Il programma delle 10 giornate è articolato nelle seguenti 10 lezioni.

Lezione 1

- Cyber Security intro
- Cyber Security Definition
- Classification Data concept
- NIST standard and Common Criteria certification
- Security Actors
- Security Intelligence Center (SIC) & Security Operation Center (Soc)
- The CIA triad (Confidentiality / Privacy , Integrity & Availability)
- Cyber Security Math concepts (ESERCITAZIONE)

Lezione 2

- Solutions: Evolution from rule-based to AI
- Introduction to AI for Cybersecurity
- Types of machine learning for Cyber Security
- Classification for Cyber Security
- Clustering for Cyber Security
- Predictive analysis for Cyber Security
- Malware concept and typology
- Detecting spam with Perceptrons (ESERCITAZIONE)
- Security by Linear Regression (ESERCITAZIONE)

Lezione 3

- Model-based systems engineering in Cyber Security
- Network concepts
- Protecting and architecture
- Introduction Detection System (IDS)
- Password prevention and attack
- Classification of network attack
- Cloud AI solution
- Codes vs. Ciphers in Cyber Security

Lezione 4

- Cryptography
- Cryptography in Cyber Security
- Reverse Cipher (ESERCITAZIONE)
- Caesar Cipher (ESERCITAZIONE)
- Cipher Wheel (ESERCITAZIONE)
- Transposition Cipher Encryption (ESERCITAZIONE)
- Cryptography in AI

Lezione 5

- Crittoanalisi
- Direct attack
- Brute Force attack
- BRUTE-FORCE (ESERCITAZIONE)
- CPA attacks
- Side-Channel Attack by AI
- Confidentiality and AI
- Homomorphic Encryption (HE)
- Integrity analysis
- Availability analysis

Lezione 6

- Cyber Security data at rest, in motion , in use
- Symmetric encryption
- Asymmetric encryption
- Digital signatures
- Public key infrastructure (PKI) architecture
- Alice e Bob base approach by AI concept
- Alice e Bob (ESERCITAZIONE)

Lezione 7

- Security Requirement by AI
- Security Applications tools
- Different typology of attack
- STRIDE model
- Tampering, Eavesdropping, Denial of Service (DoS), Intrusion, Theft & alteration of data-at-rest concept
- Vulnerability concept
- Threat, vulnerability detection and classification
- Model Tires approach (AI in Cyber) against VIRUS attack

Lezione 8

- Malware attack
- Detecting malware by AI
- Spam detection with SVMs
- Phishing detection
- Naive Bayes approach in AI
- Malware detection by AI (ESERCITAZIONE)
- Polymorphic malware detection strategies
- Spam detection (ESERCITAZIONE)

Lezione 9

- Securing architectures
- Risk analysis and model
- Risk assessment & impact
- AI as THREATS
- GANs - Attacks and Defenses
- Deepfake (ESERCITAZIONE)
- Explainable Artificial Intelligence definition
- LIME, SHAP and LRP methods

Lezione 10

Capstone Project : user requirements analysis ,AI and Cyber development, verification and Test of solution