Information Security

Announcement

- Please come to the TA office hours!

A little bit STRING

leftover

http://www.pythonforbeginners.com/basics/string-manipulation-in-python

```
my_word = "Hello World!"

# REVERSING

print my_word[::-1]

begin = 1
end = 10
step = 2
print my_word[begin:end:step]

# TAKE HOME: figure out what the following mean by looking
# into Python manual or Googling
print ' '.join(reversed(my_word))
```

!dlroW olleH
el ol
! d l r o W o l l e H

```
# Strip off newline characters from end of the string
my_word = "   Hello World!   "

#strip()     #removes from both ends
#lstrip()    #removes leading characters (Left-strip)
#rstrip()    #removes trailing characters (Right-strip)

print my_word

print my_word.strip()

print my_word.lstrip()

print my_word.rstrip()
```

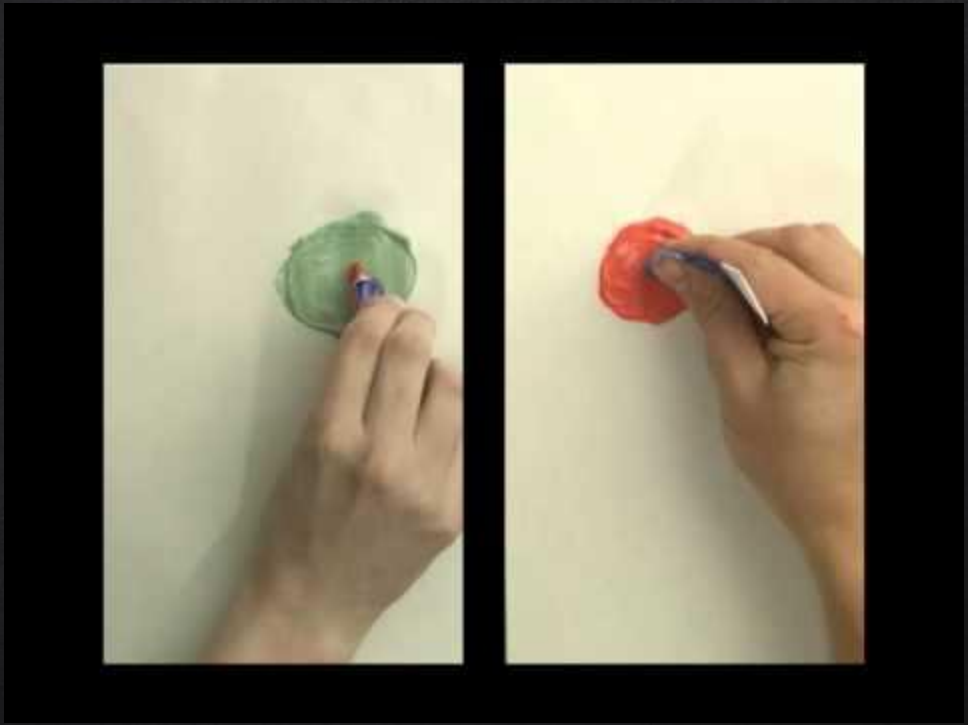
Hello World!
Hello World!
Hello World!
Hello World!

```
word = "Hello World"

print word.isalnum()       #check if all char are numbers
print word.isalpha()       #check if all char in the string are alphabetic
print word.isdigit()       #test if string contains digits
print word.istitle()       #test if string contains title words
print word.isupper()       #test if string contains upper case
print word.islower()       #test if string contains lower case
print word.isspace()       #test if string contains spaces
print word.endswith('d')     #test if string endswith a d
print word.startswith('H')   #test if string startswith H
```

False
False
False
True
False
False
False
True
True

Cryptography and key exchange



https://www.youtube.com/watch?v=YEBfamv-_do

Review

Communication errors

- Binary data error: a bit changes from 0 to 1 or 1 to 0

Solutions

- Repetition
- Redundancy

Some definitions

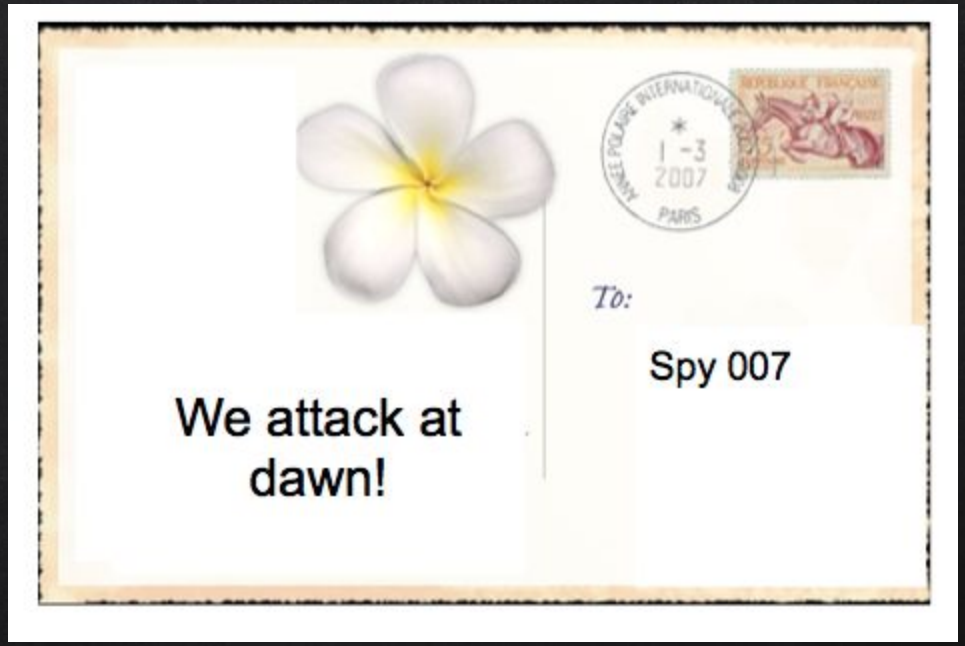
Parity: adding a bit so that the # of 1s is even

Checksums: add up all the data and store the result (LATER)

Hamming Codes: add several parity bits to detect and correct an error (LATER)

Keeping Secrets

- There is no privacy on the Internet
  - All messages get passed from one machine to the next
  - No control over which machines see a packet
  - A malicious machine could copy the message before passing it along
- Analogy
  - Sending a secret using a postcard
  - The mail carrier can read the message


ANNÉE POLAIRE INTERNATIONALE
1 -3
2007
PARIS
REPUBLIQUE FRANÇAISE
To:
Spy 007
We attack at dawn!

Information Security

Any good solution for information security must address:

- Confidentiality: data is protected from unauthorized access
- Integrity: data can only be modified by appropriate mechanisms
  - Detectable modifications
- Availability: the degree to which authorized users can access information for legitimate purposes
  - How can security backfire?

Copyright 2004 by Randy Glasbergen.
www.glasbergen.com

"The boss is worried about information security, so he sends his messages one alphabet letter at a time in random sequence.'

Security and the Internet

The internet has created new demand for secure communication

Want trusted communication without knowing for sure who the other party is:

- Email
- Shopping
- Software updates
- Media downloads

Cryptography

Cryptography

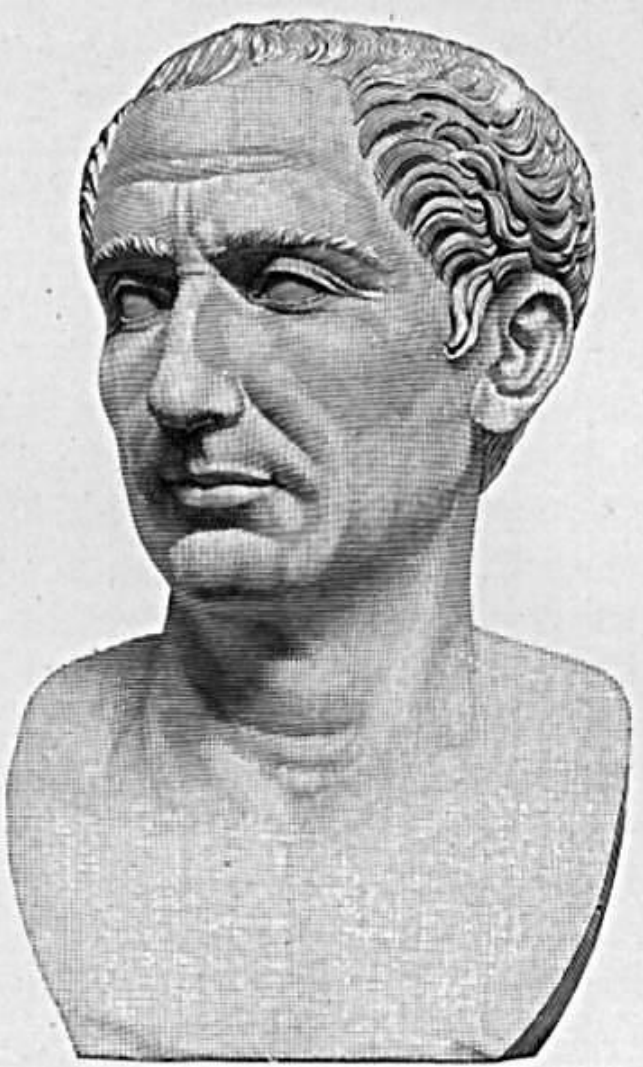
- The field of study related to encoded information
- Greek for secret writing
- Plaintext: original, readable
- Ciphertext: encoded, unreadable
- A cipher is an algorithm used to perform a particular type of encryption/decryption
  - Its key is the set of particular parameters that guide the cipher
- Different from a code, which links symbols to words in a code book

Substitution Ciphers

- Substitute one character in the plaintext message with another character
- To decode, perform the opposite substitution
- Example

Example: Caesar Cipher

- The Caesar cipher shifts the characters of a plaintext message by X positions in the alphabet
- The key consists of the value of X and the direction to shift



Substitution Ciphers

Plaintext: BRUTUS WILL BETRAY YOU

Ciphertext: ZPSRSQ UGEE ZCRPYW WMS

What is the key to the cipher used in this encryption?

Many other ciphers:

- Transposition ciphers
- Book ciphers
- One-time pad

Code-Breaking

- Cryptanalysis is the attempt to figure out the plaintext message without the cipher or its key
- How can a computer be used for code breaking?
  - Try different keys
  - Letter frequency analysis
  - Check results with an electronic dictionary

QUICK LAB!

- http://web.forret.com/tools/rot13.asp
- N HFS GWJFP YMNX HTIJ
- Please guess the key!

QUICK LAB!

- http://web.forret.com/tools/rot13.asp
- N HFS GWJFP YMNX HTIJ
- Please guess the key!
- Alphabet shift: 5


A'LA'IH, DO'NEH'LINI,
DO'NEH'LINI, A'LA'IH,
A'LA'IH, DO'NEH'LINI,
DO'NEH'LINI, DO'NEH'LINI,
A'LA'IH, A'LA'IH,
DO'NEH'LINI, A'LA'IH,
DO'NEH'LINI, DO'NEH'LINI,
DO'NEH'LINI . . .
FOR ADDED SECURITY, AFTER WE ENCRYPT THE DATA STREAM, WE SEND IT THROUGH OUR NAVAJO CODE TALKER.
. . . IS HE JUST USING NAVAJO WORDS FOR "ZERO" AND "ONE"?
WHOA, HEY, KEEP YOUR VOICE DOWN!

Key Exchange

- The sender and the receiver of an encrypted message must share the cipher key
  - Key used to encode and then decode the message
- Anyone with the key can decode the message
  - The key must be kept secret
- Isn't the key at as much risk of interception as the messages?
  - Should the key be encrypted before being sent?

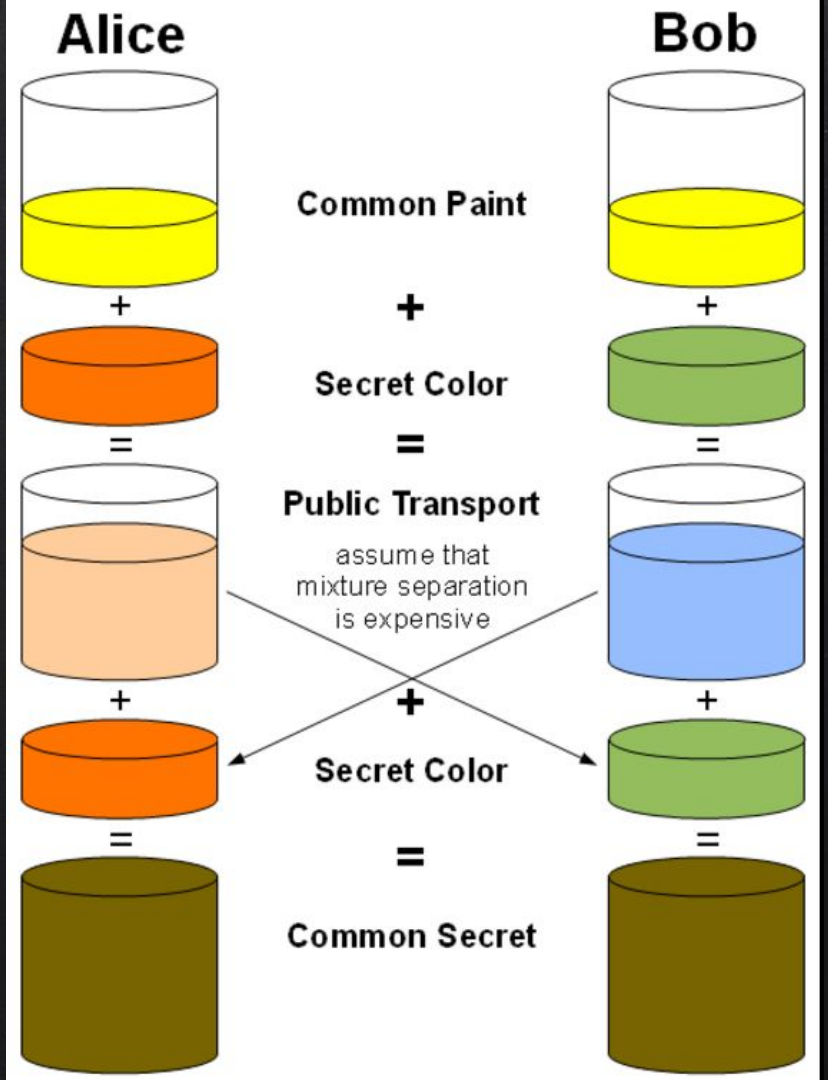
Key Exchange

- Key exchange deals with the problem of exchanging keys over a possibly insecure information channel
  - All communication between the 2 people is public
  - End up with a private key that only the 2 people know
  - Uses math called one-way functions
    - Easy to use
    - Difficult to reverse
- http://www.youtube.com/watch?v=LGGFpQMOAYQ

  Lecture 4 from 16:18 to 20:35

http://www.youtube.com/watch?v=LGGFpQMOAYQ

Lecture 4 from 16:18 to 20:35



Credit and further reading:
https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange

Diffie-Hellman Key Exchange

Basic Idea (using easier math)

- Each person picks a private #
- A public # is chosen by Bob and Arnold

- Mix (multiply) your private and public #s
  - Announce the results
- Mix your private # with the other person's shared #
- Use this as the key

- Bob picks 4
- Arnold picks 6

- Public # is 7

- Bob has 4 x 7 = 28
- Arnold has 6 x 7 = 42

- Bob has 4 x 42 = 168
- Arnold has 6 x 28 = 168

Better Mixing Math

- Multiplication is not a good mixing method
  - Easy to divide, test factors
  - If public # is 7, and Bob shares 28, easy to compute 28/7 = 4 (Bob's private #)
- Want a one-way function
  - Can't easily undo

Clock Arithmetic

- What happens when a clock reaches 12 o'clock?
  - Starts over at 0
- This is an example of modular arithmetic
  - Taking the module (mod), 13 mod 12 = 1
  - A clock is module 12
  - This is just the remainder after division
  - 23 mod 5 = 3 (23 divided by 5 is 4, remainder 3)
- Python: 23 % 5

```
# http://www.pythontutor.com/index.html
print 6%2
print 7%2
print 1125%11
```

0
1
3

More Definitions

- Raise a # to a power
  - 3^4 = 3 x 3 x 3 x 3
  - Multiple the base by itself 4 times
- Prime #s
  - A # greater than 1 that is only evenly divisible by itself and 1
    - 4 is not a prime as you can divide it by 1, 4 and also 2
    - 5 is a prime
    - 2, 3, 5, 7, 11, 13, 17, 19, 23, 31, 37, … are prime
    - Largest prime

As January 2016, the **largest known prime number** is $2^{74,207,281} - 1$, a number with 22,338,618 digits. It was found in 2016 by the Great Internet Mersenne Prime Search.

Credit: https://en.wikipedia.org/wiki/Largest_known_prime_number

Improved Public Key Exchange

- Each person chooses a private #
- Two public #s are agreed upon
  - Base B
  - Prime # P to be used as a modulo
- Make a mixed #
  - mixed = (B^private) mod P
- Share the mixed # and mix in your private #
  - shared secret = other mixed^private mod P

Blue means public, Red means private/secret.

1. Alice and Bob agree to use a modulus $p = 23$ and base $g = 5$ (which is a primitive root modulo 23).
2. Alice chooses a secret integer $a = 6$, then sends Bob $A = g^a \bmod p$
   - $A = 5^6 \bmod 23 = 8$
3. Bob chooses a secret integer $b = 15$, then sends Alice $B = g^b \bmod p$
   - $B = 5^{15} \bmod 23 = 19$
4. Alice computes $s = B^a \bmod p$
   - $s = 19^6 \bmod 23 = 2$
5. Bob computes $s = A^b \bmod p$
   - $s = 8^{15} \bmod 23 = 2$
6. Alice and Bob now share a secret (the number 2).

Credit and further reading:
https://en.wikipedia.org/wiki/Diffie–Hellman_key_exchange

Purpose of Key Exchange

- Go to a website with secure communications
  - Often https
  - Shows lock in corner of browser
- That website server and your computer have done a key exchange
  - Encrypts further communications
  - Hides credit card #, etc.

Try Out Key-Exchange

- Group Exercise
- Use calculator or Google to help
  - Google in the search bar:
    - 5^3 mod 7
    - B ^ private mod P
- Once you get a #, what do you do with it?
  - Use it as a key for a cipher

THANKS!

Any questions?

You can find me at
beiwang@sci.utah.edu

http://www.sci.utah.edu/~beiwang/teaching/cs1060.html

Credits

Special thanks to all the people who made and released these awesome resources for free:

- Presentation template by SlidesCarnival
- Photographs by Unsplash