Aufgabe 3.1

Nachfolgend sind einige „Familien“ von Abbildungen beschrieben, nämlich jeweils zu jedem $K \in \mathcal{K} = \{0,1\}^k$ eine Abbildung $E_K : \{0,1\}^\ell \to \{0,1\}^\ell$. Welche dieser Familien sind PRF-sicher, welche nicht?

Bei Sicherheit ist hier kein Beweis verlangt.

Geben Sie bei Unsicherheit einen erfolgreichen PRF-Angreifer an! Das muss nicht der bestmögliche Angreifer sein.

Hinweise: PRF-Unsicherheit bedeutet, es gibt einen erfolgreichen PRF-Angreifer – also einen Angreifer mit einem PRF-Vorteil, der nicht verschwindend gering ist. Der Vorteil kann aber näher an der 0 liegen als an der 1. Auf die Laufzeit des Angriffs kommt es hier nicht an.

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

	$E_K(0)$	$E_K(1)$
$K = 00$	1	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 3.2

Soweit Sie in Aufgabe 3.1 PRF-Unsicherheit festgestellt und dazu Angreifer beschrieben haben, geben Sie jeweils den PRF-Vorteil an!