Задание 1.

Фамилия ____

1. Вычислить энтропию ($H(a)$) следующих величин:

№	Задание	Ответ
a	$a \in_R \{0,1\}^7$, равномерное распределение	
b	$a = (00000000) \in \{0,1\}^8$	
c	$a = (0110110110) \in \{0,1\}^{10}$	
d	$a = (0110101110001) \in \{0,1\}^{13}$	
e	$a \in_R \{0,1\}^{10}: a_0 = 1$	
f	$a \in_R \{0,1\}^{10}: a_0 = a_9$	
g	$a \in_R \{0,1\}^{16}: a_i = a_{i-1} \oplus 1, i = 1..15$	
h	$a \in_R \{0,1\}^{16}: a_{2k} = 0, k = 0..7$	
	Не заполнять!	/ 8

2. Рассмотрим игру с двумя экспериментами.
   a. В эксперименте 0 претендент подбрасывает монетку и возвращает **РЕШКА**, если выпала решка, и **ОРЁЛ** если орёл.
   b. В эксперименте 1 претендент всегда возвращает **ОРЁЛ**.

   Цель противника различить два эксперимента. Пусть W_b событие того, что в эксперименте $b \in \{0,1\}$ противник возвращает 1. Преимущество противника $\mathrm{Adv}[A] = |\Pr[W_0] - \Pr[W_1]| \in [0,1]$.

   Вычислить $\mathrm{Adv}[A]$ для следующих алгоритмов:

№	Задание	Ответ
a	A: всегда возвращает 1	
b	A: возвращает 1, с вероятностью $\frac{1}{2}$, иначе – 0	
c	A: возвращает 1, если от претенденто получено РЕШКА	
d	A: возвращает 0, если от претенденто получено РЕШКА	
e	A: если получено РЕШКА возвращает 1. Иначе – (возвращает 1, с вероятность $\frac{1}{2}$, иначе 0)	
f	A: $\mathrm{Adv}[A] = max$, построить A	
	Не заполнять!	/ 6

3. Выберите верные утверждения:

№	Задание	Ответ
a	Абсолютно стойкий шифр всегда семантически стойкий	
b	Любой шифр Шеннона является абсолютно стойким	
c	Аддитивный одноразовый блокнот – семантически стойкий шифр	
d	Аддитивный одноразовый блокнот переменной длины – семантически стойкий шифр	
e	Если шифр имеет длины ключей больше длин шифртекстов то он абсолютно стойкий	
f	Если шифр имеет и энтропии длины ключей больше длин и энтропий шифртекстов то он абсолютно стойкий	

g	Если для всех пар сообщение – шифртекст ($(m, c) \in M \times C$) имеется одинаковое количество ключей $k_i \in K$, таких что $E(k, m) = c$, то шифр $\mathrm{E} = (E, D)$ на (K, M, C) - абсолютно стойкий	
h	Для семантически стойкого шифра энтропия ключа всегда больше или равна энтропии открытого текста.	
	Не заполнять!	/ 8

4. Пусть $\mathrm{E} = (E, D)$ – одноразовый блокнот на (K, M, C): $M = C = \{0,1\}^L, K = \{k \in \{0.1\}^L : k_{2i} = 1, i = 0..\frac{L}{2} - 1\}$ (множество векторов длины L, для которых чётные координаты равны 1). Является ли E семантически стойким шифром? Если нет продемонстрируйте атаку с преимуществом равным 1.

	Ответ
Не заполнять!	/2

5. Пусть $\mathrm{E} = (E, D)$ – подстановочный шифр на (K, M, C): $M = C = \Sigma^L, K = S(\Sigma)$ (множество подстановок на Σ).
Является ли E семантически стойким шифром? Если нет продемонстрируйте атаку с преимуществом равным 1.

	Ответ
Не заполнять!	/2

6. 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.

№	Задание	Ответ
a	$E'(k, m) = 0 \| \| E(k, m)$	
b	$E'(k, m) = E(k, m) \| \| par(m)$, $par(a) -$ чётность сообщения a	
c	$E'(k, m) = rev\big(E(k, m)\big)$, $rev(m) -$ смена порядка битов на обратный	
d	$E'(k, m) = E(k, rev(m))$ $rev(a) -$ смена порядка битов на обратный	
e	$E'(k, m) = E(0^L, m)$	
f	$E'(k, m) = E(k, m) \| \| k$	
g	$E'(\,(k, k'),\, m) = E(k, m) \| \| E(k', m)$	
h	$E'(\,(k, k'),\, m) = (c, c): c \overset{R}{\leftarrow} E(k, m)$	
i	$E'(k, m) = c \| \| par(c): c \overset{R}{\leftarrow} E(k, m)$ $par(a) -$ чётность сообщения a	
	Не заполнять!	/9

7. $\mathrm{E} = (E, D)$ – семантически стойкий шифр на (K, M, C): $M = C = \{0,1\}^{\leq L}$. Пусть $\bar{\bar{C}}: \{0,1\}^{\leq L} \to \{0,1\}^{\leq L}$ – функция сжатия без потерь. Заметим, что $\bar{\bar{C}}$ демонстрирует разный уровень сжатия для различных сообщений.
    a. Пусть в игре на семантическую стойкость Претендент сжимает сообщения перед зашифрованием, т.е. $E'(k, m) = E(k, \bar{\bar{C}}(m))$. Является ли данная схема семантически стойкой? Если да – доказать, иначе – продемонстрировать атаку. Имеет ли данная схема смысл для уменьшения размера шифрткеста? Почему?
    b. Пусть в игре на семантическую стойкость Претендент сжимает шифртекста после зашифрования, т.е. $E''(k, m) = \bar{\bar{C}}(E(k, m))$. Является ли данная схема семантически стойкой? Если да – доказать, иначе – продемонстрировать атаку.

    Имеет ли данная схема смысл для уменьшения размера шифрткеста? Почему?

№	Задание	Ответ	
a	$E'(k, m) = E(k, \bar{\bar{C}}(m))$.		
b	$E''(k, m) = \bar{\bar{C}}(E(k, m))$		
	Не заполнять!	/2	/2

8. Пусть $\mathrm{E} = (E, D)$ – семантически стойкий шифр на (K, M, C): $K = \{0,1\}^{L}$. Банковская организация желает разделить секретный ключ $k \in K$ **на две части** p_1 и p_2, так, что **обе** необходимы для расшифрования.
    Банк генерирует случайное число $k_1 \in K$ и вычисляет $k_1' \leftarrow k \oplus k_1$. Тогда $p_1 = k_1, p_2 = k_1'$.
    Аналогичная задача для трех сторон: разделяя ключ на **три** части p_1, p_2, p_3 можно получить ключ по **любым двум** из ним: банк генерирует пары (k_1, k_1') и (k_2, k_2'), такие что $k_1 \oplus k_1' = k_2 \oplus k_2' = k$. Как следует разделить части пар между сторонами?

№	Задание	Ответ
a	$p_1 = (k_1, k_2), p_2 = (k_2, k_2'), p_3 = (k_2')$	
b	$p_1 = (k_1, k_2), p_2 = (k_1'), p_3 = (k_2')$	
c	$p_1 = (k_1, k_2), p_2 = (k_1', k_2'), p_3 = (k_2')$	
d	$p_1 = (k_1, k_2), p_2 = (k_1, k_2), p_3 = (k_2')$	
e	$p_1 = (k_1, k_2), p_2 = (k_1', k_2), p_3 = (k_2')$	
	Не заполнять!	/1