

- Filename: eccouncil-ceh31250-v11-20-5-1-cryptanalysis.md
- Show Name: CEHV11 (312-50)
- Topic Name: Cryptography - Cryptography
- Episode Name: Cryptanalysis

=====

Cryptanalysis

Objectives:

- What is Cryptanalysis?
 - Studying cryptosystems
 - Looking for exploitable weaknesses
- Methods
 - Linear
 - aka Known-Plaintext Attack
 - Requires both encrypted and plain-text data
 - Some plain-text could be guessed
 - Common words, names, and/or phrases
 - Goal is to reverse-engineer a decryption key
 - Further messages that were encrypted using that key could then be easily decrypted
 - Differential
 - Attacker defines the plaintext inputs and analyzes the results
 - Continues this process until the key is determined
 - Chosen-Plaintext Attack
 - <http://www.theamazingking.com/crypto-diff.php>
 - Integral
 - Type of Differential attack
 - Uses larger inputs
 - Applicable to block ciphers
- Code Breaking
 - Brute-Force
 - Frequency Analysis
- Attacks
 - Man-in-the-Middle
 - Meet-in-the-Middle
 - Reduces the time it takes to break encryption on ciphers that use multiple keys
 - Double-DES is vulnerable
 - Known-plaintext attack
 - $PT \rightarrow E^{k_2} \rightarrow E^{k_1} \rightarrow CT$

- Apply known-plaintext attack from both sides to 'meet in the middle'
- PT --> $E(k_1) = X$
- CT --> $E(k_2) = X$
- If X is the same for both then you've found the keys
- Side-Channel Attacks
 - Physical attack
 - Monitors environmental aspects of the target to reveal sensitive info
 - Power Usage
 - Electromagnetic Radiation
 - Light Emanation
 - Audio Emanation
- Hash Collisions
 - <https://crackstation.net>
- Related Key
 - WEP
- Rubber Hose Attack