CA301: Cryptography

30 Instructional Hours 46 CPEs 16 Labs

LIVE ONLINE OR ON-DEMAND ACCESS OR IN PERSON

INTERMEDIATE

This course provides a comprehensive and practical exploration of cryptography, covering both foundational principles and advanced applications in modern security systems. It begins with core concepts such as confidentiality, integrity, and availability, and progresses through symmetric and asymmetric encryption techniques, cryptographic algorithms, and real-world implementations. Learners are introduced to essential topics including key management, hashing, digital signatures, cryptographic protocols, and network security mechanisms like TLS and VPNs. The course also addresses emerging areas such as quantum cryptography, cryptanalysis, and steganography, while emphasizing secure implementation practices and common pitfalls. With a strong focus on applied learning, the material integrates theoretical knowledge with hands-on examples and real-world scenarios to prepare learners for practical cybersecurity challenges.

You Will Be Able To

- Apply symmetric and asymmetric encryption techniques to secure data in real-world scenarios
- Analyze and select appropriate cryptographic algorithms, modes of operation, and protocols
- Implement secure key management, hashing, and authentication mechanisms
- Identify and mitigate common cryptographic vulnerabilities and implementation flaws
- Evaluate modern cryptographic systems, including TLS, PKI, and secure communication protocols
- Understand and assess emerging threats such as quantum computing and advanced cryptanalysis

Who Should Attend

This course is designed for students, cybersecurity professionals, and IT practitioners who want to build a strong foundation in cryptography and its real-world applications. It is suitable for individuals with a basic understanding of networking or security concepts who are looking to deepen their knowledge in secure communications, encryption technologies, and data protection. The course is particularly valuable for those pursuing roles in cybersecurity, secure software development, or network defense.

Relevant Combat Roles

- Network Security Engineer
- Cryptanalyst
- Key Management Officer
- Cryptography Engineer

Topics Covered

Fundamentals & Core Principles
(CIA triad, AAA model, terminology)

Cryptographic Methods & Algorithms
(keyless, symmetric—DES/AES/stream ciphers/modes, asymmetric—RSA/Diffie-Hellman/ECC/digital signatures)

Hashing, Passwords & Security Practices
(hash functions, MACs, bcrypt/scrypt/Argon2, randomness, key derivation, IVs/nonces, encoding pitfalls)

Protocols, Infrastructure & Network Security
(PKI, certificates, authentication protocols, TLS/SSL, VPNs, secure communication)

Attacks & Advanced Topics
(cryptanalysis—brute force, frequency, padding oracles; steganography, quantum & post-quantum cryptography)

Labs

Symmetric Encryption & OpenSSL Operations
(OpenSSL DES/AES encryption, ECB/CBC modes, encryption and decryption workflows)

Public-Key Cryptography & Digital Signatures
(RSA key generation, asymmetric encryption/decryption, and digital signatures)

TLS Analysis & Certificate Inspection
(TLS configuration analysis, certificate chain inspection, and weak cipher detection)

Password Hashing & Key Derivation Security
(password hashing, salting, PBKDF2/scrypt/Argon2 key derivation)

Password Cracking & Cryptographic Attack Analysis
(weak password cracking, rainbow tables, and brute-force analysis)

Steganography & Hidden Data Analysis
(image/audio steganography, hidden data extraction, and steganalysis)