Introduction to Cryptography: Final Exam

Name: Student Name

By turning in this assignment, I agree to abide by and uphold the Honor System of Introduction to Cryptography as well as the additional policies outlined on the course website.

1 Problem 1

Alice wants to send Bob information over the internet. She wants the information to be encrypted such that only Bob can unlock the information.

1. Should Alice use Public or Private Key Cryptography?
2. Describe a mechanism for the system you could build to create this system. Include the steps for encryption, decryption, and any initialization of constants.
3. How do you know that your system is secure? Be as thorough as possible.

2 Problem 2

A videogame is divided into n files. The creators of the game want people to download the encrypted videogame files and then buy a unique key to unlock the videogame.

1. Describe a protocol for encrypting the videogame's n files and generating the keys.
2. Describe the security of your system.

3 Problem 3

A Shamir secret sharing scheme has been set up for 10 committee members. Four members of the committee need to be present to unlock the secret.

The keys of five members are: $(1, 299), (22, 491), (-3, 221), (-4, 2), (5, 101)$

1. Compute the shared secret (stored on the y-axis) by hand, showing all of your work.
2. Generate 5 new keys that match the original function (show all work).
3. Generate 5 new keys that match the original secret, but not the original function.