- Filename: eccouncil-ceh31250-v12-20-2-1-crypto-algorithms-and-implementations.md
- Show Name: CEHv12 (312-50)
- Topic Name: Cryptography - Cryptography
- Episode Name: Crypto Algorithms and Implementations
  ==

Crypto Algorithms and Implementations

Objectives:

- Algorithms
    - Symmetric
        - DES/3DES
        - RC(4/5/6)
        - Blowfish
        - AES
    - Asymmetric
        - RSA
        - Diffie-Hellman
- Hashing
    - MD(5/6)
        - https://datatracker.ietf.org/doc/html/rfc1321
    - SHA(128/256/512)
        - https://datatracker.ietf.org/doc/html/rfc3174
    - RIPEMD-160
    - HMAC
        - https://csrc.nist.gov/csrc/media/publications/fips/198/1/final/documents/fips-198-1_final.pdf
- Digital Signatures
- Hardware-based Encryption
    - TPM
    - USB
    - HSM
    - Hard-drive
- Other Encryption Implementations
    - Elliptic Curve
        - Advanced Algebraic equations to create shorter keys
            - Increased efficiency
    - Quantum
        - Stores encrypted information in the quanta
    - Homomorphic
        - Encrypted data can be modified without decrypting it