Задание 4,

Фамилия \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Пусть – PRF на . Выберите верные утверждения, доказав или опровергнув их.

|  |  |  |  |
| --- | --- | --- | --- |
| № | Задание | Ответ | |
| a | *; –* может быть стойкой |  | |
| b | *; –* **не** может быть стойкой |  | |
|  | **Не заполнять!** | / 2 | / 2 |

1. 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 с длинной ключа 128 бит на основе блочного шифра с длинной ключа 128 бит, размером блока 64 бита для сообщений длины 256 бит. |  |
|  | **Не заполнять!** | / 8 |

1. Пусть – стойкая PRF, . Для некоторого параметра рассмотрим . Является ли - стойкой PRF? Докажите

|  |  |
| --- | --- |
|  | Ответ |
|  |  |
| **Не заполнять!** | /2 |

1. 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 |

1. Пусть – стойкая PRF, . Какие из следующих алгоритмов является стойкими PRF? Для каждого алгоритма предоставить доказательство стойкости или атаку.

|  |  |  |
| --- | --- | --- |
| № | Задание | Ответ |
| a |  |  |
| b |  |  |
| c |  |  |
| d | . |  |
| e |  |  |
| f |  |  |
| g | *.* |  |
| h |  |  |
| i |  |  |
|  | **Не заполнять!** | /9 |

1. 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 противник может учитывать полученные от претендента результаты . Рассмотрим неадаптивную версию игры – противник отправляет сообщения **одновременно**, и получает результаты , где здесь и далее . Преимущество противника в неадаптивной игре описывается аналогично адаптивной версии.

Пусть стойкая PRF на - сверх-полиномиальная. Построим следующим образом: для некоторого элемента определим , для остальных . Предполагается, что противник знает , но не знает , так как зависит от использованного ключа.

Формально докажите или опровергните утверждения ниже.

Для заданий с и d определите аналогичную задачу для блочных шифров  и .

|  |  |  |  |
| --- | --- | --- | --- |
| № | Задание | Ответ | |
| a | – не стойкая PRF против адаптивных противников |  |  |
| b | *’* – стойкая PRF против неадаптивных противников |  |  |
| с | – не стойкий блочный шифр против адаптивных противников |  |  |
| d | *’* – стойкий блочный шифр против неадаптивных противников |  |  |
|  | **Не заполнять!** | /4 | /4 |