Задание 6,

Фамилия _____

В заданиях для простоты вычислений предполагать, что гага=гиби=gibi= 2^{30}, мега=меби =mebi= 2^{20}, число секунд в году $\sim 2^{23}$.

1. В некоторой криптосистеме используется блочный шифр в детерминированном режиме CTR. Ответе на вопросы ниже

№	Задание	Ответ	
a	Предполагая стойкость блочного шифра с функцией зашифрования E, 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 E, 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 E 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/s, 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 E 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/s, в котором непрерывно шифруются сообщения. Оценить необходимую частоту смены симметричного ключа, при заданной вероятности атаки равной 2^{-7}.		
	Не заполнять!	/ 8	/ 8

** при вычислениях полагать что шифруется единственное сообщение максимальной длинны, которое может быть передано в указанном канале за заданное время.*

2. После анализа симметричной криптосистемы была получена следующая оценка стойкости в сведении к псевдослучайной функции $Adv[A, C] \leq \frac{tn}{N}(\frac{tQ}{N} + Adv_{prf}[B, E])$, где E – функция зашифрования блочного шифра, Q – максимальное число обращений к криптосистеме при фиксированном ключе, $N = 2^n, n$ – размер блока PRF, t – размер выхода криптосистемы. Ответе на вопросы ниже

№	Задание	Ответ
a	Предполагая стойкость блочного шифра с функцией зашифрования E, является ли описанная криптосистема стойкой в теоретическом (предельном) смысле? (записать в ответ да или нет) Почему? (на доп листах)	

	Не заполнять!	/ 1	/ 1

3. 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 со сверх-полиномиальным 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

4. Пусть (E, D) шифр на (K, M, C).

№	Задание	Ответ
a	Пусть длина сообщений и длины соответствующих шифртекстов совпадают для всех ключей. Показать, что (E, D) – не CPA стойкий.	
b	Пусть длина шифртекстов больше длины соответствующих открытых текстов на l бит. Показать, что существует атака на CPA стойкость сложностью $2^{l/2}$ с преимуществом $½$.	
	Не заполнять!	/ 6

5. Рассмотрим следующую игру. Пусть шифр (E, D) определён на (K, M, C), где множество сообщений такое, что можно эффективно выбрать случайное сообщение с равномерным распределением. Показать, что если (E, D) 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 q откртых текстов, получая q 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.