Die Lösungen zu den Aufgaben **4.1 und 4.2** werden als Teil der Prüfungsnote **bewertet**! Bitte mit Angabe von Name, Matrikelnummer, Studiengang und Fachsemester bei der Übung am 4. Juni abgeben (oder vorher per E-Mail an `bmoeller@crypto.rub.de`).

Aufgabe 4.1

Nachfolgend sind einige Familien von Abbildungen beschrieben. Welche dieser Familien sind PRP-sicher, welche nicht?

Bei Sicherheit ist hier kein Beweis verlangt.

Geben Sie bei Unsicherheit einen erfolgreichen PRP-Angreifer an (nicht unbedingt den bestmöglichen!). Auf die Laufzeit des Angriffs kommt es hier nicht an; von PRP-Sicherheit gehen wir hier nur aus, wenn kein PRP-Angreifer einen Vorteil größer 0 erreicht.

a. $k = 1, \ell = 1$

	$E_K(0)$	$E_K(1)$
$K = 0$	0	1
$K = 1$	1	0

b. $k = 2, \ell = 1$

	$E_K(0)$	$E_K(1)$
$K = 00$	1	0
$K = 01$	0	0
$K = 10$	0	1
$K = 11$	1	1

c. $k = 2, \ell = 1$

	$E_K(0)$	$E_K(1)$
$K = 00$	0	1
$K = 01$	0	1
$K = 10$	1	0
$K = 11$	0	1

d. $k = 2, \ell = 2$

	$E_K(00)$	$E_K(01)$	$E_K(10)$	$E_K(11)$
$K = 00$	00	01	10	11
$K = 01$	01	10	11	00
$K = 10$	10	11	00	01
$K = 11$	11	00	01	10

Aufgabe 4.2

Soweit Sie in Aufgabe 4.1 PRP-Unsicherheit festgestellt und dazu Angreifer beschrieben haben, geben Sie jeweils den PRP-Vorteil an!