10 points for each of the questions 1-8

1. Textbook 4.5.4: What is a practical method for finding a triple of keys that maps a given plaintext to a given ciphertext using EDE.

2. Manually complete the following operations. Explain your reason for each step. (Hints: Use Fermat Theorem, Euler Theorem, etc.)

(a) 1234^{16} mod 17
(b) 54^{51} mod 17
(c) ø(51)
(d) gcd(33, 121)
(e) 2^{-1} mod 17
(f) $\log_{2,5}(4)$

3. A server uses a Challenge-Response protocol to authenticate users. The server stores the legitimate users' public key. Each time when a user wants to login, the server generates a random challenge and sends it to the user. The user then generates a digital signature on his/her workstation and sends the digital signature to the server. The server authenticates the user by verifying his/her signature on the random message. Describe an attack against the server.

4. Perform encryption and decryption using the RSA algorithm for p = 5; q=11, e=3; M = 9. Show how you got your results.

5. Bob uses Alice's public key <e, n> to encrypt an original message M by computing C = M^e mod n. Eve doesn't know Alice's private key d, but she was told that M and n have a non-trivial common divisor (i.e., the common divisor is not equal to 1). Suppose Eve intercepts C. Is it possible for Eve to figure out Alice's private key d and obtain Bob's original message M? (Hint: Eve may test whether or not C is a prime number)

6. Bob intercepts a ciphertext C intended for Alice and encrypted with Alice's public key e,n. Bob wants to obtain the original message M = C^d mod n. Bob chooses a random value r less than n and computes

$Z = r^e \bmod n$
$X = ZC \bmod n$
$t = r \bmod n$

Next, Bob gets Alice to authenticate (sign) X with her private key, thereby decrypting X. Alice returns Y = X^d mod n. Show how Bob can use this information now available to him to determine M.

7. Consider the following key establishment protocol. Alice selects a random number x and computes x^g, where g is a number that is known to the public. Bob selects a random number y and computes y^g. Alice and Bob send x^g and y^g to each other. The shared key is computed as $(xy)^g$. Describe an attack against such key establishment protocol.

8. Alice and Bob use the Diffie-Hellman protocol to create two keys k1 and k2. In generating k1, Alice selects a random number x and computes SA = g^x mod p. Bob selects a random number y and computes SB = g^y mod p. Alice and Bob exchange SA and SB, and k1 = g^{xy} mod p. In generating k2. Alice chooses another random number x1 but Bob still uses the same random number y. Suppose an eavesdropper knows that x and x1 differ each other by t (i.e., ||x-x1|| = t). Given the knowledge of k1 and a pair of plaintext M and ciphertext C encrypted by k2, can the eavesdropper find out k2?