Exam exercises, SIS + MRI: Advanced crypto:

1. List the properties of a hash function.
   Assume we have a public-key encryption scheme. We generate the secret key sk and the public key pk, then destroy the secret key sk. We implement a hash scheme by using the PK Encryption scheme as $H(m) \coloneqq Enc_{pk}(m)$.
   a. Should the PK Encryption scheme be deterministic or can it be probabilistic?
   b. In the case of textbook RSA, the system setup is:
      i. Generate large primes p and q, set $N \coloneqq pq$ and $\varphi(N) \coloneqq (p-1)(q-1)$
      ii. Public key: find e with $GCD\big(e, \varphi(N)\big) = 1$ (they are co-prime). Publish (N,e)
      iii. Secret key: find d such that $de = 1 \; mod \; \varphi(N)$
      iv. Encryption of message M: $Enc_{ok}(M) \coloneqq M^e \; (mod \; N)$
      v. Decryption of ciphertext c: $Dec_{sk}(c) \coloneqq c^d \; (mod \; N)$

      Which properties of the hash function are guaranteed?

   c. Assume now that we use a generic PK Encryption scheme, which ensures that, given a ciphertext c, no attacker can output the plaintext M. Which properties of the hash function are guaranteed?
2. Symmetric vs. public keys: Say that Amelie, Baptiste, Christine and Dennis want to securely communicate with each other.
   a) Say that the four users want to use symmetric encryption (like a block cipher) to communicate pairwise (each user wants to communicate to each of the others, confidentially from everyone else). How many keys do they need to generate in order to achieve this?
   b) What if the encryption is public-key? How many keys need to be generated so that every user can communicate with everyone else?
   c) More generically, how many symmetric keys need to be generated to ensure that N users are all able to communicate with one another? How about PKE key-pairs?
3. Block Ciphers: Suppose Amelie and Baptiste share a secret key sk used for a block cipher. Assume this block cipher is chained as follows: $C_i = M_{i-1} \; \mathrm{XOR} \; Enc_{sk}(M_i \; \mathrm{XOR} \; C_{i-1})$, where Enc denotes the symmetric encryption step and XOR denotes the bitwise exclusive OR operation. The message is $M_1 \dots M_N$ and the received ciphertext is $C_1 \dots C_N$, while C_0, M_0 denote publicly known starting vectors.
   a) If Amelie uses this block cipher to encrypt some message $M_1 \dots M_N$ to Baptiste, how does he decrypt it?
   b) If the 5th ciphertext block, C_5 is corrupted in transmission, which other blocks are affected?
   c) Suggest one way to let Baptiste know whether corruption of the ciphertexts took place (in other word, we want the integrity of the ciphertext).

4. Mark, for each of the following statements, whether they are true or false and explain your reasoning shortly.
   a) If a hash function has inputs of size l_{input} and outputs strings of length l_{output}, if $l_{input} > l_{output}$, then there will always be collisions.
   b) Hash functions can ensure secure (confidential) transmission of a message from one party (Amelie) to another (Baptiste).
   c) In a sanitizable signature scheme, the signer should always have the sanitizer's key.
   d) Key indistinguishability is a necessary ingredient of receiver-anonymous public-key encryption.
   e) Signature schemes ensure non-repudiation.
   f) A collision-resistant hash function always has pseudo-random outputs.
5. (Long question) Say that Amélie, Baptiste, Christine, and Dennis are all friends. They want to go to a restaurant one evening, but they don't know to which restaurant they want to go. They all have public-key encryption public and secret keys, and each pair of friends share a symmetric key used for a MAC scheme. They are also communicating via a broadcast network (all the messages can be seen by everyone else). For each of the following situations, design a method to ensure they correctly agree on the restaurant.

   Example: Amélie is the expert on restaurants. The restaurants she proposes will be chosen. However, each of the others wants to propose their own favourite restaurant. Ensure that the correct decision is taken.

   Solution: Amélie chooses her restaurant, which we denote $rest_A$. She broadcasts the following message: $rest_A \big| MAC_{sk_{AB}}(rest_A) \big| MAC_{sk_{AC}}(rest_A) | MAC_{sk_{AD}}(rest_A)$. In this expression, sk_{AB} refers to the symmetric MAC key shared between Amélie and Baptiste, sk_{AC} is the key Amelie shares with Christine, etc.

   a) Amélie's connection to the broadcast channel is broken and she can only communicate to Baptiste (without the others seeing the message). Show how Amelie can communicate her choice to Baptiste and how Baptiste can forward her choice so that Christine and Dennis are convinced that it was Amélie's suggestion and not something Baptiste came up with.
   b) Amélie and Christine are organizing a surprise birthday party for Baptiste and they want the restaurant to be a surprise. However, they disagree about the restaurant: Amelie wants to go to a crêperie, Christine prefers a bistro. They have agreed that Dennis should cast the decisive vote.
   c) Since it is Baptiste's birthday, the other three friends have agreed to let him decide where to go. There is a choice, between a crêperie and a bistro. The three friends know that Baptiste will just take a majority decision – the place with the most votes wins. How can you prevent double voting? (the same person votes twice) How can you ensure that the vote is fair (that none of the participants can in fact take advantage of knowing the other votes beforehand)?

   At this point, assume that the four friends have secret keys to a group signature scheme, with an impartial, and honest fifth user, Emma, being the group manager and opener.

d) The four participants will all vote anonymously on the proposal between a crêperie and a bistro. However, if there is a tie, Baptiste's choice will be the decisive one. Additionally, if any of the participants double-voted, none of their votes is taken into account.
e) In this scenario, we consider three possible restaurants: a crêperie (Amélie's choice), a bistro (Christine's choice), and an Indian restaurant (Dennis' choice), who all have signing keys for a sanitizable signature scheme, for which they can delegate sanitizer keys to users of their choice. First, Amélie, Christine, and Dennis must obtain offers from the restaurants which are within a given budget. The offers must contain prices and must be sent by the restaurant. Whoever is caught with a false menu automatically drops off. Then Baptiste will make the choice of restaurant this time, based on contents of the menus (if these are genuine), but without seeing the prices.

6. Explain in your own words why robustness is a necessary property of receiver-anonymous encryption.
7. Define commitment schemes. By using an example explain their properties.