Задание 2.

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

1. Среди указанных ниже величин найдите пренебрежимо малые (negl), сверх-полиномиальные (sup) и полиномиально-ограниченные (poly-b) (в теоретическом смысле):

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № | Задание | Ответ | | |
|  |  | negl | sup | poly-b |
| a |  |  |  |  |
| b |  |  |  |  |
| c |  |  |  |  |
| d |  |  |  |  |
| e |  |  |  |  |
| f |  |  |  |  |
| g |  |  |  |  |
| h |  |  |  |  |
| i |  |  |  |  |
|  | **Не заполнять!** | / 2 | / 2 | / 2 |

1. Пусть – эффективный алгоритм, позволяющий пересказывать следующий бит по битам для некоторого генератора . Т.е. величина не пренебрежимо малая. Определим игру на предсказание предыдущего бита: имя биты ] предсказать бит . (определяется аналогично игре на определение следующего бита). Постройте эффективный алгоритм , позволяющий выиграть игру на предсказание прошлого бита, используя алгоритм . Найдите – преимущество алгоритма в игре на предсказание прошлого бита (определяется аналогично ).

|  |  |  |  |
| --- | --- | --- | --- |
| № | Задание | Ответ | |
| a |  |  | |
|  | **Не заполнять!** | / 2 | / 2 |

1. Выберите верные утверждения:

|  |  |  |
| --- | --- | --- |
| № | Задание | Ответ |
| a | Если алгоритм противника в некоторой игре против эффективный, то величина – пренебрежимо малая |  |
| b | Любая пренебрежимо малая – полиномиально ограниченная |  |
| c | Любая полиномиально ограниченная – пренебрежимо малая |  |
| d | Аддитивный одноразовый блокнот переменной длины – семантически стойкий шифр |  |
| e | Пусть алгоритм от параметра . На вход алгоритма подали вход длинной , он детерминированно выполнился за время , не являющимся полиномиально ограниченным от . – точно не эффективный. |  |
| f | Пусть алгоритм от параметра . На вход алгоритма подали вход длинной , он детерминированно выполнился за время , – эффективный. |  |
| g | Любой эффективный алгоритм – полиномиально ограничен памятью |  |
| h | Если и на стойкие PRG, то для (последовательности статистически неразличимы). |  |
|  | **Не заполнять!** | / 8 |

1. Пусть – стойкий PRG. Пусть , где - побитовый AND. Рассмотрим следующий статистический тест на : , где   
    - получает последний бит вектора .

Каково преимущество алгоритма ? ( - ?)

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

1. Пусть – абсолютно стойкий шифр на

Является ли абсолютно стойким шифром? Если нет продемонстрируйте атаку.

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

1. Пусть – стойкий PRG. Какие из следующих алгоритмов является стойкими PRG? Для каждого алгоритма предоставить доказательство стойкости или атаку.

|  |  |  |
| --- | --- | --- |
| № | Задание | Ответ |
| a |  |  |
| b |  |  |
| c |  |  |
| d |  |  |
| e |  |  |
| f | *-* побитовый OR |  |
| g |  |  |
| h |  |  |
| i |  |  |
|  | **Не заполнять!** | /18 |

1. –шифр на . Пусть имеется возможность случайно выбирать шифртекст равновероятно из . Рассмотрим игру: Противник посылает сообщение претенденту. Претендент вычисляет  и отправляет противнику, который затем вычисляет бит , являющегося результатом игры. Определим . Определим – стойкий шифр с псевдослучайными шифртекстами (pseudo-random ciphertext secure), если для любых противников величина – пренебрежимо малая.

Формально докажите или опровергните утверждения ниже.

|  |  |  |  |
| --- | --- | --- | --- |
| № | Задание | Ответ | |
| a | Если – стойкий шифр с псевдослучайными шифртекстами, то он всегда семантически стойкий |  |  |
| b | Одноразовый блокнот - стойкий шифр с псевдослучайными шифртекстами |  |  |
| с | Невозможно построить шифр, который будет семантически стойким, но не стойким с псевдослучайными шифртекстами. |  |  |
|  | **Не заполнять!** | /3 | /3 |

1. Пусть стойкий PRG на . Показать, что - сверх-полиномиальна. Для этого показать наличие противника с преимуществом не менее против с временем атаки линейным от .

|  |  |
| --- | --- |
|  | Ответ |
|  |  |
| **Не заполнять!** | /4 |