Work Log Paul Holderbaum

Main responsibilities:

- Key generation
- Encryption
- Decryption
- Game Functionality
- I/O corrections and input validation
- Report

Date	**Task**	**Time**	**Problem**	**Solution**	**Remark**
30 Nov.2023	Read the lab description and try to understand how RSA-encryption works	2hrs			-watched videos of Eddie wo lectures on YouTube
1 Dec.2023	Division of tasks for project	1hr	Estimating how long a task might take		
	Creation of GitHub repo Implementation of the project file structure	1hr 30	Merge conflicts due to lack of experience	Use GitHub with only one user for now	
4 Dec.2023	is_prime()	35min			
	gcd()	45min	worked well for small inputs only.	gcd Euclidean algorithm from Coursera	Learned about runtime complexity and Big-O notation

	modulus()
	phi()
		40min			

	public_exponent()	2hrs	Stack oveflow Random numbers did not work	Used only the first possible value of e, so the loop ended faster.	
5 Dec 2023	private_exponent()	3hrs	The extended Euclidean algorithm was hard to implement and did not work all the time with my implementation.	Used GCD extended Euclidean algorithm from geek for geeks.	
6 Dec 2023	encrypt()	4hrs	Modular exponentiation and bit shift operations Finding how to convert from a string to a number	ChatGPT Used ASCII and type casting as a reference.	
	decrypt()	3 hrs	Dealing with non ascii values	Replaced the decrypted character with ‘?’	
8 Dec 2023	public_exponent()	2hrs		implemented random numbers and made the algorithm run faster by skipping all even numbers in the loop.	Seeded the random number with the Current time, to simulate true randomness
	Input validation on all functions.	2hrs			
10 Dec 2023	Correction of read_cryp() + validation of input of all I/O functions	2hrs			

14 Dec 2023	Function testing and Optimization trying to get max run times of O(n)	2hrs			
15 Dec 2023	Brainstorm Ideas for additional functionality	1hr 30			
	Riddle game Implementation	2hr			
16 Dec 2023	report	2hr			
17 Dec 2023	report	2hr 45			
21 Dec	report	3 hr			
		37.5			