Задание 8,

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

1. Выберите верные утверждения:

|  |  |  |
| --- | --- | --- |
| № | Задание | Ответ |
| a | Любой случайный оракул стойкий к нахождению коллизий второго рода |  |
| b | Любая стойкая к коллизиям второго рода хэш-функция является стойкой к коллизиям первого рода |  |
| c | Любая стойкая к коллизиям второго рода хэш-функция является стойкой односторонней хэш-функцией |  |
| d | Любой стойкий MAC с фиксированным ключом и сверх-полиномиальной областью определения даёт стойкую к коллизиям хэш-функцию |  |
| e | На любую хэш-функцию на возможна теоретическая атака сложностью |  |
| f | Атака на стойкость хэш-функции в модели случайного оракула даёт атаку в модели односторонней хэш-функции |  |
| g | Атака на стойкость к коллизиям второго рода для некоторой хэш-функции даёт атаку на случайный оракул для данной функции. |  |
| h | Отправка хэш-значения для некоторой величины (выбранной равномерно из множества со сверх-полиномиальной мощностью) по открытому каналу гарантирует, что противник не сможет восстановить данную величину. (используется хэш-функция, стойкая к коллизиям второго рода) |  |
|  | **Не заполнять!** | / 8 |

1. Рассмотри следующие функции сжатия

Задача – найти 4 различные пары :

Необходимо вывести в виде формулы получение этих пар и представить ответ в виде hex-строки.

|  |  |
| --- | --- |
|  | Ответ |
|  | Доп. Листы. |
| **Не заполнять!** | /4 |

1. Пусть и – стойкие к коллизиям хэш-функции на . Доказать, что – стойкая к коллизиям хэш-функция. Доказать от противного – предположить, что не стойкая к коллизиям.

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

1. Пусть – стойкая к коллизиям хэш-функция. Какая их описанных хэш-функций является стойкой? Формально докажите или опровергните стойкость.

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

1. Докажите утверждения ниже

Пусть – случайный оракул. . Какова сложность нахождения тройной коллизии, т.е. трех различных величин ? (ответ + его вывод на доп. Листах)

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

1. Почитать что такое дерево Меркла (Merkle tree), просмотра и осознание картинки на последней странице дз – достаточно.

Пусть имеется 647 различных файлов. Ответе на вопросы ниже.

|  |  |  |
| --- | --- | --- |
| № | Задание | Ответ |
| a | Какова высота дерева меркла для вычисления хэш-значения, обеспечивающего целостность всех файлов? |  |
| b | Какое количество хэшей необходимо пересчитать, при замене одного из файлов? |  |
| c | Какое минимальное количество хэшей необходимо пересчитать при замене 4-х файлов? |  |
| d | Какое максимальное количество хэшей необходимо пересчитать при замене 4-х файлов? |  |
| e | Какое количество хэшей необходимо вычислить при построении дерева? |  |
| f | Сколько узлов хэш значений отвечает за целостность одного файла? |  |
| g | За целостность какого количество файлов отвечает корневой узел? |  |
| h | Предположим необходимо переслать один из файлов. Предполагая, что получатель знает только значение корня дерева (и может проверить только его) Меркла, какое минимальное количество узлов дерева необходимо переслать вместе с файлом, для осуществления проверки файла получателем? (authentication path) |  |
|  | **Не заполнять!** | / 8 |



