Задание 1.

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

1. Вычислить энтропию () следующих величин:

|  |  |  |
| --- | --- | --- |
| № | Задание | Ответ |
| a | , равномерное распределение |  |
| b |  |  |
| c |  |  |
| d |  |  |
| e |  |  |
| f |  |  |
| g |  |  |
| h |  |  |
|  | **Не заполнять!** | / 8 |

1. Рассмотрим игру с двумя экспериментами.
   1. В эксперименте 0 претендент подбрасывает монетку и возвращает **РЕШКА**, если выпал орёл, и **ОРЁЛ** если орёл.
   2. В эксперименте 1 претендент всегда возвращает **ОРЁЛ**.

Цель противника различить два эксперимента. Пусть событие того, что в эксперименте противник возвращает 1. Преимущество противника .

Вычислить для следующих алгоритмов:

|  |  |  |
| --- | --- | --- |
| № | Задание | Ответ |
| a |  |  |
| b |  |  |
| c |  |  |
| d |  |  |
| e |  |  |
| f | , построить |  |
|  | **Не заполнять!** | / 6 |

1. Выберите верные утверждения:

|  |  |  |
| --- | --- | --- |
| № | Задание | Ответ |
| a | Абсолютно стойкий шифр всегда семантически стойкий |  |
| b | Любой шифр Шеннона является абсолютно стойким |  |
| c | Аддитивный одноразовый блокнот – семантически стойкий шифр |  |
| d | Аддитивный одноразовый блокнот переменной длины – семантически стойкий шифр |  |
| e | Если шифр имеет длины ключей больше длин шифртекстов то он абсолютно стойкий |  |
| f | Если шифр имеет и энтропии длины ключей больше длин и энтропий шифртекстов то он абсолютно стойкий |  |
| g | Если для всех пар сообщение – шифртекст () имеется одинаковое количество ключей , таких что , то шифр на - абсолютно стойкий |  |
| h | Для семантически стойкого шифра энтропия ключа всегда больше или равна энтропии открытого текста. |  |
|  | **Не заполнять!** | / 8 |

1. Пусть – одноразовый блокнот на (множество векторов длины , для которых чётные координаты равны 1.   
   Является ли семантически стойким шифром? Если нет продемонстрируйте атаку с преимуществом равным 1.

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

1. Пусть – подстановочный шифр на (множество подстановок на ).   
   Является ли семантически стойким шифром? Если нет продемонстрируйте атаку с преимуществом равным 1.

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

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

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

1. – семантически стойкий шифр на . Пусть – функция сжатия без потерь. Заметим, что демонстрирует разный уровень сжатия для различных сообщений.
   1. Пусть в игре на семантическую стойкость Претендент сжимает сообщения перед зашифрованием, т.е. . Является ли данная схема семантически стойкой? Если да – доказать, иначе – продемонстрировать атаку. Имеет ли данная схема смысл для уменьшения размера шифрткеста? Почему?
   2. Пусть в игре на семантическую стойкость Претендент сжимает шифртекста после зашифрования, т.е. . Является ли данная схема семантически стойкой? Если да – доказать, иначе – продемонстрировать атаку.

Имеет ли данная схема смысл для уменьшения размера шифрткеста? Почему?

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

1. Пусть – семантически стойкий шифр на . Банковская организация желает разделить секретный ключ **на две части** и , так, что **обе** необходимы для расшифрования.

Банк генерирует случайное число и вычисляет . Тогда .

Аналогичная задача для трех сторон: разделяя ключ на **три** части можно получить ключ по **любым двум** из ним: банк генерирует пары и , такие что . Как следует разделить части пар между частями?

|  |  |  |
| --- | --- | --- |
| № | Задание | Ответ |
| a |  |  |
| b |  |  |
| c |  |  |
| d |  |  |
| e |  |  |
|  | **Не заполнять!** | /1 |