Билет 1.

1. Вычислимый шифр и шифр Шеннона. Понятие абсолютной стойкости
2. CPA стойкость, модель, игры, отличия от одноразовой семантической стойкости.
3. Пусть (S, V) – стойкий MAC на $(K, M, T), M = \{0,1\}^n, T = \{0,1\}^{128}$. Какой их описанных MAC является стойким? Формально докажите или опровергните стойкость.

$S'(k, m) = S(k, m\|\|m), V'(k, m, t) = V(k, m\|\|m, t)$
$S'\big((k_1, k_2), (a_1, a_2)\big) = S(k_1, a_1)\|\|S(k_2, a_2)$

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 $F: K \times X \to Y$ – стойкая PRF, $K = X = Y = \{0,1\}^n$. Какие из следующих алгоритмов является стойкими PRF? Для каждого алгоритма предоставить доказательство стойкости или атаку.

$F'(k, x) = F(k, x) \oplus 1^n$
$F'(k, x) = F(k, x)\|\|0$

Билет 3.

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

$H(m) \oplus H(m)$
$H(m)\|\|H(m)$

Билет 4.

1. Хэш-функции модель, игры, причины появления, понятие стойкости (4 штуки).
2. Построение кодов аутентичности сообщений на основе блочных шифров.
3. Пусть (E, D) – схема стойкого аутентифицированного симметричного шифрования на $(K, \{0,1\}^n, \{0,1\}^s)$. Какие из схем ниже являются стойкими схемами аутентифицированного шифрования (формально докажите или опровергните).

$E'(k,m) = (E(k,m), 0)$ $D'\big(k,(c,d)\big) = D(k,c)$
$E'(k,m) = E(k, m \oplus 1^n)$ $D'(k,c) = \begin{cases} D(k,c) \oplus 1^n, \text{if } D(k,c) \neq \perp \\ \perp, \text{else} \end{cases}$

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 $G: \{0,1\}^s \to \{0,1\}^n$ – стойкий PRG. Какие из следующих алгоритмов является семантически стойкими? Для каждого алгоритма предоставить доказательство стойкости или атаку.

$G'(k) = G(k) \| \| G(k)$
$G'(k, k') = G(k) \vee G(k')$,∨- побитовый OR