6.0 Cryptography and PKI

6.1 Compare and contrast basic concepts of cryptography.

- **Symmetric algorithms**
- **Modes of operation**
- **Asymmetric algorithms**
- **Hashing**
- **Salt, IV, nonce**
- **Elliptic curve**
- **Weak/deprecated algorithms**
- **Key exchange**
- **Digital signatures**
- **Diffusion**
- **Confusion**
- **Collision**
- **Steganography**
- **Obfuscation**
- **Stream vs. block**
- **Key strength**
- **Session keys**
- **Ephemeral key**
- **Secret algorithm**
- **Data-in-transit**
- **Data-at-rest**
- **Data-in-use**
- **Random/pseudo-random number generation**
- **Key stretching**
- **Implementation vs. algorithm selection**
  - Crypto service provider
  - Crypto modules
- **Perfect forward secrecy**
- **Security through obscurity**
- **Common use cases**
  - Low power devices
  - Low latency
  - High resiliency
  - Supporting confidentiality
  - Supporting integrity
  - Supporting obfuscation
  - Supporting authentication
  - Supporting non-repudiation
  - Resource vs. security constraints

6.2 Explain cryptography algorithms and their basic characteristics.

- **Symmetric algorithms**
  - AES
  - DES
  - 3DES
  - RC4
  - Blowfish/Twofish
- **Cipher modes**
  - CBC
  - GCM
  - ECB
  - CTR
  - Stream vs. block
- **Asymmetric algorithms**
  - RSA
  - DSA
  - Diffie-Hellman
    - Groups
    - DHE
    - ECDHE
  - Elliptic curve
  - PGP/GPG
- **Hashing algorithms**
  - MD5
  - SHA
  - HMAC
  - RIPEMD
- **Key stretching algorithms**
  - BCRYPT
  - PBKDF2
- **Obfuscation**
  - XOR
  - ROT13
  - Substitution ciphers

6.3 Given a scenario, install and configure wireless security settings.

- **Cryptographic protocols**
  - WPA
  - WPA2
  - CCMP
  - TKIP
- **Authentication protocols**
  - EAP
  - PEAP
  - EAP-FAST
  - EAP-TLS
  - EAP-TTLS
  - IEEE 802.1x
  - RADIUS Federation
- **Methods**
  - PSK vs. Enterprise vs. Open
  - WPS
  - Captive portals

6.4 Given a scenario, implement public key infrastructure.

- **Components**
  - CA
  - Intermediate CA
  - CRL
  - OCSP
  - CSR
  - Certificate
  - Public key
  - Private key
  - Object identifiers (OID)
- **Concepts**
  - Online vs. offline CA
  - Stapling
  - Pinning
  - Trust model
  - Key escrow
  - Certificate chaining
- **Types of certificates**
  - Wildcard
  - SAN
  - Code signing
  - Self-signed
  - Machine/computer
  - Email
  - User
  - Root
  - Domain validation
  - Extended validation
- **Certificate formats**
  - DER
  - PEM
  - PFX
  - CER
  - P12
  - P7B