**1)**      **Question about DH (all discussed on the board in detail, slides available for back-up)**

a.       Describe DH private/public keys for Alice and Bob. Show how DH key exchange works.

b.      How how Oscar can perform MiTM as described on the board and say why this is possible

c.       Depict how MiTM can be prevent and which additional entity is needed for this (and why)

d.      ElGamal encryption scheme is given. Describe in detail how DH protocol serves as a building block for Elgamal encryption (remember four key point discussed twice)

**2)**      **Hash-function Fundamentals (discussed in all occasions)**

a.       What are the four essential properties of a cryptographic hash function (you can enumerate more if you wish)

b.      What is Target Collision Resistant (TCR) property, and  how can it be simply achieved? What is the role of TCR in the RSA dihital signature of Coron described over the board?

c.       Describe HMAC construction. You can depict block diagram or write its expression.

**3)**      **Merkle Hash Tree (MHT)**

a.       Similar question to HW2 Question 1 but with a different message.

**4)**      **One-time/Multiple-time Signatures**(covered on the board in multiple occasions): Remember Lamport signature with |pk|=|sk|=|sigma|=2|f|O(L’)O(L) overhead. Describe, *in full detail* (not just verbally, write chains and equations as done on the board), four variants discussed in the class

**a.**       Variant I: Reduce one of the linear factors from the overhead by just simply applying a crypto function

**b.**      Variant II: Reduce the size of |sigma| from Variant I to half by doing a signing trick

**c.**       Variant III: For |sk| with *l*-keys in it, it is possible to store only one key and obtain other keys from it. Show how it is done. Also, a public key can be used K times instead of one. Show how it can be done (similar method for both).

**d.**      Variant IV: Given state i,  show we do not have to store O(L) public key. The public key storage can be reduced to constant with a recursive strategy. Write down this simple strategy and explain what is the potential drawback of it.

**5)**      **Digital Signatures Relying on DLP:** A question in the line of HW2 Question 2. In it, you will work on Schnorr signature. In midterm, you will apply exactly the same principle, but for DSA algorithm that I will discuss over the board on Tuesday.

**6)**      **RSA and Hybrid Crypto with Order of Primitives:**I have descripted this question in detail already during the class, hence I will not repeat all details. Things to remember

**a.**       Given RSA private/public key, know how to encrypt/decrypt

**b.**      Given RSA private/public key, know how to sign/verify, where you will be using Coron version such as \sigma= H(m||r)^{d}  \bmod  n

**c.**       Know the order of compression, encryption and HMAC, which is one of the questions in HW1.

**d.**      Given all the above building blocks, writing the protocol will be easy. Notations will be provided.

You had both HW1 and HW2 around 20 days before, discussions on the board and now you also know the questions. I think it should be “computationally infeasible” for you not to enjoy and succeed  .