- Filename: eccouncil-ceh31250-v12-20-1-1-cryptography-basics.md
- Show Name: CEHv12 (312-50)
- Topic Name: Cryptography - Cryptography
- Episode Name: Cryptography Basics
  ================================================================================

## Cryptography Basics

## Objectives:

---

- Purpose of Cryptography
    - Protect CIA + Non-Repudiation
      <P>
- Crypto Types
    - Symmetric
    - Asymmetric
      <P>
- 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
              <P>
- Ciphers
    - Classical Ciphers
        - Substitution
        - Transposition
            - Rail-Fence
                - `YOURE WATCHING ITPROTV`
                - ```
                  Y...E...C...G...P...V
                  .O.R.W.T.H.N.I.T.R.T.
                  ..U...A...I...T...O..
                  ```
                - Now Reads
                    - `YECGPV ORWTHNITRT UAITO`
    - Key Based
        - Private-key
            - aka Symmetric
        - Public-key
            - aka Asymmetric
    - Input Based
        - Block Cipher
            - Transforms plaintext 1 BLOCK at a time
                - BLOCK = 64/128/256 bits
                    - Examples: AES, Blowfish, 3DES
        - Stream Cipher
                  ```

- Transforms plaintext 1 BYTE at a time
    - Example: RC4