- Filename: eccouncil-ceh31250-v11-20-1-1-cryptography-basics.md
- Show Name: CEHv11 (312-50)
- Topic Name: Cryptography - Cryptography
- Episode Name: Cryptography Basics
  ==

Cryptography Basics

Objectives:

- Purpose of Cryptography
    - Protect CIA + Non-Repudiation
- Crypto Types
    - Symmetric
    - Asymmetric
- GAK
    - Government Access to Keys
        - All keys are given to Gov
        - Gov securely stores keys
        - Gov can access keys with court order
        - Gov can 'eavesdrop' using keys
            - Like a wiretap order
- Ciphers
    - Classical Ciphers
        - Substitution
        - Transposition
    - Key Based
        - Private-key
            - aka Symmetric
        - Public-key
            - aka Asymmetric
    - Input Based
        - Block Cipher
        - Stream Cipher