

Cybersecurity Master's Program

Module 2: Network Security & Cryptography

Course Outline

1. Network Fundamentals Review
 - Network architecture and OSI model
 - TCP/IP and routing concepts
 - Common vulnerabilities in network design
2. Network Security Components
 - Firewalls, routers, and switches configuration
 - VPNs and secure tunneling techniques
 - IDS/IPS and network monitoring tools
3. Cryptography Essentials
 - Symmetric and asymmetric encryption
 - Hashing algorithms and digital signatures
 - Public Key Infrastructure (PKI)
4. Secure Network Protocols
 - HTTPS, SSL/TLS, SSH, IPSec
 - Wireless network security (WPA3, 802.1X)
 - Email and file transfer security
5. Network Threats and Defense Strategies
 - Denial of Service (DoS) and DDoS attacks
 - Network reconnaissance and exploitation
 - Implementing layered defense models