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

Билет 1.

1. Принципы доказательной криптографии, понятие модели и игры.
2. Схемы AEAD шифрования.
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. Пренебрежимо малые, суперполиномиальные 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 $H: M \to T$ – 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 3.

1. Псевдослучайные генераторы.
2. Различия в моделях стойкости к коллизиям первого и второго рода в хэш-функциях. (Какая сильнее, примеры примитивов).
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 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 (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 стойкость).

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

Билет 5.

1. Семантическая стойкость, следствия и необходимые условия.
2. Стандартная модель и модель случайного оракула.
3. Пусть $G: \{0,1\}^s \to \{0,1\}^n$ – стойкий PRG. Какие из следующих алгоритмов является стойкими PRG? Для каждого алгоритма предоставить доказательство стойкости или атаку.

$G'(k) = G(k)\|\|G(k)$
$G'(k,k') = G(k) \vee G(k')$,∨- 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 $H: M \to T$ – стойкая к коллизиям хэш-функция. Какая их описанных хэш-функций является стойкой? Формально докажите или опровергните стойкость.

$H'(m) = H(m) \| H(0)$
$H'(m) = HMAC(m, m)$

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 (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. Если явно не указан алгоритм проверки V – считать MAC детерминированным.

$S'\big(k, (a_1, a_2)\big) = S(k, a_1) \| \| S(k, a_2)$
$S'\big(k, (a_1, a_2)\big) = S(k, a_1) \oplus S(k, a_2)$

Билет 8.

1. Коды аутентичности сообщений, обеспечение целостности сообщений.
2. Принципы построения блочных шифров. DES, AES, Кузнечик, Магма.
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.

$F'((k_1, k_2), x) = F(k_1, x) \oplus F(k_2, x)$
$F'(k, x) = F(k, x) \| \| F(k, x \oplus 1^n)$

Билет 9.

1. Построение кодов аутентичности сообщений на основе блочных шифров.
2. Модели абсолютной и семантической стойкости шифров. Их различия и применимость.
3. Пусть $\mathrm{E} = (E, D)$ – семантически стойкий шифр на (K, M, C): $M = C = \{0,1\}^L$. Какие из следующих алгоритмов является семантически стойкими? Для каждого алгоритма предоставить доказательство стойкости или атаку.

$E'(\,(k, k'),\, m) = E(k, m)\|\|E(k', m)$
$E'(\,(k, k'),\, m) = (c, c)$: $c \overset{R}{\leftarrow} E(k, m)$

Билет 10.

1. Стойкие к коллизиям и односторонние хэш-функции.
2. Аутентифицированное шифрование. Encrypt-And-Mac, Encrypt-Then-Mac, Mac-Then-Encrypt.
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.

$F'\big(k,(x,y)\big) = F(k,x) \oplus F(k,y)$
$F'(k,x) = F(k,x) \oplus x.$

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 (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. Если явно не указан алгоритм проверки V – считать MAC детерминированным.

$S'(k,m) = S(k, m \oplus 1^n), V'(k,m,t)$ $= (k, m \oplus 1^n, t)$
$S'(k,m) = [t \leftarrow S(k,m), output\ (t,t)]$ $V'(k,m,(t_1,t_2)) = \begin{cases} V(k,m,t), if\ t_1 = t_2 \\ 0, else \end{cases}$