- Filename: eccouncil-ceh31250-v12-20-6-1-crypto-attack-countermeasures.md
- Show Name: CEHv12 (312-50)
- Topic Name: Cryptography - Cryptography
- Episode Name: Crypto-Attack Countermeasures
  ==========

Crypto-Attack Countermeasures

Objectives:

- Secure key sharing
- Use higher bit length hashing and symmetric key algorithms
    - At least 168 bit key size
        - Preferably 256 bit
- Use encryption with proven track record of security
    - At least 2048 bit key size
- Don't hard-code keys into source code or compiled into a binary
- Encrypt your keys with a password/passphrase
- Use IDS to monitor key exchanges
- Implement Key Stretching
    - Makes weak keys stronger through increasing their length
        - Password-Based Key Derivation Function 2 (PBKDF2)
        - bcrypt