Homework 4

- Questions from Lecture unit 4
- Please refer to the lecture slides for more information about the context in which the questions arise.
- Due date: Wednesday, October 9, 2019

1. The idea in the chosen-ciphertext attack on RSA encryption can be applied to show that if one can decrypt 1% of RSA encryption then one can break 100% of RSA encryption. Describe how it works. Explicitly, assuming there is an algorithm A that can decrypt 1% of input instances, show that using A as a black box one can decrypt all instances.

2. Bob and Alice want to determine a bit value (toss a coin) with the following procedure:

   - Alice chooses a bit $a \in \{0, 1\}$
   - Bob chooses a bit $b \in \{0, 1\}$
   - The outcome of the coin toss is $a \oplus b$

   How do we implement the above procedure so that instead of directly sending a to Bob, Alice can send her commitment without revealing the value? Describe the protocol with which the procedure can be carried out using a bit commitment scheme.

3. The challenge-response identification scheme whereby the verifier sends a random challenge ciphertext for the prover to decrypt is not a good idea. Explain how it can be used by the verifier to mount a chosen-ciphertext attack. More precisely the verifier can get the decryption of a specific ciphertext by sending a random challenge ciphertext for the prover to decrypt.

4. The notion of *zero-knowledge* in zero-knowledge interactive proof as discussed above is *computational* or *informational* zero knowledge. Explain why?