Tutorial 3: Public Key Crypto

1. Suppose that Alice's RSA public key is *(N,* e) = (33,3) and her private key is *d* = 7.

   a. 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.*
   b. 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.

2. Why is it a bad idea to use the same RSA key pair for both signing and decryption?

3. To speed up RSA, it is possible to choose e = 3 for all users. However, this creates the possibility of a cube root attack as discussed in the lecture.

   a. Explain the cube root attack and how to prevent it.
   b. For *(N,* e) = (33,3) and *d* = 7, show that the cube root attack works when M = 3 but not when *M* = 4.

4. Consider the Diffie-Hellman key exchange protocol. Suppose that Alice sends her Diffie-Hellman value, g^a mod *p,* to Bob. Further, suppose that Bob wants the resulting shared secret to be a specific value *X.* Can Bob choose his Diffie-Hellman value so that, following the protocol, Alice will compute the shared secret *X?* If so, provide precise details and if not, why not?

5. This problem deals with Diffie-Hellman.

   a. Why is *g* — 1 not an allowable choice for *g?*
   b. Why is *g* = *p* — 1 not an allowable choice for *g?*

6. Suppose that for the knapsack cryptosystem, the superincreasing knapsack is (3,5,12,23) with *n* = 47 and *m* = 6.

   a. Give the public and private keys.
   b. Encrypt the message M = 1110 (given in binary). Give your result in decimal.

7. Consider the knapsack cryptosystem. Suppose the public key consists of (18,30,7,26) and *n* = 47.

   a. Find the private key, assuming *m* = 6.
   b. Encrypt the message M = 1101 (given in binary). Give your result in decimal.

8. Consider the elliptic curve:

$$E: y^2 = x^3 + 11x + 19 \pmod{167}.$$

a. Verify that the point P = (2, 7) is on E.

b. Suppose this E and $P = (2, 7)$ are used in an ECC Diffie-Hellman key exchange, where Alice chooses the secret value $A = 2$ and Bob chooses the secret value $B = 3$. What value does Alice send to Bob? What does Bob send to Alice? What is the shared secret?

c. Provide an implementation of ECC that computes automatically the shared secret between Alice and Bob. (i.e. Given the Input: the parameters of elliptic curve, coordinates of the point on the curve and the two secret values A and B. Calculate Output: shared secret coordinates)