Cryptography

Introduction to Capture The Flag Workshop

What do we need?

- Python 3

- Online Tools
  - factordb.com
  - CyberChef
  - dcode.fr
  - Cryptii

- Linux Tools
  - openssl
  - hashcat

Number Systems

- Things we've studied in HSC
  - Octal
  - Hexadecimal
  - BCD
  - And of course, Binary
- Base 16, 32, 64, 85, etc.

Examples – Number Systems

- 01001000 01100101 01101100 01101100 01101111 00100000 01010111 01101111 01110010 01101100 01100100

- 6>0eA/0J_AF_#/o+DbJ!F(G

- RkxBR3tUaGlzX2lzX2FfZmxhZ30=

Basic Ciphers

- Bitwise XOR
- Morse Code
- Caesar Cipher
- ROT13
- Baconian Cipher
- Vigenere Cipher
- Hill Cipher
  - And more!

Examples – Basic Ciphers

- Whfg ebgngr

- ..-. .-.. .- --. -... . . .--. ..--.- -... --- .--.

- ☞☹✌ ☝

Hash

- MD5
- SHA-1
- SHA-256
- SHA-512

Examples - Hash

#1 Crack The Hash

A hacker leaked the below hash online.Can you crack it to know the password of the CEO?

1ab566b9fa5c0297295743e7c2a6ec27

Iamtheflag

#2 Guess The Password (H/W)

A hacker leaked the below hash online. Can you crack it to know the password of the CEO? The flag is the password

Hash:
06f8aa28b9237866e3e289f18ade19e1736d809d

#3 HashError

we got this corrupted hash password from a file with a note

(password = sha-1(hash-result)).

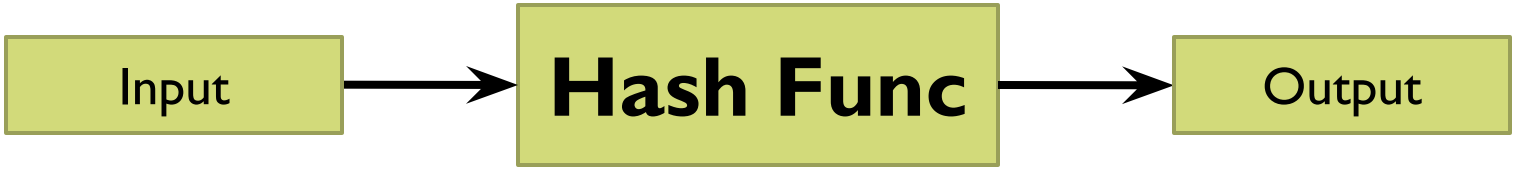
HASH:77be5d24ed2e3e590045e1d6o7e84i50d2799c19f48ede46804a8734e287df120f

Encryption

- Common Encryptions
  - RSA
  - AES
  - Blowfish

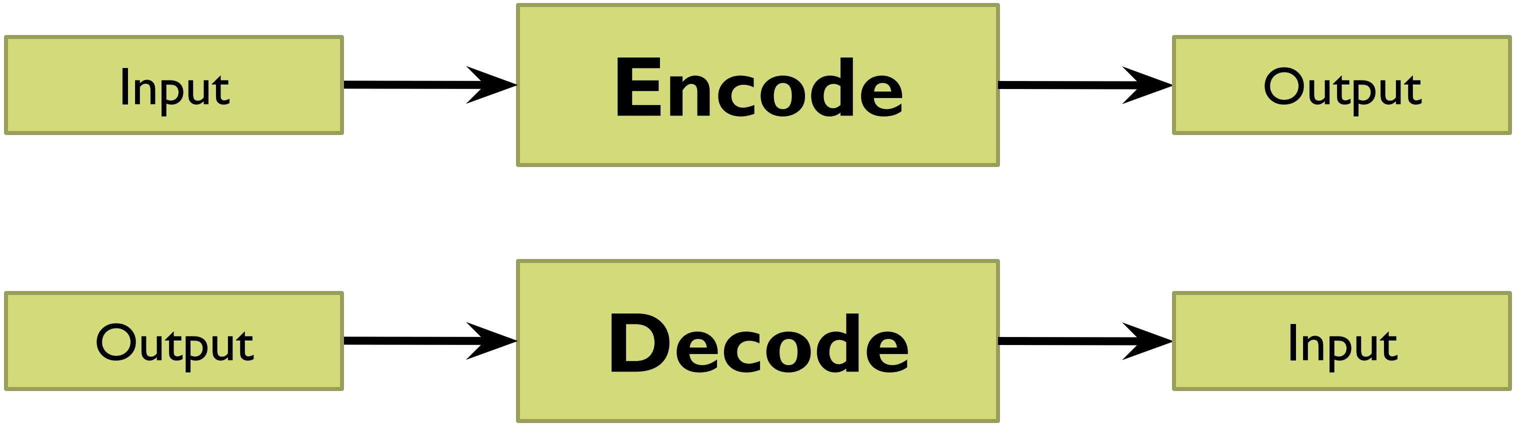
What’s the difference, anon?

- Hashing
  - Non-reversible



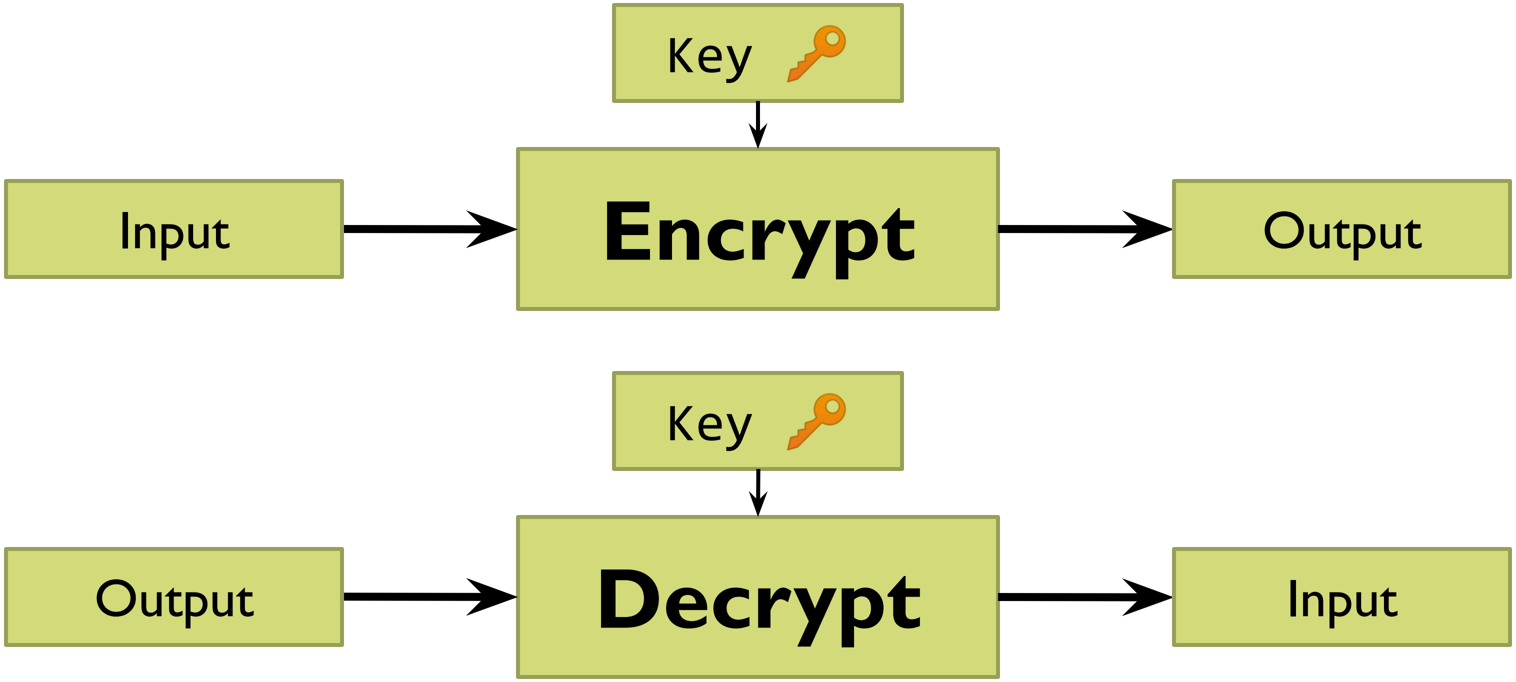
What’s the difference, anon?

- Encoding
  - Reversible



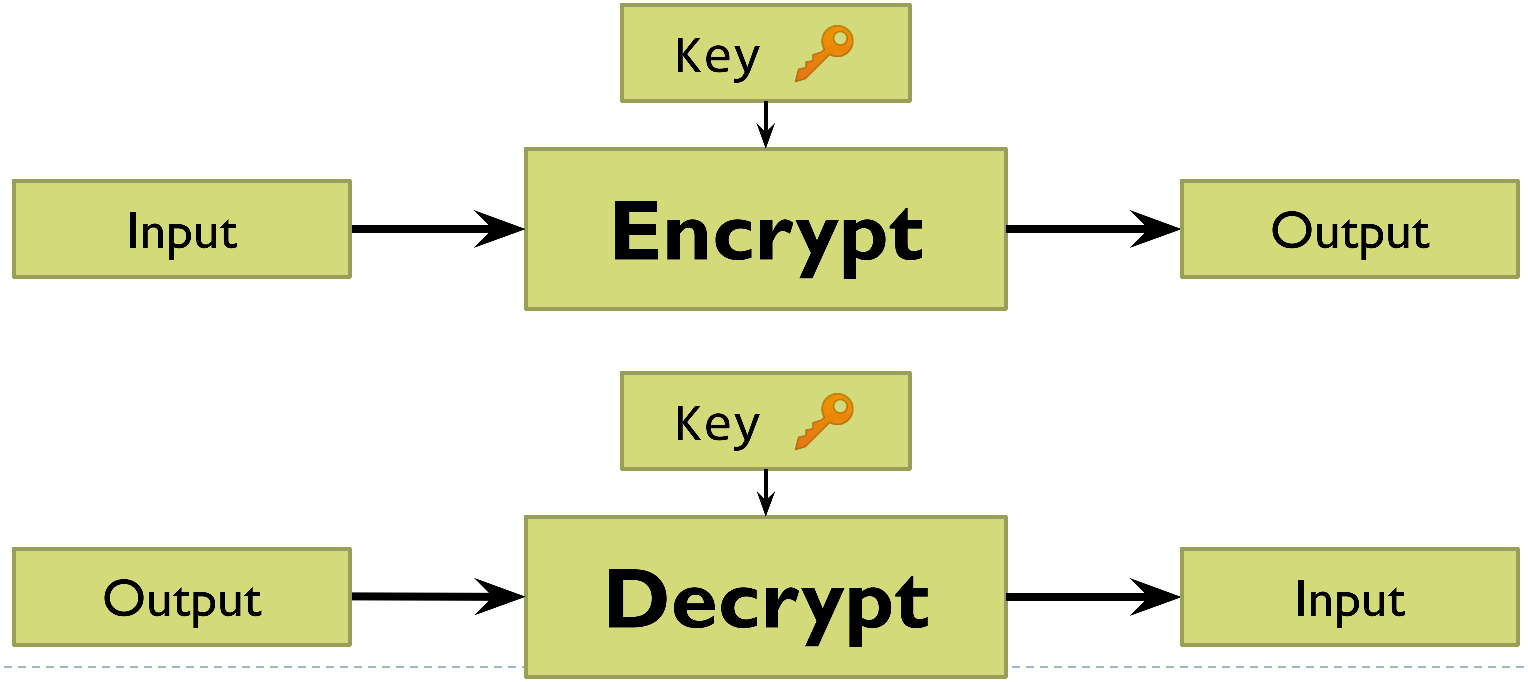
What's the difference, anon?

- Encryption
  - Reversible, but you need a **key**



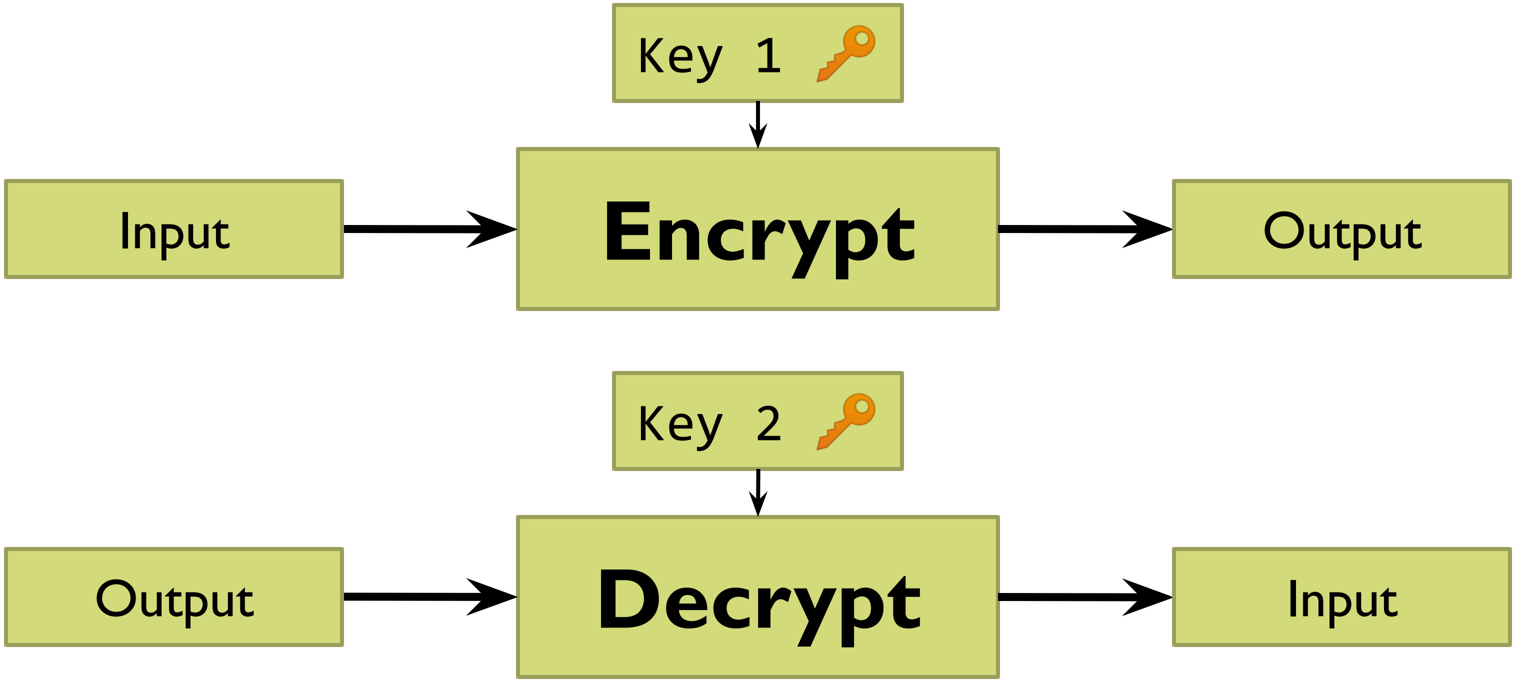
What’s the difference, anon?

- Symmetric Encryption
  - Same **key, and process** for encryption and decryption
  - Example: One Time Pad, AES, DES, Curve225
    - Tesla uses Curve225



What’s the difference, anon?

- Asymmetric Encryption
  - Different **key, and process** for encryption and decryption
  - Example: RSA, Elgamal



RSA

Follow VSCode