Билет 1.

1. Вычислимый шифр и шифр Шеннона. Понятие абсолютной стойкости
2. CPA стойкость, модель, игры, отличия от одноразовой семантической стойкости.
3. Пусть – стойкий MAC на . Какой их описанных MAC является стойким? Формально докажите или опровергните стойкость.

|  |
| --- |
|  |
|  |

Билет 2.

1. Поточные шифры и псевдослучайные генераторы, модель, игры, принципы построения, примеры
2. Режимы шифрования, различия, стойкость в моделях CPA и семантической стойкости.
3. Пусть – стойкая PRF, . Какие из следующих алгоритмов является стойкими PRF? Для каждого алгоритма предоставить доказательство стойкости или атаку.

|  |
| --- |
|  |
|  |

Билет 3.

1. Блочные шифры, PRP, PRF, модель, игры, примеры.
2. Схемы аутентифицированного шифрования. Преимущества и недостатки.
3. Пусть – стойкая к коллизиям хэш-функция. Какая их описанных хэш-функций является стойкой? Формально докажите или опровергните стойкость.

|  |
| --- |
|  |
|  |

Билет 4.

1. Хэш-функции модель, игры, причины появления, понятие стойкости (4 штуки).
2. Построение кодов аутентичности сообщений на основе блочных шифров.
3. Пусть – схема стойкого аутентифицированного симметричного шифрования на . Какие из схем ниже являются стойкими схемами аутентифицированного шифрования (формально докажите или опровергните).

|  |
| --- |
|  |
|  |

Билет 5.

1. Аутентифицированное шифрование, модель, игры, причины появления, понятие стойкости (стойкий аутентифицированный шифр и CAA стойкость).
2. Выработка ключей с использованием HKDF.
3. Пусть – стойкий PRG. Какие из следующих алгоритмов является семантически стойкими? Для каждого алгоритма предоставить доказательство стойкости или атаку.

|  |
| --- |
|  |
| *-* побитовый OR |

Билет 1.

1. Принципы доказательной криптографии, понятие модели и игры.
2. Схемы AEAD шифрования.
3. Пусть – стойкий MAC на . Какой их описанных MAC является стойким? Формально докажите или опровергните стойкость.

|  |
| --- |
|  |
|  |

Билет 2.

1. Пренебрежимо малые, сверх-полиномиальные и полиномиально ограниченные величины. Ограничения на противников и параметры схемы при рассмотрении стойкости.
2. Различия CPA и CCA стойкости. (Какая сильнее, примеры примитивов).
3. Пусть – стойкая к коллизиям хэш-функция. Какая их описанных хэш-функций является стойкой? Формально докажите или опровергните стойкость.

|  |
| --- |
|  |
|  |

Билет 3.

1. Псевдослучайные генераторы.
2. Различия в моделях стойкости к коллизиям первого и второго рода в хэш-функциях. (Какая сильнее, примеры примитивов).
3. Пусть – стойкая PRF, . Какие из следующих алгоритмов является стойкими PRF? Для каждого алгоритма предоставить доказательство стойкости или атаку.

|  |
| --- |
|  |
|  |

Билет 4.

1. Модель стойкого блочного шифра, PRF и PRP.
2. Губчатая конструкция при построении хэш-функции, SHA-3, построение схемы аутентифицированного шифрования с использованием губчатой конструкции.
3. Пусть – схема стойкого аутентифицированного симметричного шифрования на . Какие из схем ниже являются стойкими схемами аутентифицированного шифрования (формально докажите или опровергните стойкость).

|  |
| --- |
|  |
|  |

Билет 5.

1. Семантическая стойкость, следствия и необходимые условия.
2. Стандартная модель и модель случайного оракула.
3. Пусть – стойкий PRG. Какие из следующих алгоритмов является стойкими PRG? Для каждого алгоритма предоставить доказательство стойкости или атаку.

|  |
| --- |
|  |
| *-* побитовый OR |

Билет 6.

1. Стойкость при множественном использовании ключа, CPA стойкость.
2. Выработка ключей с использованием источника энтропии с неравномерным распределением, KDF, HKDF
3. Пусть – стойкая к коллизиям хэш-функция. Какая их описанных хэш-функций является стойкой? Формально докажите или опровергните стойкость.

|  |
| --- |
|  |
|  |

Билет 7.

1. Режимы шифрования блочных шифров.
2. Недостатки режимов Encrypt-And-Mac и Mac-Then-Encrypt при построении аутентифицированных шифров. Возможные атаки.
3. Пусть – стойкий MAC на . Какой их описанных MAC является стойким? Формально докажите или опровергните стойкость. Если явно не указан алгоритм проверки – считать MAC детерминированным.

|  |
| --- |
|  |
|  |

Билет 8.

1. Коды аутентичности сообщений, обеспечение целостности сообщений.
2. Принципы построения блочных шифров. DES, AES, Кузнечик, Магма.
3. Пусть – стойкая PRF, . Какие из следующих алгоритмов является стойкими PRF? Для каждого алгоритма предоставить доказательство стойкости или атаку.

|  |
| --- |
|  |
|  |

Билет 9.

1. Построение кодов аутентичности сообщений на основе блочных шифров.
2. Модели абсолютной и семантической стойкости шифров. Их различия и применимость.
3. Пусть – семантически стойкий шифр на . Какие из следующих алгоритмов является семантически стойкими? Для каждого алгоритма предоставить доказательство стойкости или атаку.

|  |
| --- |
|  |
|  |

Билет 10.

1. Стойкие к коллизиям и односторонние хэш-функции.
2. Аутентифицированное шифрование. Encrypt-And-Mac, Encrypt-Then-Mac, Mac-Then-Encrypt.
3. Пусть – стойкая PRF, . Какие из следующих алгоритмов является стойкими PRF? Для каждого алгоритма предоставить доказательство стойкости или атаку.

|  |
| --- |
|  |
| . |

Билет 11.

1. Принципы построения хэш-функций.
2. Построение кодов аутентичности сообщений с использование хэш-функций. Выработка симметричных ключей с использованием хэш-функций и источника энтропии.
3. Пусть – стойкий MAC на . Какой их описанных MAC является стойким? Формально докажите или опровергните стойкость. Если явно не указан алгоритм проверки – считать MAC детерминированным.

|  |
| --- |
|  |
|  |

Билет e11

1. Понятие игры. Пренебрежимо малые, сверх-полиномиальные и полиномиально ограниченные величины. Ограничения на противников и параметры схемы при рассмотрении стойкости.
2. Аутентифицированное шифрование. Построение аутентифицированных шифров на основе блочных шифров. Модели стойкости CCA, AE. Режимы AEAD шифрования.
3. Пусть – стойкий MAC на . Какой их описанных MAC является стойким? Формально докажите или опровергните стойкость обоих конструкций. Если явно не указан алгоритм проверки – считать MAC детерминированным.

|  |
| --- |
|  |
|  |

1. Хэш функции, модели стойкости, принципы построения.