ITN 276
Computer Forensics I

Saturday, 2 February 2019

Agenda

- Announcements
- Quiz 2 Review
- Steganography Revisit
  - JSTEG Demo
- Cryptographic Hash Functions: Purpose and Use
  - MD5 & SHA
- Binary Operations
  - AND
  - OR
  - XOR
- Quiz 3: Hiding and Scrambling Data

Announcements

- Project 1: Due week 8
  - Questions from stragglers. You know who you are!
  - Interviewee contact information due today
    - If you haven’t called ~10 – 15 people/agencies, you’re not trying hard enough
- Project 2: Due weeks 14 - 16
  - Formal Demo/Presentation
  - You have your choice of deep-diving into:
    - Forensic Hardware
    - Forensic Software
    - Digital Forensics Topic of Interest

Announcements (Continued)

- Labs 1,2,4,6
  - Due week 8
  - Grading Structure Adjustment
    - To account for labs
    - Reduces weight of Midterm and Final

Quiz 2 Review

- The quiz focused on computer number systems
  - Binary
  - Hexadecimal

Steganography Revisit: OpenStego

- Available at https://openstego.com
- Download the appropriate release
  - I downloaded the source code zip file
  - Ensure ANT and Java is installed
  - Compile:
    - $ ant build.xml
  - Need Carrier (image) file & Message file
    - Project Gutenberg

File Format Specifications

- JPEG Spec: https://jpeg.org/jpeg/
- JPEG File Layout: http://vip.sugovica.hu/Sardi/kepnezo/JPEG%20File%20Layout%20and%20Format.htm
- PNG: https://www.w3.org/TR/2003/REC-PNG-20031110/
- PNG File Layout: http://www.libpng.org/pub/png/spec/1.2/PNG-Structure.html
- BMP File Layout: http://www.ece.ualberta.ca/~elliott/ee552/studentAppNotes/2003_w/misc/bmp_file_format/bmp_file_format.htm

Cryptographic Hash Functions: Purpose & Use

- Purpose:
  - Integrity Verification
  - Signature Generation & Verification
  - Password Verification
  - Proof-of-Work
  - File or Data Identifier
- Characteristics
  - One-Way
  - Infeasible to invert
  - Maps arbitrary sized input to fixed-sized bit string output (hash)
- Demo

Binary Operations

AND

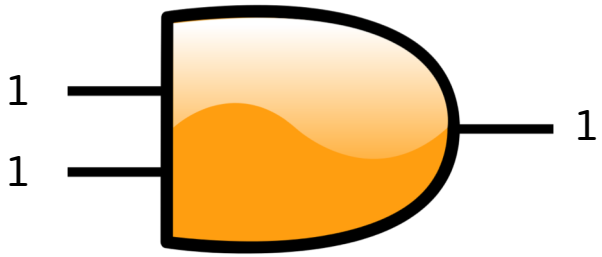
Inputs		Output
A	B	F
0	0	0
0	1	0
1	0	0
1	1	1

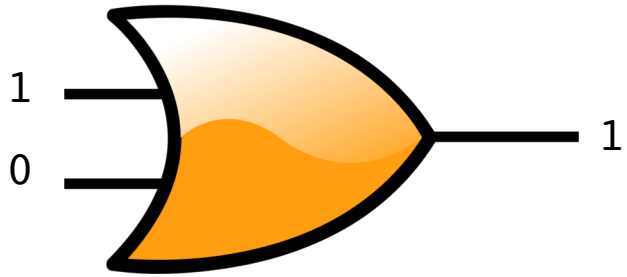
OR

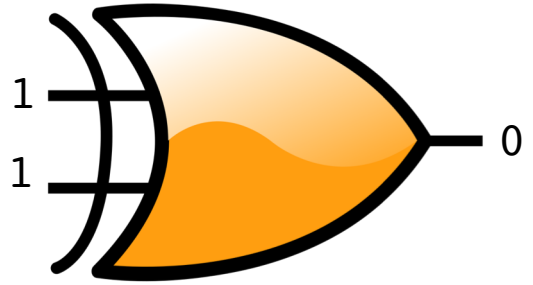
Inputs		Output
A	B	F
0	0	0
0	1	1
1	0	1
1	1	1

XOR

Inputs		Output
A	B	F
0	0	0
0	1	1
1	0	1
1	1	0







Binary Operations: Practice

```
1111 AND 1010 =
0001 OR  1010 =
1010 XOR 1010 =
00010001 AND 11111111 =
0xBC AND 0x22 =
```