

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.

- В эксперименте 0 претендент подбрасывает монетку и возвращает **РЕШКА**, если выпала решка, и **ОРЁЛ** если орёл.
- 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 $\text{Adv}[A] = |\Pr[W_0] - \Pr[W_1]| \in [0,1]$.

Вычислить $\text{Adv}[A]$ 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, иначе 0	
d	A : возвращает 0, если от претенденто получено РЕШКА, иначе 1	
e	A : если получено РЕШКА возвращает 1. Иначе – (возвращает 1, с вероятностью $\frac{1}{2}$, иначе 0)	
f	A : $\text{Adv}[A] = \max$, построить A	
	Не заполнять!	/ 12

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 энтропии и длины ключей больше энтропий и длин 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 $E = (E, D)$ 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 $E = (E, D)$ – 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 $E = (E, D)$ – шифр подстановки 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 $E = (E, D)$ – 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	$E'(k, m) = rev(E(k, m))$, $rev(a)$ – 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	$E'(k, m) = (c, c): c \xleftarrow{R} E(k, m)$	
i	$E'(k, m) = c par(c): c \xleftarrow{R} E(k, m)$ $par(a)$ – чётность сообщения a	
	Не заполнять!	/18

7. $E = (E, D)$ – семантически стойкий шифр на (K, M, C) : $M = C = \{0,1\}^{\leq L}$. Пусть $\bar{C}: \{0,1\}^{\leq L} \rightarrow \{0,1\}^{\leq L}$ – функция сжатия без потерь. Заметим, что \bar{C} демонстрирует разный уровень сжатия для различных сообщений.

- а. Пусть в игре на семантическую стойкость Претендент сжимает сообщения перед зашифрованием, т.е. $E'(k, m) = E(k, \bar{C}(m))$. Является ли данная схема семантически стойкой? Если да – доказать, иначе – продемонстрировать атаку. Имеет ли данная схема смысл для уменьшения размера шифртекста? Почему?
- б. Пусть в игре на семантическую стойкость Претендент сжимает шифртекст после зашифрования, т.е. $E''(k, m) = \bar{C}(E(k, m))$. Является ли данная схема семантически стойкой? Если да – доказать, иначе – продемонстрировать атаку.

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

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

8. Пусть $E = (E, D)$ – 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 них: 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 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!	/3