Information Systems and Network Security

Prof. Stefano Leucci

Question 1: CCA security & Malleability

- Explain what it means for a encryption scheme to be malleable **(2 points)** and provide an example of a malleable encryption scheme **(2 points)**.
- Describe the chosen ciphertext threat model **(2 points)** and provide a formal definition of CCA-secure private-key encryption scheme via a security experiment **(4 points)**.
- Describe how malleability relates to CCA-security **(2 points)**.

Question 2: Hash functions

- Define the concepts of *hash function* and *compression functions* **(2 points)** and provide a definition of collision resistance **(2 points)**.
- Model a hash function as a random function $H : \{0,1\}^* \to \{0,1\}^\ell$ (for sufficiently large values of ℓ). A trivial algorithm to find a collision performs $2^\ell + 1$ evaluations of H. Prove that it is possible to find a collision with at least some constant positive probability by evaluating H only $2^{\ell/2}$ times. **(6 points)**

  Hint: study the probability of the complementary event and use the inequality $1 - x \leq e^{-x}$.

Question 3: Diffie-Hellman Key Exchange

- Alice and Bob use the Diffie-Hellman Key Exchange protocol to agree on a secret shared key k. For the sake of this exercise, they use the (insecure!) group $\mathbb{Z}_{11}^*$ and the generator 6. The first message sent from Alice to Bob is 3 and the shared key is $k = 5$. What is the message sent from Bob to Alice? **(4 points)**
- Argue that if Alice and Bob use a group $\mathcal{G}$ for which the discrete logarithm can be computed efficiently, then an eavesdropper can (efficiently) recover the key. **(4 points)**
- The shared key agreed on using the Diffie-Hellman Key Exchange is a random group element in $\mathcal{G}$. However, many encryption schemes require the key to be a (sufficiently) random binary string. Explain how this problem can be circumvented. **(2 points)**