Cryptography – Questionnaire 3

Name: _____

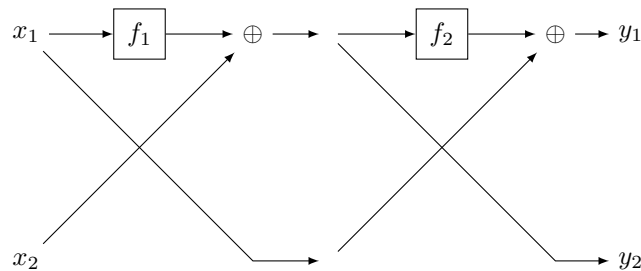**Matr.:** _____

"One-liners"

Exercise 3.1   Feistel-Networks   **1P+1P+1P = 3P**

Consider the two-round Feistel-Network drawn below, with $f_1, f_2 : \{0,1\}^n \to \{0,1\}^n$.

(a) Compute the outputs y_1, y_2 of the network for $x_1 = 0^n$ and $x_2 = 0^n$
    Answer:_____

(b) Compute the outputs y_1, y_2 of the network for $x_1 = 0^n$ and $x_2 = f_1(0^n)$
    Answer:_____

(c) Does the two-round Feistel-Network realize a PRP if used with two PRFs f_{k_1}, f_{k_2}? Why/why not?
    Answer:_____

Exercise 3.2   PRG from PRF   **2P**

Let F be a PRF with $l_{\text{in}}(n) = l_{\text{out}}(n) = n$. Construct from F a PRG G of stretch $2n$.

Answer: $G(k) :=$ _____

Questions– 1P each = 5P

	true	false
Let F be a PRP, F-rCBC is computationally secret.	☐	☐
Let G be a PRG of stretch $s \cdot n$, then $F_k : \{0,1\}^{sn} \to \{0,1\}^{sn}$ defined by $F_k(x) = G(k) \oplus x$ is a PRF.	☐	☐
Let F be a PRF of block length $l(n) = n$. We define $\widetilde{F}$ for every $n \in \mathbb{N}$, $k \in \{0,1\}^n$ and $x_1 \ldots x_{2n} \in \{0,1\}^{2n}$ by using F in a one-round Feistel-network: $$\widetilde{F}_k(x_1 \ldots x_{2n}) = \mathsf{FN}_{F_k}(x_1 \ldots x_n, x_{n+1} \ldots x_{2n}).$$ $\widetilde{F}$ is a PRP of block length $2n$.	☐	☐
Let RO be a random function oracle of input and output length n. Then $G(k) := \mathsf{RO}(k)\|\mathsf{RO}(k)$ is a PRG of stretch $2n$.	☐	☐
Let F be a PRF. Then F-rCTR is CCA-secure.	☐	☐