIANIFICAZIONE E GESTIONE DELLO SPETTRO RADIO**
Ore previste:	**20**

OBIETTIVI DEL CORSO	*Il modulo si propone l'obiettivo di fornire i concetti base della pianificazione e della gestione dello spettro radio, mettendo in risalto la necessità di stabilire regole adottate a livello mondiale. La risorsa naturale «spettro radio» si propaga in spazi non limitati che vanno oltre i confini nazionali; pertanto, è necessario armonizzare le regole attraverso Organismi internazionali di regolamentazione.* *Nella prima parte, il modulo illustra i principi di carattere generale della risorsa spettro radio dopodiché descrive la struttura degli Organismi internazionali, il metodo di lavoro e gli Atti Normativi. Poi si cala nella descrizione degli Organismi italiani e nella trattazione dettagliata delle principali norme quali il Regolamento mondiale delle radiocomunicazioni dell'UIT, il PNRF (Piano Nazionale di Ripartizione delle Frequenze) ed il Codice delle Comunicazioni Elettroniche.* *Nella seconda parte, il modulo descrive i principali processi ed attività utilizzati nella gestione dello spettro radio ed illustra l'evoluzione degli scenari di radiocomunicazione e delle tecnologie di trasmissione radio fino alla tecnologia 5G.*

PROGRAMMA	• Introduzione all'attività di pianificazione e gestione dello spettro radioelettrico
	  ○ Caratteristiche dello spettro radio, risorsa scarsa
	  ○ Necessità di coordinamento e regole armonizzate a livello mondiale
	  ○ Attribuzione delle frequenze radio, servizi radio e stazioni radio
	  ○ Servizi primari e secondari e regole del coordinamento
	  ○ Ruolo dell'Organismo nazionale
	• Unione Internazionale delle Telecomunicazioni (UIT)
	  ○ Compiti e struttura dell'UIT
	  ○ Il Regolamento delle Radiocomunicazioni
	  ○ Conferenze Mondiali delle Radiocomunicazioni
	• Organismi europei di regolamentazione. Compiti, obiettivi, struttura e attività
	  ○ CEPT
	  ○ Unione Europea
	  ○ ETSI
	• Organismi e normativa nazionale.
	  ○ Il Ministero delle Imprese e del Made in Italy (MIMIT)
	  ○ Il Ministero della Difesa
	  ○ L'Autorità per le Garanzie nelle comunicazioni
	  ○ Piano Nazionale di Ripartizione delle Frequenze
	  ○ Piani di Assegnazione e di Allocazione delle frequenze
	• Il Codice delle comunicazioni elettroniche
	  ○ Semplificazioni apportate dal codice (neutralità dei servizi e delle tecnologie, vendita ed affitto secondario delle frequenze, ...)
	  ○ Autorizzazione generale per l'esercizio di reti e servizi di comunicazione elettronica: SCIA e diritti d'uso delle frequenze
	  ○ WISP (Wireless Internet Service Provider)
	  ○ Uso collettivo dello spettro radio e Short Range Devices (SRD)
	• Nuovi scenari nella gestione dello spettro radio
	  ○ Convergenza dei servizi radio, delle tecnologie e delle infrastrutture di rete

	○ Reti di accesso radio - WiFI, WiMax, WLL26/28 (Wireless Local Loop, FWA) ○ Tecniche di condivisione dello spettro radio, Tecnologie cognitive e Licenced Shared Access (LSA) ○ Sperimentazione di rete LSA in banda 2300-2400 MHz - MISE Roma EUR • Pianificazione dello spettro radio per le reti IMT2020 e 5G ed evoluzione delle reti mobili ○ UIT-R - Identificazione delle bande IMT ○ Introduzione, obiettivi e scenari d'uso delle reti in tecnologia 5G ○ Evoluzione delle reti mobili (slicing della rete, reti eterogenee) ○ Piano d'azione e roadmap dell'UE e della CEPT ○ Bande di frequenze pioniere (3400-3800 MHz 24,25-26,5 GHz) ○ Introduzione del 5G in Italia, sperimentazione e bando di gara del 2018

Modulo di	**DIGITAL SINGLE MARKET: REGOLAMENTAZIONE E STANDARDIZZAZIONE**
Ore previste:	**10**

OBIETTIVI DEL CORSO	*Il modulo si prefigge di fornire la chiave di lettura per decodificare, dal punto di vista industriale ed economico, la portata del Mercato Unico Digitale (in particolare dei prodotti radio) nel mercato interno, attraverso una analisi delle disposizioni regolamentari, della standardizzazione, dell'NLF e delle iniziative sulla cyber security*.
PROGRAMMA	**MERCATO UNICO** • ONE SINGLE MARKET ○ Timeline del processo di apertura del mercato ○ Digital Single Market and e-Commerce ○ Prospettive 2024, 2030, 2050 ○ Mercato B2C - B2B - C2C - B2G, (Business – Commercial – Government) ○ e-procurement, e-signature ○ Cenni sul Regolamento EIDAS su trust services ○ Common standards for Digital Single Market • GOODS MARKET ○ Building blocks of the Single Market ○ New Legislative Framework: Regolamenti e decisioni costituenti l'attuale quadro regolamentare e le prospettive future (Reg. 765/2008/CE e 2019/1020 UE, Dec. 768/2008/CE, Reg. 764/2008/CE e altri documenti di indirizzo). In particolare: migliorare le regole per la vigilanza del mercato, aumentare la qualità (e la fiducia) della valutazione della conformità dei prodotti, istituire un quadro giuridico comune che comprende la sicurezza informatica (proposta di Regolamento relativo a requisiti orizzontali di cybersicurezza per i prodotti con elementi digitali) ○ Notified Body ○ Conformity Assessment Body ○ Conformity Assessment Procedure ○ Market surveillance ○ Esempio di direttiva generica (EMC) • RADIO EQUIPMENT MARKET

	• DIRETTIVA 2014/53/UE sulle “apparecchiature radio”
	  ○ Scopo
	  ○ Requisiti essenziali, CAB, CAP, NB
	  ○ Effective Vs Efficient
	  ○ Prodotti “faster than regulation”
	  ○ Study cases: “La SAR nei telefonini”, Il caso “Cayla”, Il caso degli “zainetti”
	• GLI STANDARDS NEL CONTESTO REGOLAMENTARE EUROPEO E MONDIALE
	  ○ European Standard
	  ○ Stydy case “James Elliott vs Irish Asphalt Limited”
	  ○ International standard
	  ○ Regolamento 1025/2012 e varie modifiche
	  ○ ESO (European Standardisation Organisations) SDO (Standard Developing Organizations)
	  ○ Le azioni intraprese per la protezione del mercato interno da holding di soggetti terzi

Modulo di	**SISTEMI SATELLITARI, INGEGNERIA DELLO SPETTRO ELETTROMAGNETICO E REGOLAMENTAZIONE INTERNAZIONALE**
Ore previste:	**10**

OBIETTIVI DEL CORSO	*Brevi cenni sulle principali nozioni di dinamica orbitale, delle tecniche di telecomunicazione e trasmissione delle onde elettromagnetiche nello spazio, per comprendere i principi necessari a garantire un’equa distribuzione, fra i numerosi operatori, delle risorse disponibili in termini di posizioni orbitali e spettro elettromagnetico. Il corso include alcuni elementi teorici per l’apprendimento delle tecniche necessarie alla valutazione delle interferenze fra costellazioni geostazionarie e non geostazionarie anche attraverso l’utilizzo dei principali strumenti software.*

PROGRAMMA	• I sistemi satellitari (4 ore)
	  ○ Cenni di dinamica orbitale
	  ○ I principi delle Comunicazioni Satellitari
	  ○ Stazioni di terra e collegamenti satellitari
	  ○ Reti e sistemi di comunicazione
	• Interferenze e Regolamentazione (4 ore)
	  ○ Regolamentazione Internazionale e regionale
	  ○ I concetti base dell’ingegneria dello spettro elettromagnetico
	  ○ I modelli di propagazione delle onde elettromagnetiche
	  ○ Il calcolo delle interferenze
	• Gli strumenti software (2 ore)
	  ○ Strumenti software per le analisi delle interferenze
	  ○ Il software dell’ITU
	  ○ Software disponibili sul mercato

Modulo di	**CAMPI ELETTROMAGNETICI – NORMATIVA E STRUMENTAZIONE**
Ore previste:	**10**
OBIETTIVI DEL CORSO	*Il modulo si propone l'obiettivo di fornire un livello di conoscenza più approfondita ed integrale dei campi elettromagnetici sia in alta frequenza sia in bassa frequenza, della normativa nazionale ed internazionale ad essi applicabile, dei principi di funzionamento della strumentazione di misura con possibilità di eventuale laboratorio di 5 ore per attività di misurazione delle sorgenti in alta frequenza presso i laboratori del Ministero delle Imprese e del Made in Italy (mediante analizzatori di spettro e antenne in dotazione presso i laboratori).*
PROGRAMMA	• Presentazione del corso • ICNIRP – Linee Guida del 1998 • D.M. 10 settembre 1998 n.381 • Raccomandazione 519/CEE/1999 • Legge quadro 22 febbraio 2001 n. 36 • DPCM 8 luglio 2003 – ELF • Strumentazione di misura ELF • Proprietà dei campi ELF • Pressioni sul territorio nazionale di sorgenti di campi elettromagnetici • SAR – tasso di assorbimento specifico e classificazione IARC • Le agenzie regionali sul territorio: attività e compiti • Statistiche e analisi dei dati aggiornati • Sistema agenziale per il 5G • Saturazione dei siti • Campi da elettrodotti e da cabine e sottostazioni elettriche • DPCM 8 luglio 2003 RF • Decreto-legge 18 ottobre 2012 n.179 • Sistema Agenziale – ISPRA e ARPA • DM 2 dicembre 2014 – Linee guida ISPRA/ARPA • Linee guida ICNIRP 2020 • Centraline di monitoraggio • Legge 111/2011 articolo 35 • Direttiva UE 2018/1972 • Nuovo Regolamento Europeo 30 giugno 2020 • Decreto legislativo 207/2021 • Presentazione delle attività di misura • Proprietà dei campi: campo vicino e campo lontano, etc. • Caratteristiche generali della strumentazione • Strumentazione a banda larga • Strumentazione a banda stretta • Analizzatore di spettro e tecniche di misura • Norma CEI 211-7 • Esempio numerico di misurazione in banda stretta • Software di simulazione dei CEM • Tecniche di estrapolazione • Tecniche di riduzione a conformità

	• Incertezza di misura • Taratura della strumentazione • Legge n.214 del 30 dicembre 2023 • Innalzamento dei limiti per le radiofrequenze