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 |