23.11.20 16:01

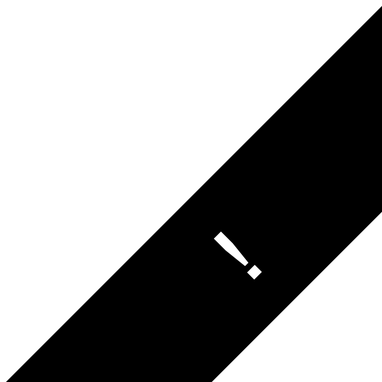
CSCI 101
Connecting with Computer Science
Computerised Society II

Jetic Gū

2020 Fall Semester (S3)

Announcement

- Get ready to present next Wednesday at the earliest
- Should include outline of your final essay, some key information etc.
- Maximum 10mins per student



Overview

- Focus: Social Implication
- Readings: R15
- Core Ideas:
    1. Cryptography
    2. Privacy

Cryptography

The Science of Hiding Stuff

Summary

What is cryptography?

- A method of protecting information and communication, such that only the intended parties can view its content

  - *crypto*
    late Middle English (in the sense ‘cavern’)
    from Latin crypta
    from Greek kruptē ‘a vault’, from kruptos 'hidden’

  - Simplest example: password!

Concept

Cryptosystem Pipeline

- Cryptosystems: a suit of algorithms designed to perform encryption

plain text

encryption

cipher text

decryption

plain text

"007, go to London and kill Spectre"

"sakhfgalBDKasgdhasidha!"

"007, go to London and kill Spectre"

Concept

P1
Cryptography

Caesar Cipher

- Given plain text in English, replace each letter with a different one **a fixed number of places** down the alphabet (let's say the number of places is $\mathcal{X}$)
  - e.g. $\mathcal{X}$=1, **plaintext** = `I like cheese`
    - **ciphertext** = `J mjlf difftf`
  - Receiver knows that $\mathcal{X}$=1, so he/she can recover the plaintext after receiving cipher text
  - $\mathcal{X}$ is called the **Key**

C → D
E → F
I → J
K → L
L → M
S → T

Example

Caesar Cipher

- $\mathcal{X} = 3$, **Cipher Text**: `Pb qdph lv Mhwlf`
- $\mathcal{X} = -5$, **Cipher Text**: `Fqq mfnq Atqijrtwy`
- What happens if you do not know the value for $\mathcal{X}$ (the key)?

Exercise

P1
Cryptography

Cracking the Caesar Cipher

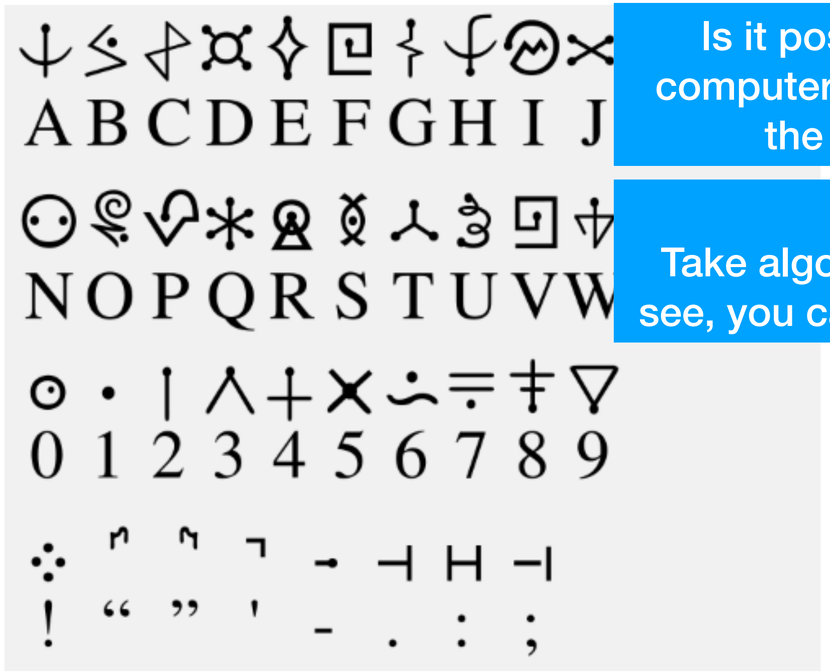
- **Brute-force**:
  - Given cipher text, tryout **all possible values** for $\mathscr{X}$, see which one makes sense
  - all possible values: $\mathscr{X} = [-25,25]$, 51 cases, a computer can do this easily
  - Computers can use a **dictionary** to filter out unlikely cases

Exercise

P1
Cryptography

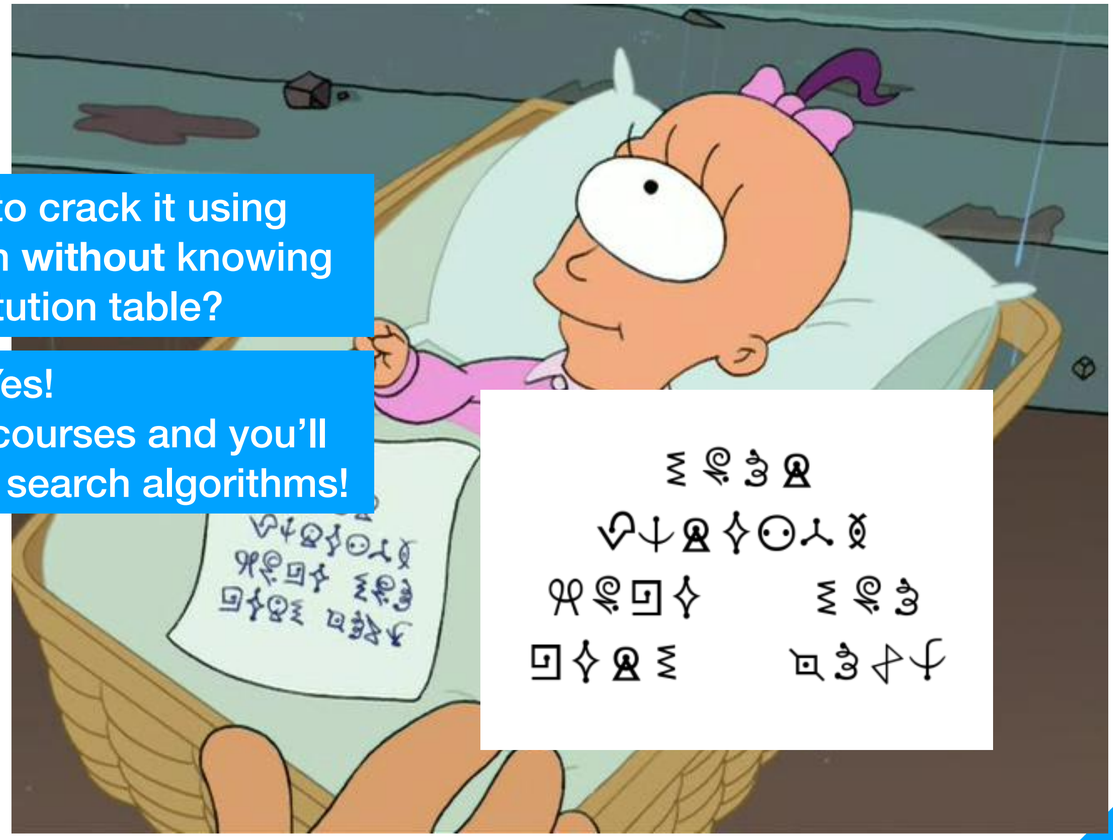
Alien Language Cipher

- Each Alien Symbol is an English letter
- Substitution Table:



Is it possible to crack it using computers, even **without** knowing the substitution table?

Yes!
Take algorithm courses and you'll see, you can use search algorithms!



Example

P1
Cryptography

Modern Digital Encryption

- RSA algorithm
  - Named after **R**ivest, **S**hamir, and **A**dleman
  - You have 2 keys: a public key, and a private key

Example

P1
Cryptography

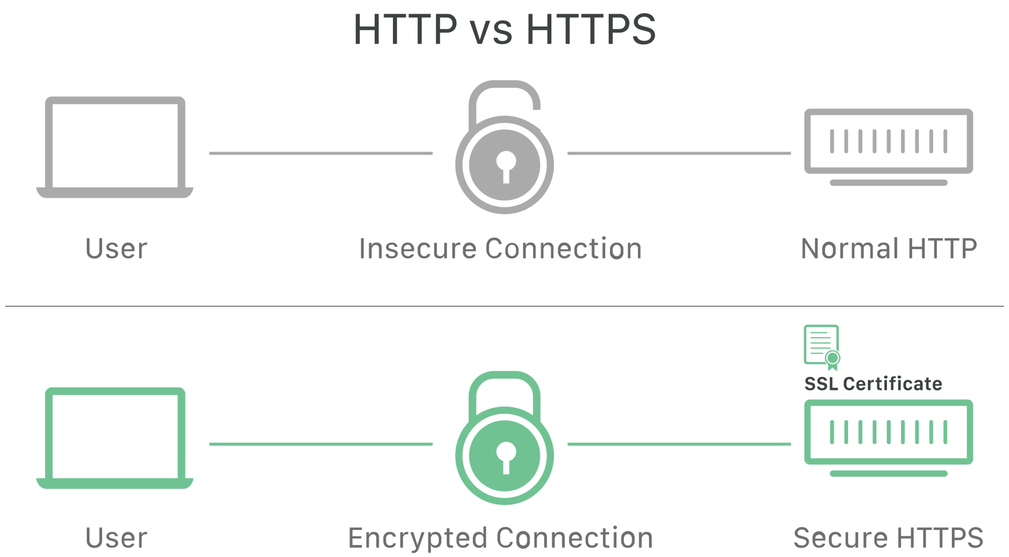
What makes RSA Amazing?

- The **public key** is different from the **private key**
  - The **public key** can be known by **everyone**, it is used to **encrypt** the message
  - The **private key** is only known to the **receiver**, it is used to **decrypt** the message
  - **The public key cannot* decrypt the message!**
    - Well, using brute-force it takes about 2700 years on a powerful computer
    - How? The magic of **math**!

Example

Cryptosystems

- **Cryptosystems like RSA**
  make secured information exchange possible
- **Most modern websites use encryption**
  So others can’t see what you are doing
- **Your computer is safe, you are not**
  Most common hacks come from **human error** such as scamming and phishing, not using encryptions, etc.



Concept

Privacy

And the lack of which

Summary

The Problem of Privacy

- State-of-the-Art **encryption technology** protects your information
- How does your information get **leaked**?
  - **Not using encryption**
  - Telling **untrustworthy** people your personal info and secrets
  - Installing **malicious** software (e.g. free downloads)
  - **Not protecting your browser history** from your mum
  - etc.

Concept

The Problem of Privacy

- Telling **untrustworthy** people your personal info and secrets
  - Facebook, Instagram, Twitter
  - Google, Microsoft, Apple
  - iMessage, SnapChat, Messenger
  - Whatever it is that kids nowadays use

Concept

What can you do?

- DO **NOT** SHARE IMPORTANT STUFF THROUGH EMAIL
  Email is the least safe tool for communication

- Be **Careful** when using online services
  Know your rights, never share unnecessary information

- Protect **Sensitive** Information
  Do **NOT** use your birthday as your password

- Always **Verify** the Person/Service Provider
  Prevent identity theft and Phishing/Scamming

- Do **NOT** believe in the promise of **FREE stuff**
  Chances are, these are viruses

Limitations of Privacy

- Anonymity
  - Cybercrime
  - Cyberbullying
  - Harrassment

Discuss