Задание 6,

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

**В заданиях для простоты вычислений предполагать, что гага=гиби=gibi= , мега=меби =mebi= , число секунд в году .**

1. В некоторой криптосистеме используется поточный блочный шифр в детерминированном режиме CTR.

Ответе на вопросы ниже

|  |  |  |  |
| --- | --- | --- | --- |
| № | Задание | Ответ | |
| a | Предполагая стойкость блочного шифра с функцией зашифрования , является ли описанная криптосистема стойкой при **одноразовом использовании ключа** в теоретическом (предельном) смысле? (записать в ответ да или нет) Почему? (на доп листах) |  | |
| b | Предполагая стойкость блочного шифра с функцией зашифрования , является ли описанная криптосистема стойкой при **многоразовом использовании ключа (ключ используется для шифрования нескольких сообщений)** в теоретическом (предельном) смысле? (записать в ответ да или нет) Почему? (на доп листах) |  | |
| c | Пусть в качестве используется PRP, с длинной ключа 128 бит, размер блока 128 бит, параметр стойкости принять равным 128 бит.  Пусть имеется защищенный канал связи с пропускной способностью 100 mebibit, в котором непрерывно шифруются сообщения. Оценить вероятность атаки на криптосистему в течении одного года, при условии что симметричный ключ не меняется. |  | |
| d | Пусть в качестве используется PRP, с длинной ключа 128 бит, размер блока 64 бит, параметр стойкости принять равным 120 бит.  Пусть имеется защищенный канал связи с пропускной способностью 100 mebibit, в котором непрерывно шифруются сообщения. Оценить необходимую частоту смены симметричного ключа, при заданной вероятности атаки равной . |  | |
|  | **Не заполнять!** | / 8 | / 8 |

1. После анализа симметричной криптосистемы была получена следующая оценка стойкости в сведении к псевдослучайной функции , где – функция зашифрования блочного шифра, – максимальное число обращений к криптосистеме при фиксированном ключе, – размер блока PRF, – размер выхода криптосистемы.

Ответе на вопросы ниже

|  |  |  |  |
| --- | --- | --- | --- |
| № | Задание | Ответ | |
| a | Предполагая стойкость блочного шифра с функцией зашифрования , является ли описанная криптосистема стойкой в теоретическом (предельном) смысле? (записать в ответ да или нет) Почему? (на доп листах) |  | |
|  | **Не заполнять!** | / 1 | / 1 |

1. Выберите верные утверждения:

|  |  |  |
| --- | --- | --- |
| № | Задание | Ответ |
| a | Любая PRP является PRF |  |
| b | Любая PRF является PRP |  |
| c | Любая стойкая PRF является PRP |  |
| d | Любая стойкая PRP является стойкой PRF |  |
| e | Любая стойкая PRP с суперполиномиальным образом является стойкой PRF |  |
| f | Любой стойкий блочный шифр является стойкой PRF |  |
| g | Любой семантически стойкий шифр (одноразовое использование ключа) должен быть детерминированным |  |
| h | Любой CPA стойкий шифр является семантически стойким при одноразовом использовании ключа. |  |
|  | **Не заполнять!** | / 8 |

1. Пусть шифр на .

|  |  |  |
| --- | --- | --- |
| № | Задание | Ответ |
| a | Пусть длина сообщений и длины соответствующих шифртекстов совпадают для всех ключей. Показать, что – не CPA стойкий. |  |
| b | Пусть длина шифртекстов больше длины соответствующих открытых текстов на бит. Показать, что существует атака на CPA стойкость сложностью с преимуществом . |  |
|  | **Не заполнять!** | / 6 |

1. Рассмотрим следующую игру. Пусть шифр определён на , где множество сообщений такое, что можно эффективно выбрать случайное сообщение с равномерным распределением. Показать, что если CPA стойкий, тогда невозможно выиграть игру на генерацию двух одинаковых шифртекстов. Оценить преимущества в игре на генерацию одинаковых шифртекстов для CPA стойкого шифра. Игра на генерацию выглядит следующим образом – претендент генерирует случайный ключ, противник отправляет откртых текстов, получая шифртекстов на ключе претендента. Если хотя бы одна пара шифртекстов совпадает – противник выигрывает игру.

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

*n. Hard mode on.* ***Опционально (т.е. можно не делать).***

*Решить задачу 4.2. на странице 165 книги A Graduate Course in Applied Cryptography v0.4*

*+ 10 к итоговой оценке за семестр.*