# Cryptography

## Lecture 13 III 2013

**Definition The CPA indistinguishability experiment** $\mathsf{PrivK}^{\mathsf{cpa}}_{\mathcal{A},\Pi}(n)$:

1. A key $k$ is generated by running $\mathsf{Gen}(1^n)$.
2. The adversary $\mathcal{A}$ is given input $1^n$ and oracle access to $\mathsf{Enc}_k(\cdot)$, and outputs a pair of messages $m_0, m_1$ of the same length.
3. A random bit $b \leftarrow \{0,1\}$ is chosen, and then a ciphertext $c \leftarrow \mathsf{Enc}_k(m_b)$ is computed and given to $\mathcal{A}$. We call $c$ the challenge ciphertext.
4. The adversary $\mathcal{A}$ continues to have oracle access to $\mathsf{Enc}_k(\cdot)$, and outputs a bit $b'$.
5. The output of the experiment is defined to be $1$ if $b' = b$, and $0$ otherwise. (In case $\mathsf{PrivK}^{\mathsf{cpa}}_{\mathcal{A},\Pi}(n) = 1$, we say that $\mathcal{A}$ succeeded.)

**Definition** (**CPA-security**) A private-key encryption scheme $\Pi = \langle \mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec} \rangle$ has indistinguishable encryptions under a chosen-plaintext attack (or is CPA-secure) if for all probabilistic polynomial-time adversaries $\mathcal{A}$ there exists a negliglibible function negl such that

$$P\left[\mathsf{PrivK}^{\mathsf{cpa}}_{\mathcal{A},\Pi}(n) = 1\right] \leq \frac{1}{2} + \mathsf{negl}(n),$$

whee ther probability is taken over the random coins used by $\mathcal{A}$ , as well as the random coins used in the experiment.

**Definition** (**CCA-secure**) For CCA experiment is defined as CPA experiment but:

- in the second and in the fourth step an adversary has also access to the decryption oracle: $\mathsf{Dec}_k(\cdot)$.
- but in the fourth step, an adversary is not allowed to ask for the decryption of $c$.