Auto-Evaluation Questions
(Public Key Cryptography and Digital Signatures)

1. What are the security properties of a public-key cryptosystem?

2. List and briefly define three uses of a public-key cryptosystem.

3. Present a public-key cryptosystem that can be used for confidentiality, authentication and key-exchange

4. For what purpose is used the Diffie-Helman algorithm?

5. What is the difference between a private key and a secret key?

6. What is a digital signature? Explain the essential of a digital signature construction

7. If Alice sends to Bob a Message M and a digital signature of M, how can Bob validate the digital signature to be sure that ir comes from Alice?

8. Perform encryption and decryption using the RSA algorithm for the following:

   a) p=3; q=11, e=7; M=5

   b) p=5; q=11, e=3; M=9

   c) p=7; q=11, e=17; M=8

   d) p=11; q=13, e=11; M=7

   e) p=17; q=31, e=7; M=2

   Hint: Decryption is not as hard as you think; use some finesse.

9. 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?

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

11. Suppose we have a set of blocks encoded with the RSA algorithm and we don't have the private key. Assume $n = pq$, e is the public key. Suppose also someone tells us they know one of the plaintext blocks has a common factor with n. Does this help us in any way?

12. Suppose Bob uses the RSA cryptosystem with a very large modulus n for which the factorization cannot be found in a reasonable amount of time. Suppose Alice sends a message to Bob by representing each alphabetic character as an integer between 0 and 25 (A : 0, . . ., Z : 25), and then encrypting each number separately using RSA with large e and large n. Is this method secure? If not, describe the most efficient attack against this encryption method.

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

    If user A has public key $Y_A = 9$, what is A's private key X_A?

    If user B has public key $Y_B = 3$, what is the shared secret key K?

14. Try to design an authentication and key-distribution protocol (only supporting the necessary secure association parameters required) for the Part II of your TP1 assignment.
15. Design an authenticated Diffie-Hellman key-exchange between Alice and Bob, using RSA Digital Signatures. You must precise how to process the public DH numbers in order to provide a secure authentication.
16. According to your proposal for the question 15, do you think that something can differ if we use different digital signatures using other methods (ex., DSA, or ECC-DSA).
17. A message represented as an integer will be encrypted with RSA using OAEP. Padding. The idea is to use RSA keys of 2048 bits, mod 2048. The integer representing the message M has 2032 bits. Is it possible to make the encryption? Why?
18. Repeat 17 if we will use RSA eith PKCS#1.
19. Repeat 17 if we want to sign the message using RSA with SHA 286, and PSS as padding.
20. Repeat 17 if we want to sign the message using RSA with SHA 512, and PKCS#1 as padding