Week: 10 Date: 03/28/2024

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

**Reminders**

* How was Exam 2?
* HW5 due Monday 04/01 at Noon.
* [Feedback form](https://forms.gle/dWgvmGvTSMbRi7rv5)

**Overview**

* Meme Cipher Encryption
* RSA
* Top Down Preview

| Problems |
| --- |

# **Meme Cipher Encryption**

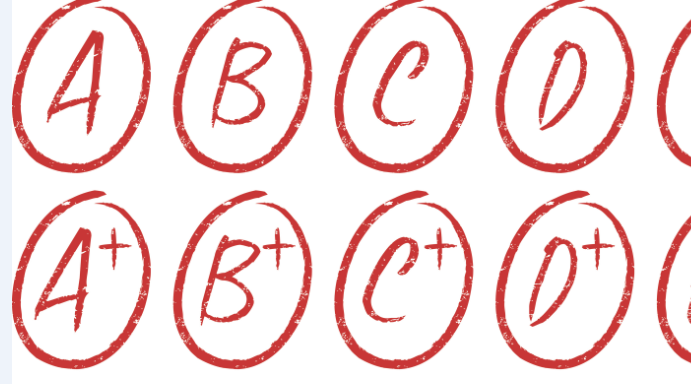
| Carnegie Mellon |  |
| --- | --- |
| surprised |  |
| I |  |
| good |  |
| cool |  |
| grade |  |

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**

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

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

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

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

Sean gasps!

# **Top Down Design**

Amogh 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:

| I |
| --- |

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