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 in question 1a. 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 Amélie 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 Amélie 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)?

6. Describe the attack on EC-DSA if signers use the same k to sign messages (instead of an ephemeral value).

7. Explain in your own words the technique of "game hopping" in provable security. Think of mentioning what a game is, why one does game hopping, and what are the considerations at every game hop

8. Consider a pseudo-random generator PRG, which takes as input a seed $seed$ of 128 bits and which outputs random integers of length 128 bits. We call PRG a secure pseudo-random generator if any adversary A against PRG has at most probability $\frac{1}{2} + \varepsilon$ (for a negligible ε) to succeed in the following experiment:

   GAME $\mathbb{G}_b$(PRG)

   $seed \leftarrow_R \{0,1\}^{128}$
   $d \leftarrow A^{Gen_b(\cdot)}$ with $Gen_b(\cdot) = PRG(seed)$ if $b = 0$ and $Gen_b(\cdot) \leftarrow_R \{0,1\}^{128}$ if $b = 1$

   A wins if and only if $b = d$

   a. Explain what this game means, in your own words.
   b. What is the difference between the game above and the following definition: a PRG is a secure' pseudo-random generator if for any seed $seed \in \{0,1\}^{128}$ it holds that any adversary A against PRG has at most probability $\frac{1}{2} + \varepsilon$ (for a negligible ε) to succeed in the following experiment:

      GAME $\mathbb{G}'_b$(PRG)

      $d \leftarrow A^{Gen_b(\cdot)}$ with $Gen_b(\cdot) = PRG(seed)$ if $b = 0$ and $Gen_b(\cdot) \leftarrow_R \{0,1\}^{128}$ if $b = 1$

      A wins if and only if $b = d$

   c. Assume PRG is a secure pseudorandom generator (with regard to notion a.). Construct a pseudorandom generator PRG' which, for every seed apart from $seed = 0^{128}$ (the all-zero string), outputs PRG(*seed*). For the all-zero seed, PRG(*seed*) always outputs 0^{128}. Is PRG' secure in the sense of a. ? Is it secure in the sense of b.?

d. Which notion (security in terms of point a. or security in terms of point b.) offers better security?

9. Explain the notion of relay attacks in authentication, mentioning why they can bypass cryptographic countermeasures, such as encryption and digital signatures.

10. Explain the following notions: mafia fraud, distance fraud, terrorist fraud

11. Consider the following distance-bounding protocol:

Prover
(K)

Verifier
(K)

$N_P \leftarrow_R \{0,1\}^{128}$ $\qquad\qquad$ $N_V \leftarrow_R \{0,1\}^{128}$

$$\xrightarrow{N_p}$$

$$\xleftarrow{N_V}$$

Compute
$R \leftarrow \mathrm{SEnc}_K(N_P|N_V)$
s.t.
$|R| = n$

Compute
$R_0|R_1 \leftarrow \mathrm{SEnc}_K(N_P|N_V)$

For I = 1 to n, do:

Choose $c \in \{0,1\}$
Start clock

$$\xleftarrow{c}$$

$$\xrightarrow{c\,XOR\ \ R_i}$$

Stop clock
Store time and response

Verify that all responses are
correct and that times are
below t_{max}.

If all OK, then accept
Else reject

In this protocol, assume that for all keys K the symmetric encryption function gives pseudo-random responses.

a. Is this protocol distance-fraud resistant?

b. Is it mafia-fraud resistant?

12. You have chosen the following elliptic curve over the field $F_{13} = \{0,1,2\ldots,12\}$:

$$y^2 = x^3 + x + 1$$

a. Fill out the following tables:

x	x^3	$x^3 + x + 1$

0		
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		

y	y^2
0	
1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	

b. What is the relationship between the first half of the table (the orange rows) and the lower half of the table (the green rows)?

c. Take the point $P = (1,4)$. Is this point on the elliptic curve? By using the formula for point doubling, calculate the coordinates of $2P, 4P, \dots kP$ such that $(k+2)P = \infty$

d. By using point addition, calculate the coordinates of the remaining points: $3P, 5P, \dots (k+1)P$

e. Consider Diffie-Hellman key exchange on elliptic curves, with this elliptic curve. Alice and Bob agree to use the point $Q = 2P$ as a group generator. Alice chooses the integer 5 at random, and sets her public key to $PK_A = 5Q$. Bob chooses the integer 8 at random, and sets his public key to $PK_B = 8Q$. What is the key they agree on?