Задание 9,

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

1. Выберите верные утверждения:

|  |  |  |
| --- | --- | --- |
| № | Задание | Ответ |
| a | Любую схему стойкого аутентифицированного шифрования можно использовать в качестве стойкого кода аутентичности |  |
| b | При использовании схемы MAC-then-Encrypt необходимо использовать независимые ключи для MAC и шифрования |  |
| c | При использовании схемы EAX необходимо использовать независимые ключи для MAC и шифрования |  |
| d | CCA стойкость более сильно определение, чем CPA стойкость |  |
| e | Возможно построить CCA стойкий шифр, который не будет CPA стойким |  |
| f | Обеспечение целостности открытых текстов не может быть обеспечено через целостность соответствующих шифртекстов |  |
| g | Схема Encrypt-and-MAC в общем случае является нестойкой |  |
| h | CCA стойкости достаточно для защиты аутентичности от пассивных противников |  |
| i | Целостность шифртекстов более сильное определение, чем целостность открытых текстов, при передаче шифртекстов по каналу связи |  |
|  | **Не заполнять!** | / 9 |

1. Пусть – случайная величина, полученная с использованием **неравномерного** распределения, :

Иными словами, выбирается из подмножества векторов в , для которых первые 128 бит – нулевые.

Пусть – стойкая PRF, с множеством ключей . Какие из PRF ниже является стойкими PRF (в практическом смысле, минимальный параметр стойкость – 80 бит), но не является стойкими при выборе c использованием распределения, описанного выше?

|  |  |  |
| --- | --- | --- |
| № | Задание | Ответ |
| a |  |  |
| b |  |  |
| c |  |  |
| d |  |  |
|  | **Не заполнять!** | / 8 |

1. Пусть – схема стойкого аутентифицированного симметричного шифрования на . Какие из схем ниже являются стойкими схемами аутентифицированного шифрования (формально докажите или опровергните).

|  |  |  |
| --- | --- | --- |
| № | Задание | Ответ |
| a |  |  |
| b |  |  |
| c |  |  |
| d |  |  |
| e |  |  |
| f |  |  |
|  | **Не заполнять!** | /12 |

1. Пусть – строго стойкий блочный шифр на - пренебрежимо малая. Докажите, что шифр ниже стойкий CCA шифр, но не стойкий AE шифр (не обеспечивается целостность шифртекстов). Строго стойкий блочных шифр (strongly secure block cipher) – шифр, стойкий против противников, которые могут помимо запросов на зашифрование произвольных блоков запрашивать запросы на расшифрование произвольных блоков блочного шифра в игре на стойкость блочного шифра (PRP).

|  |  |
| --- | --- |
|  | Ответ |
|  | Доп. Листы. |
| **Не заполнять!** | /2 |