Week: 10 Date: 4/8/2021

|  |
| --- |
| 15-110 Recitation Week 10 |

# **Reminders**

* How was Quiz 4?
* HW5 due next Monday (4/12)
  + Tomorrow’s lecture on Managing Large Code Projects will help with functions 4 and 5
  + HW 5 collaboration form: <https://forms.gle/DUSMRE1CRBvf5NHi9>

**Overview**

* Quick internet questions
* Security review
* Encryption (meme cypher)
* Unit 3 Review / Open OH

|  |
| --- |
| Problems |

# **QUICK INTERNET QUESTIONS**

**Answer the following True/False questions:**

The internet is governed by a series of protocols, HTTPS is one of them. Answer

The net neutrality debate surrounds whether internet users should be able to create biased content and share it on public internet forums. Answer

There are an infinite number of IP addresses Answer

IP addresses can be static or dynamic Answer

All packets routed back to your computer from a website are guaranteed to be routed through the same wire. Answer

The internet is built such that if some components go down, it can continue operating with no interruption. Answer

**SECURITY REVIEW**

Quick Questions:

1. Describe the two main types of authentication.
   1. Answer 1
   2. Answer 2
2. What makes RSA nearly impossible to break?

Answer

1. What is the process called by which a VPN keeps a user’s internet activity private?

Answer

1. Match the descriptions below to the corresponding types of security attack:
2. Every student in 15-110 goes to gradescope at the same time to check their Test 4 grades

Answer

1. One malicious student connects to a class wifi access point and looks at the packets for their roommate's andrew ID and password to send prank emails from their accounts

Answer

# **MEME CIPHER/ENCRYPTION**

Consider this meme cipher below, where instead of letters mapping to pictures, **words** are mapped to pictures. Note: we can map letters to pictures but it would make messages way too large.

|  |  |
| --- | --- |
| Carnegie Mellon |  |
| surprised |  |
| I |  |
| good |  |
| cool |  |
| grade |  |

For the following problems, exclude common articles when encrypting and decrypting.

Encrypt:

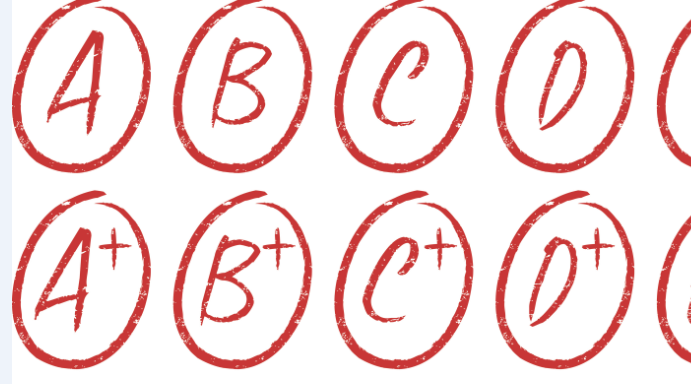
**Carnegie Mellon is cool.**

Insert pictures

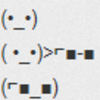
**I got a good grade at Carnegie Mellon**

Insert pictures

Decrypt:



Answer



Answer

Answer these questions:

What is the plaintext? Answer

What is the ciphertext? Answer

Is this a symmetric or asymmetric encryption algorithm? Answer

How many keys are used? Answer

What is the key? Answer

What is the runtime to break this cipher? Keep in mind that an adversary knows each meme corresponds to a word, but they don’t know which words are being used in the message. This means they would have to check each possibility in the dictionary. For this question, assume there are N words in the dictionary and 6 memes that are used. Answer

# 

# **UNIT 3 REVIEW & OPEN OH**

Unit 3 topics: concurrency, parallelism, internet, and authentication and encryption

Do you have any questions on these topics?

Kahoot Review: <https://kahoot.it>

Have you started HW5? (don’t forget to fill out the collaboration form if you want to talk with other students!)