1)

12 statements that are either **true** or **false**. No justification is required. Correct answers count +1 points, incorrect answers -1 points. Overall, you cannot receive negative points for this exercise.

- [ ] An unbounded adversary can break perfect secrecy
- [ ] $f(n) := 1^{-\frac{1}{n}}$ is negligible *(I'm not 100% sure about the function, but I think it was this one)*
- [ ] DES uses longer keys than AES
- [ ] The three modes of operation (ECB, CBC, CTR) are CPA-secure
- [ ] The CBC and CTR modes of operation are CCA-secure
- [ ] Deterministic MAC schemes cannot be secure (in the standard sense of *existential unforgeability under adaptive chosen-message attacks*)
- [ ] Using MACs of the sent message, one can prevent replay attacks
- [ ] A hash function takes a string of arbitrary length and outputs a string of fixed length
- [ ] $(\mathbb{Z}, \cdot)$ is a group
- [ ] $x \to [x^e \bmod N]$ is a permutation over $\mathbb{Z}_N^*$
- [ ] The discrete logarithm problem is hard for $(\mathbb{Z}_p, +)$ with p being prime
- [ ] For private-key encryption, NIST recommends longer keys than for public-key encryption to reach a similar level of security

2)

a)

They wrote down the definition of CCA-security (the game with the challenger and adversary)

What modifications to the definition are necessary if you want to prove CPA-security?

b)

Give a definition for the one-time pad (define the functions $\mathtt{Gen}$, $\mathtt{Enc}$ and $\mathtt{Dec}$)

c)

Is the one-time pad CCA-secure? Justify your answer.

d)

Name one advantage and one disadvantage of private-key encryption compared to public-key encryption.

3)

Let $H : \{0,1\}^* \to \{0,1\}^n$ be a hash function and $f_k : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a PRF.

Let Π be a MAC scheme that is defined like this:

- $\texttt{Gen}(1^n)$: Return random $k \leftarrow \{0,1\}^n$
- $\texttt{Mac}_k(m)$: Return $t := f_k(H(m))$
- $\texttt{Vrfy}_k(m,t)$: Return 1 if $f_k(H(m)) = t$, return 0 otherwise

Show that if H is **not** collision-resistant, then Π is not secure (in the standard sense of *existential unforgeability under adaptive chosen-message attacks*)

4)

a)

Compute $[2^{63} \bmod 11]$

b)

You are given two RSA public keys, (N_1, e_1) and (N_2, e_2), where N_1 and N_2 share one of their prime factors. Show how you can efficiently obtain the secret keys from the public keys.

5)

a)

El-Gamal encryption is defined like this:

$\texttt{Gen}(1^n)$:

- Sample a group $(\mathbb{G}, q, g) \leftarrow \mathcal{G}(1^n)$ *(Maybe the group was fixed as well, I'm not sure anymore)*
- Sample a group element $x \leftarrow \mathbb{Z}_q$
- Return the secret key $sk := x$ and the public key $pk := g^x$

$\texttt{Enc}_{pk}(m)$:

- Sample a group element $y \leftarrow \mathbb{Z}_q$
- Compute $c_1 := g^y$ and $c_2 := pk^y \cdot m$
- Return $c := (c_1, c_2)$

Define $\texttt{Dec}_{sk}(c)$ and prove the correctness of the scheme.

b)

Let Π be the El-Gamal encryption scheme as defined in **a)** and Π' ($\texttt{Gen}'(1^n)$, $\texttt{Enc}'_k(m)$, $\texttt{Dec}'_k(c)$) be a CCA-secure private-key encryption scheme. Show that the following scheme is **not** CCA-secure:

$\texttt{Gen}''(1^n)$:

- Same as $\texttt{Gen}(1^n)$ from **a)**

$\texttt{Enc}''_{pk}(m)$:

- Sample a random key $k \leftarrow \{0,1\}^n$
- Compute $c_1 := \texttt{Enc}_{pk}(k)$ and $c_2 := \texttt{Enc}'_k(m)$
- Return $c := (c_1, c_2)$

$\texttt{Dec}''_{sk}(c)$:

- $c := (c_1, c_2)$
- Compute $k := \texttt{Dec}_{sk}(c_1)$
- Return $m := Dec'_k(c_2)$