Week: 10 Date: 11/10/2022

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

**Reminders**

* How was Exam 2?
* HW5 due Monday 11/14 at noon.

**Overview**

* Security Review
* Meme Cipher Encryption
* RSA
* Top Down Preview
* OH

| Problems |
| --- |

# **Security Review**

Describe the two main types of authentication.

|  |
| --- |

What makes RSA nearly impossible to break?

|  |
| --- |

Match the descriptions below to the corresponding types of security attack:

| Every student at CMU goes to SIO at the same time to check their schedules  Answer: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  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**

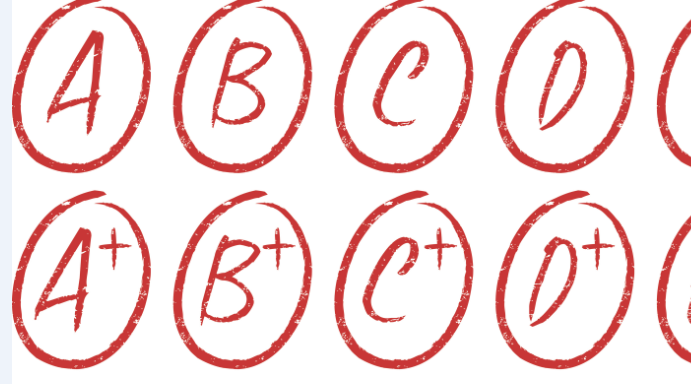
| Carnegie Mellon |  |
| --- | --- |
| surprised |  |
| I |  |
| good |  |
| cool |  |
| grade |  |

Encrypt:

**Carnegie Mellon is cool.**

|  |
| --- |

Decrypt:



|  |
| --- |

What is the plaintext? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

What is the ciphertext? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Is this a symmetric or asymmetric encryption algorithm? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

How many keys are used? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

What is the key? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

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.

**RSA Recap**

Elisa wants to send a super secret message to Gabe about the 110 exam. She translates the message into a number: **11**, and then finds Gabe’s public key online. His key is **(5, 133).**

We create the ciphertext by: \_\_\_\_\_\_\_\_\_\_\_\_\_

Elisa puts this number on her instagram story, and tags Gabe. Why should this not worry Gabe or Elisa?

Then Gabe sees it and decrypts it with his \_\_\_\_\_\_\_\_\_\_\_\_\_\_ **(65, 133)** by \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Gabe gasps!

# **Top Down Preview**

Avani wants to build a game where you try to remove the numbers 2 through 10. The game involves rolling two dice, and summing them. You can then remove **a pair of numbers** that add up to the number, or that **number itself.** When you remove all the numbers you win, if you get stuck and can’t remove any numbers you lose. Ex: the first turn I roll a 3 and a 4. I can either remove 7, (5,2), (3,4), etc.

How might we describe the steps needed to make this game in plain english:

|  |
| --- |

Now download the starter code. Avani created a couple helper functions that implement these steps, but she forgot to write the playGame function! Let’s help her out. (First look over the helper functions! What are they doing?)

**OH**

Feel free to ask questions 1:1 about HW or if you want to talk about how the exam went.