**CS 430 – Introduction to Computer Security**

**Project 2**

1. Suppose that Alice's RSA public key is (N, e) = (33, 3) and her private key is d = 7.
2. If Bob encrypts the message M = 19 using Alice's public key, what is the ciphertext C? Show that Alice can decrypt C to obtain M.
3. Let S be the result when Alice digitally signs the message M = 25. What is S? If Bob receives M and S, explain the process Bob will use to verify the signature and show that in this particular case, the signature verification succeeds.
4. Consider the knapsack cryptosystem. Suppose the public key consists of (18, 30, 7, 26) and n = 47.
5. Find the private key, assuming m = 6.
6. Encrypt the message M = 1101 (given in binary). Give your result in decimal.
7. Consider the elliptic curve



1. Verify that the point P = (2, 7) is on E.
2. Suppose this E and P = (2, 7) are used in an ECC Diffie-Hellman key exchange, where Alice chooses the secret value A = 12 and Bob chooses the secret value B = 31. What value does Alice send to Bob? What does Bob send to Alice? What is the shared secret?

For this problem, write code. Since you will apply the **mod** operator also on negative numbers, use the following definition:

a **mod** b = (a % b + b) % b

*What to upload in a compressed folder (Canvas):**Your code, the results, your conclusions/observations.*