CSS337: Secure Systems
Assignment 2: Cryptography

1. In this problem, we will compare the security services that are provided by digital signature (DS) and message authentication codes (MAC).We assume that Oscar is able to observe all messages send from Alice to Bob and vice versa. Oscar has no knowledge of any keys but the public one in case of DS. State whether and how (i) DS and (ii) MAC protect against each attack. The value auth(x) is computed with a DS or a MAC algorithm, respectively.

a. (Message integrity) Alice sends a message x "Transfer $1000 to Mark" in the clear and also sends auth(x) to Bob. Oscar intercepts the message and replaces "Mark" with "Oscar". Will Bob detect this?
b. (Replay) Alice sends a message x "Transfer $1000 to Oscar" in the clear and also sends auth(x) to Bob. Oscar observes the message and signature and sends them 100 times to Bob. Will Bob detect this?
c. (Sender Authentication with cheating third party) Oscar claims that he sent some message x with a valid auth(x) to Bob, but Alice claims the same. Can Bob clear the question in either case?
d. (Authentication with Bob cheating) Bob claims that he received a message x with a valid signature auth(x) from Alice (e.g., "Transfer $1000 from Alice to Bob") but Alice claims she has never sent it. Can Alice clear this question in either case?

2. Perform encryption and decryption using the RSA algorithm (Figure 3.10) for the following:

a. p= 3; q= 11, e = 7;M =5
b. p =11; q =13, e= 11;M= 7
c. p= 17; q= 31, e= 7;M =2

3. In a public-key system using RSA, you intercept the ciphertext C = 10 sent to a user whose public key is e = 5, n = 35.What is the plaintext M?

4. In an RSA system, the public key of a given user is e = 31, n = 3599.What is the private key of this user?

5. Consider a Diffie-Hellman scheme with a common prime q = 11 and a primitive root α =2.

a. If user A has public key Y_A =9, what is A's private key X_A?
b. If user B has public key Y_B = 3, what is the shared secret key K?