

Задание 6,

Фамилия _____

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 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 многократном использовании ключа (ключ используется для шифрования нескольких сообщений) в теоретическом (предельном) смысле? (записать в ответ да или нет) Почему? (на доп листах)		
b	Пусть в качестве E используется функция зашифрования AES, с длиной ключа 128 бит, размер блока 128 бит, параметр стойкости принять равным 126 бит. Предполагая, что при реализации криптосистемы использован процессор, с частотой 16ГГц, и на за шифрование одного блока требуется 4 такта, оценить вероятность взлома криптосистемы в ближайшие 10 лет (предположить, что ключ не меняется).		
c	Аналогично заданию b, только вместо AES использовать ГОСТ «МАГМА», размер блока 64 бита, размер ключа 128 бит. Параметр стойкости предположить равным 120 бит.		
	Не заполнять!	/ 6	/ 6

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 блочного шифра, 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)		
b	Пусть в качестве E используется функция зашифрования AES, с длиной ключа 128 бит, размер блока 128 бит, параметр стойкости принять равным 126 бит. Пусть размер выхода криптосистемы – 256 бит. Пусть противник способен взаимодействовать с криптосистемой каждые 4 такта. Противник имеет 16 ядерный процессор с частотой 32 гГц. Оценить вероятность успешной атаки на		

	криптосистему для описанного противника, при условии что доступ к системе он имел не более 30 секунд.		
c	Аналогично заданию b, только противник имел доступ к криптосистеме в течении года.		
d	Аналогично заданию b, только вместо AES использовать ГОСТ «МАГМА», размер блока 64 бита, размер ключа 128 бит. Параметр стойкости предположить равным 120 бит.		
	Не заполнять!	/ 8	/ 8

3. После анализа симметричной криптосистемы была получена следующая оценка стойкости в сведении к семантической стойкости блочного шифра в режиме CRT $Adv[A, C] \leq \frac{(tQ)^7}{n^{16}} Adv_{SS}[B, E]$, где E – функция зашифрования блочного шифра в режиме CTR, Q – максимальное число обращений к криптосистеме при фиксированном ключе, $N = 2^n$, n – размер блока блочного шифра, 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)		
b	Пусть в качестве шифра E используется поточный шифр на основе функции зашифрования AES, с длиной ключа 128 бит, размер блока 128 бит, параметр стойкости принять равным 126 бит. Пусть размер выхода криптосистемы – 256 бит. Получить параметр стойкости описанной криптосистемы, предполагая что ключ криптосистемы меняется каждые 2^{24} операции обращения.		
c	Аналогично заданию b, тогда ключ меняется каждые 2^{17} операции.		
d	Аналогично заданию b, только вместо AES использовать ГОСТ «МАГМА», размер блока 64 бита, размер ключа 128 бит. Параметр стойкости предположить равным 120 бит.		
	Не заполнять!	/ 6	/ 6

4. 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	

n. Hard mode on.

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

*+ 10 и итоговой оценке за семестр. **Опционально (те можно не делать).***