Задание 7,

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

1. Выберите верные утверждения:

|  |  |  |
| --- | --- | --- |
| № | Задание | Ответ |
| a | Любая стойкая PRF даёт стойкий MAC |  |
| b | Любая стойкая PRF, с суперполиномиальной областью значений даёт стойкий MAC |  |
| c | Любая стойкая PRP, с суперполиномиальной областью значений даёт стойкий MAC |  |
| d | Стойкая PRF является более сильным определением, чем стойкий MAC |  |
| e | На любой MAC на возможна теоретическая атака сложностью |  |
| f | На любой CBC-MAC на возможна теоретическая атака сложностью |  |
| g | CMAC требует использования трех независимых случайных ключей |  |
| h | Любое беспрификсное кодирование увеличивает длину сообщения |  |
| i | MAC обеспечивает целостность сообщений при передаче |  |
| j | MAC обеспечивает аутентичность источника информации (т.е. гарантирует, что только имеющий секретный ключ мог отправить это сообщение) |  |
| k | Добавление длины сообщения в конец сообщения является беспрификсным кодированием |  |
|  | **Не заполнять!** | / 10 |

1. Рассмотрим ECBC MAC. Вместо использования нулевого IV будем использовать случайный IV для каждого сообщения и включать его в состав итоговой метки. Т.е. . Данная система не является стойким MAC. Задача – от имени противника получить верный MAC для сообщения , где – размер блока PRF. Является ли данный MAC **беспрификсным** PRF?

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

1. Alice отправляет данные 6 получателям . Задача – обеспечить целостность. Alice использует MAC. Использование одного ключа для всех получателей не обеспечивает целостность, так как если противником является один из получателей он может подделать MAC для любого сообщения и рассылать пакета от имени Alice. Вместо этого Alice использует 4 секретных ключа . Alice пересылает по защищенному каналу некое подмножество каждому получателю . Пересылая затем каждое сообщение, она включает также 4 кода аутентичности для каждого сообщения, выработанных на этих ключах. Каждый пользователь считает пакет целостным, если для всех его ключей совпали коды аутентичности (те кода, которые не соответствуют ключам пользователя им игнорируются).

Как Alice должна распределить ключи между пользователями?

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

1. Пусть – стойкий MAC на . Какой их описанных MAC является стойким? Формально докажите или опровергните стойкость. Если явно не указан алгоритм проверки – считать MAC детерминированным.

|  |  |  |
| --- | --- | --- |
| № | Задание | Ответ |
| a |  |  |
| b |  |  |
| c |  |  |
| d |  |  |
| e |  |  |
| f |  |  |
| g |  |  |
| h |  |  |
| i |  |  |
| j |  |  |
| k |  |  |
|  | **Не заполнять!** | /22 |

1. Докажите утверждения ниже

|  |  |  |
| --- | --- | --- |
| № | Задание | Ответ |
| a | Пусть – MAC.  Пусть , .  Докажите, что – стойкий, если хотя бы один из – стойкий MAC | (доп листы) |
| b | Пусть – **детерминированные** MAC.  Пусть .  Докажите, что – стойкий, если хотя бы один из – стойкий MAC | (доп листы) |
|  | **Не заполнять!** | /4 |