1. Расположите модели стойкости хэш-функций от более слабых к более сильным (из более сильных определений следуют более слабые):
   1. Случайный оракул
   2. Стойкость к коллизиям первого рода
   3. Стойкость к коллизиям второго рода
   4. Односторонняя хэш-функция

**Ответ: d, b, c, a**

1. Сколько сообщений шифрует претендент в ходе игры на семантическую стойкость шифра (одноразовое использование ключа)?

**Ответ: 1**

1. Какое из следующих утверждений **НЕ** верно?
   1. Для семантической стойкости шифра на основе режима CBC в модели атак по открытому тексту (CPA стойкость, множественное использование ключа) необходимо использование случайного равномерно распределенного вектора в качестве IV для каждого шифруемого сообщения.
   2. Режим шифрования CTR не требует обратимости используемой псевдослучайной функции (PRF) в процедурах шифрования и расшифрования
   3. ECB является семантически стойким шифром для сообщений, длинны которых кратны размеру входа псевдослучайной перестановки (PRP)
   4. Режим CTR позволяет вычислять зашифрование каждого блока открытого текста независимо от других

**Ответ: c**

1. Какое из следующих утверждений верно?
   1. Если алгоритм противника A в некоторой игре против Ε эффективный, то величина Adv[A,Ε] (преимущество противника A против E) – пренебрежимо малая
   2. Любая полиномиально ограниченная величина– пренебрежимо малая величина
   3. Аддитивный одноразовый блокнот переменной длины – семантически стойкий шифр
   4. Если шифр имеет длины ключей больше длин шифртекстов, то он абсолютно стойкий

**Ответ: с**

1. Установите соответствие между моделями стойкости и целями противника
   1. Стойкий код аутентичности сообщений (MAC)
   2. Стойкая псевдослучайная функция (PRF)
   3. Семантически стойкий шифр
   4. Стойкий аутентифицированный шифр
      1. Выработка новой пары сообщение-метка
      2. Навязывание новых шифртекстов и/или различимость множества пар сообщений, зашифрованных на одном ключе, по их шифртекстам
      3. Эффективная различимость наблюдаемых противником значений, полученных с использованием фиксированного ключа, от случайных
      4. Эффективная различимость пары сообщений, зашифрованных на одном ключе, по их шифртекстам

**Ответ: a – 1, b – 3, c – 4, d – 2**

1. Какое из следующих утверждений верно?
   1. Обеспечение целостности открытых текстов не может быть обеспечено через целостность соответствующих шифртекстов
   2. Любую схему стойкого аутентифицированного шифрования можно использовать в качестве стойкого кода аутентичности сообщений (MAC)
   3. Любой стойкий код аутентичности сообщений (MAC) с фиксированным ключом и сверх полиномиальной областью определения даёт стойкую к коллизиям хэш-функцию
   4. Возможно существование стойкого блочного шифра (в модели PRP), не стойкого к восстановлению ключа

**Ответ: b**

1. Какое из следующих утверждений **НЕ** верно?
   1. Любая пренебрежимо малая величина – полиномиально ограниченная на бесконечности
   2. Любой эффективный алгоритм – полиномиально ограничен памятью
   3. Эффективное (за полиномиальное время) вычисление абсолютно стойких шифров невозможно

**Ответ: c**

1. Какова максимально возможная энтропия ключа длинны 128 бит?

**Ответ: 128**

1. Пусть имеется некоторая псевдослучайная перестановка (PRP), с размером ключа 128 бит, и размером выхода 256 бит. Какова максимально возможная энтропия выхода данной функции, при случайном равновероятном выборе ключа?

**Ответ: 128**

1. Какое из следующих утверждений верно?
   1. Encrypt-then-mac в общем случае реализует стойкую схему аутентифицированного шифрования
   2. Mac-then-encrypt в общем случае реализует стойкую схему аутентифицированного шифрования
   3. Encrypt-and-mac в общем случае реализует стойкую схему аутентифицированного шифрования
   4. Все из описанных выше схем являются стойкими схемами аутентифицированного шифрования

**Ответ: a**