Introduction to Cryptography Final Spring 2021

Answer two out of three questions below:

1. [20 pts] In a t*hree- prime* RIVEST-SHAMIR-ADLEMAN (RSA) public- key cryptosystem, with n = 1771, e = 7, Bob receives a ciphertext from Alice that is *753 mod 1771*. Compute the secret exponent *d* and Alice's plaintext using Chinese Remainder Theorem.

2. [20 pts] In the ELGAMAL public key crypto system with P =263, Bob, Alice and Carol use smallest generator g for Z_p*. One morning Bob decides to send same message to Alice and Carol.

    a. What is Bob's half mask if his secret component b = 7?
    b. What is Alice's half mask if her secret component a = 5?
    c. What is carol's half mask if her secret component c = 9?
    d. One fine day Alice and Carol receive a ciphertext from Bob containing the sequences (14, 129) and (14, 218) respectively, where half mask is the first element and cipher is the second. What is the ASCII character that Bob sent to Alice and Carol? Show all your work including the modular inverse computation.

3. [20 pts] In BLUM GOLDWASSER probabilistic public key cryptosystem with n = 1333, Bob receives a ciphertext from Alice containing the sequence (001, 101, 010, 001, 000, 110, 001) and the number x_8 = 453 mod 1333. Show How Bob recovers the plain text form cipher text and what is the plaintext.