Exercises II

Note: We discuss solutions to the exercises together in the class on the **25th November 2024**.

Exercise 1. *Euler function*

Recall Euler's totient function $\varphi\colon \mathbb{N} \to \mathbb{N}$, where $\varphi(N) = \mathsf{ord}(\{x \in \{1,\dots,N\} \mid \gcd(x,N) = 1\})$.

1. Let p be a prime, show that $\varphi(p) = p - 1$.

2. Let p and q be distinct primes and $N = pq$, show that $\varphi(N) = (p-1)(q-1)$.
   Hint: Start from the other way: which elements are divisible by p or q?

Exercise 2. *RSA to Factoring*

1. Show (formally) that the problem RSA reduces to the factoring problem, both introduced in the second lecture. In other words, show that if there exists an algorithm $\mathcal{A}$ which solves the factoring problem with non-negligible probability, one can construct an algorithm $\mathcal{B}$ which solves the RSA problem with non-negligible probability.
   Hint: Think about what information you need to solve RSA. The extended Euclidean algorithm applied to e and $\varphi(N)$ might be of use.

Exercise 3. *IND-CCA Security*

We consider the ElGamal encryption in a cyclic group $\mathcal{G}$ where the DDH problem is hard.

1. Show that the ElGamal encryption scheme is homomorphic with respect to multiplication: given c, c', the ciphertexts of two messages m and m', it is possible to compute a valid ciphertext of $m \cdot m'$ without knowing m and m'.

We define a new security experiment:

Definition 1 (Chosen Ciphertext Attack Security)**.** *We define the following experiment:*

$\mathcal{C}$		$\mathcal{A}$
$(pk, sk) \leftarrow KeyGen(1^\lambda)$		
	$\xrightarrow{pk}$	
	$\xleftarrow{c_i}$	
$m_i = Dec(sk, c_i)$	$\xrightarrow{m_i}$	
		Chooses m_0, m_1 $(\neq m_i)$
	$\xleftarrow{m_0, m_1}$	
$b \leftarrow \{0,1\}$		
$c \leftarrow Enc(pk, m_b)$		
	$\xrightarrow{c}$	
	$\xleftarrow{c'_i}$	*for* $c'_i \neq c$
$m'_i = Dec(sk, c'_i)$	$\xrightarrow{m'_i}$	
		Computes a bit b'*, output it*

A public-key encryption scheme $\Pi = (KeyGen, Enc, Dec)$ *is called* $IND-CCA$ *secure, if for all PPT adversaries* $\mathcal{A}$ *and for all security levels* $\lambda \in \mathbb{N}$*, it holds that*

$$\Pr[b' = b] \leq \frac{1}{2} + negl(1^\lambda).$$

2. Show that the ElGamal encryption scheme is not IND-CCA. This implies that IND-CPA security is strictly weaker than IND-CCA security.