Задание 4,

Фамилия _____

1. Пусть F – PRF на $(\{0,1\}^n, \{0,1\}^n, Y)$. Выберите верные утверждения, доказав или опровергнув их.

№	Задание	Ответ	
a	$F: \forall k, x, c \in \{0,1]^n\ F(k, x \oplus c) = F(k, x) \oplus c;$ F – может быть стойкой		
b	$F: \forall k, x, c \in \{0,1]^n\ F(k \oplus c, x) = F(k, x) \oplus c;$ F – **не** может быть стойкой		
	Не заполнять!	/ 2	/ 2

2. Выберите верные утверждения:

№	Задание	Ответ
a	Любой стойкий блочных шифр семантически стойкий для любых сообщений имеющих размер, кратный длине блока	
b	Если блочный шифр имеет ключ длины 128 бит, его параметр стойкости не может превосходить 128 бит	
c	Если блочный шифр имеет ключ длины 128 бит, его параметр стойкости не может быть ниже 64 бит	
d	Возможно существование стойкого блочного шифра, не стойкого к восстановлению ключа	
e	Стойкость блочного шифра можно свести к стойкости его функции зашифрования, как псевдослучайной подстановки	
f	Блочной шифр в режиме ECB является шифром подстановки	
g	Если стойкий блочный шифр имеет ключ длины 128 бит и размер блока 128 бит то он является абсолютно стойким.	
h	Невозможно построить абсолютно стойкий шифр на основе блочного шифра с длинной ключа 128 бит, размером блока 64 бита для сообщений длины 128 бит.	
	Не заполнять!	/ 8

3. Пусть $F: K \times X \to Y$ – стойкая PRF, $Y = \{0,1\}^n$. Для некоторого параметра $l < n$ рассмотрим $F': K \times X \to Y', Y' = \{0,1\}^l: F'(k, x) = F(k, x)[0, .., l-1]$. Является ли F' - стойкой PRF? Докажите

	Ответ
Не заполнять!	/2

4. Рассмотрим игру на семантическую стойкость для случайных сообщений: вместо выбора произвольных сообщений противник может выбрать сообщения только случайно из множества сообщений. В остальном игра идентично обычной игре на семантическую стойкость. Являются ли игры эквивалентными? (записать в ответ). Если нет – выясните какая из них является более строгой, докажите это сведением, продемонстрируйте пример шифра, стойкого в одной из моделей семантической стойкости, и не стойкого в другой. Если игры эквивалентны – формально докажите это.

	Ответ
Не заполнять!	/4

5. Пусть $F: K \times X \to Y$ – стойкая PRF, $K = X = Y = \{0,1\}^n$. Какие из следующих алгоритмов является стойкими PRF? Для каждого алгоритма предоставить доказательство стойкости или атаку.

№	Задание	Ответ
a	$F'(k,x) = F(k,x)\|\|0$	
b	$F'(k,x) = F(k,x) \oplus 1^n$	
c	$F'\big(k,(x,y)\big) = F(k,x) \oplus F(k,y)$	
d	$F'(k,x) = F(k,x) \oplus x.$	
e	$F'((k_1,k_2),x) = F(k_1,x) \oplus F(k_2,x)$	
f	$F'(k,x) = F(k,x)\|\|F(k,x \oplus 1^n)$	
g	$F'(k,x) = F(F(k,0^n),x).$	
h	$F'(k,x) = F(F(k,0^n),x)\|\|F(k,x)$	
i	$F'(k,x) = F(k,x)\|\|F(k,F(k,x))$	
	Не заполнять!	/9

6. Рассмотрим модифицированную игру на стойкость PRF. Назовём игру, описанную в лекции – адаптивной, в том смысле, что противник отправляет сообщения последовательно, после получения ответа на свое предыдущее сообщения от претендента. Т.е. при формировании сообщения x_i противник может учитывать полученные от претендента результаты $y_1, \dots, y_{i-1}$. Рассмотрим неадаптивную версию игры – противник отправляет сообщения $x_1, \dots, x_q$ **одновременно**, и получает результаты $y_1, \dots, y_q$, где здесь и далее $y_i = f(x_i)$. Преимущество противника в неадаптивной игре описывается аналогично адаптивной версии.
   Пусть F стойкая PRF на (K, X, X), $|X|$ - супер полиномиальная. Построим F' следующим образом: для некоторого элемента $x' \in X, y' = F(k,x')$ определим $F'(k,y') = x'$, для остальных $x \in X: x \neq y' \quad F'(k,x) = F(k,x)$.
   Формально докажите или опровергните утверждения ниже.

   Для заданий c и d определите аналогичную задачу для блочных шифров E и E'.

№	Задание	Ответ	
a	F' – не стойкая PRF против адаптивных противников		
b	F' –стойкая PRF против неадаптивных противников		
c	E' – не стойкий блочный шифр против адаптивных противников		
d	E' – стойкий блочный шифр против неадаптивных противников		
	Не заполнять!	/4	/4