Fundamentals of Computer Security

Crypto Basics

Lab 1

Contents

- Cryptos
- Steganography
- Cryptanalysis

Crypto Basics

- Write a program that encrypts and decrypts using the following algorithms (one algorithm for each one of them):
  - Substitution Cipher
  - Transposition Cipher
  - Rotor Machines or Simple XOR
- http://www.crypto-it.net/eng/simple/index.html

Steganography Basics

- Image: https://stylesuxx.github.io/steganography/
- Audio: Deep Sound (http://jpinsoft.net/deepsound)
- Covert channels: Tunnelshell (ICMP)

- https://betterprogramming.pub/a-guide-to-video-steganography-using-python-4f010b32a5b7

Cryptanalysis

- Decode the following data:
  “Chyrljuuh, j lxvyuncn cajwbvrbrxw fxdum rwludmn cqn bnwmna’b jwm anlnrena’b ljuu-brpwb, oanzdnwlh, brpwju bcanwpcq, anjmjkrurch, rwcnalnyc bcjcrxw wdvkna, crvn xo xarprw, dapnwlh, wdvkna xo yjacb rw cqn brpwju, wdvkna xo ldaanwc yjac, wdvkna xo unccnab rw ldaanwc yjac, Tnwwpadyyn mrblarvrwjwc (cx bcjcn fqrlq tnh fjb knrwp dbnm - CGV rw cqrb ngjvyun) jwm Padwmbcnuudwp (AWO rw cqrb ngjvyun). Cqrb fjb juu cajwbvrccnm nw lujra jwm oxuuxfnm kh cqn nwlryqnanm vnbbjpn-bnccrwp (KTC rw cqrb ngjvyun), cqn nwlryqnanm vnbbjpn jwm orwjuuh cqn nwm xo vnbbjpn brpwju.”

Cryptanalysis

- Describe the weaknesses of the enigma that led to the creation of Bombe which was the device used by the British cryptologists to help decipher German Enigma-machine-encrypted secret messages during World War II.

  https://en.wikipedia.org/wiki/Bombe