Задание 2.

Фамилия ____

1. Среди указанных ниже величин найдите пренебрежимо малые (negl), супер-полиномиальные (sup) и полиномиально-ограниченные (poly-b) (в теоретическом смысле):

№	Задание	Ответ		
		negl	sup	poly-b
a	$f(n) = 7$			
b	$f(n) = 0.0000018$			
c	$f(n) = 1024^{128}$			
d	$f(n) = n^{-16n}$			
e	$f(n) = n^{-1}$			
f	$f(n) = 1/(n\log(n))$			
g	$f(n) = n!$			
h	$f(n) = n^{-1024} + 2^{-0.00000000001*\log(n)}$			
i	$f(n) = n^{n^2}$			
	Не заполнять!	/ 2	/ 2	/ 2

2. Пусть A – эффективный алгоритм, позволяющий пересказывать следующий бит $r[i+1]$ по битам $r[0 \dots i]$ для некоторого генератора G. Т.е. величина $Adv_{pred}[A,G] = \epsilon$ не пренебрежимо малая. Определим игру на предсказание предыдущего бита: имя биты $r[k+1, \dots, k+i+1]$ предсказать бит $r[k]$. (определяется аналогично игре на определение следующего бита). Постройте эффективный алгоритм B, позволяющий выиграть игру на предсказание прошлого бита, используя алгоритм A. Найдите $Adv_{pred\_prev}[B,G]$ – преимущество алгоритма B в игре на предсказание прошлого бита (определяется аналогично Adv_{pred}).

№	Задание	Ответ	
a	$Adv_{pred\_prev}[B,G]$		
	Не заполнять!	/ 2	/ 2

3. Выберите верные утверждения:

№	Задание	Ответ
a	Если алгоритм противника A в некоторой игре против E эффективный, то величина $Adv[A,\mathrm{E}]$ – пренебрежимо малая	
b	Любая пренебрежимо малая – полиномиально ограниченная	
c	Любая полиномиально ограниченная – пренебрежимо малая	
d	Аддитивный одноразовый блокнот переменной длины – семантически стойкий шифр	
e	Пусть A алгоритм от параметра λ. На вход алгоритма подали вход длинной 2^{λ}, он детерминированно выполнился за время $t(\lambda)$, не являющимся полиномиально ограниченным от λ. A – точно не эффективный.	
f	Пусть A алгоритм от параметра λ. На вход алгоритма подали вход длинной λ, он детерминированно выполнился за время $t(\lambda) = \lambda^{156} + \lambda^{56}\log(\lambda^{-1}\log(\lambda^{65.6}) + 74$, A – эффективный.	
g	Любой эффективный алгоритм – полиномиально ограничен памятью	

h	Если G и G' на (S,T) стойкие PRG, то для $r \leftarrow G(s), r' \leftarrow G'(s)$ $r' \approx_p r$ (последовательности статистически неразличимы).	
	Не заполнять!	/ 8

4. Пусть $G: K \to \{0,1\}^n$ – стойкий PRG. Пусть $G'(k_1, k_2) = G(k_1) \wedge G(k_2)$, где $\wedge$ - побитовый AND. Рассмотрим следующий статистический тест на $\{0,1\}^n$: $A(x) = LSB(x)$, где $LSB(x)$ - получает последний бит вектора $x \in \{0,1\}^n$.
Каково преимущество алгоритма A? ($Adv_{PRG}[A, G]$ - ?)

	Ответ
Не заполнять!	/2

5. Пусть $\mathrm{E} = (E, D)$ – абсолютно стойкий шифр на (K, M, C): $M = C, K = \{0,1\}^n$
Является ли $\mathrm{E}' = (E', D')$: $E((k_1, k_2), m) = E(k_1, k_2)||E(k_2, m)$ абсолютно стойким шифром? Если нет продемонстрируйте атаку.

	Ответ
Не заполнять!	/2

6. 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.

№	Задание	Ответ
a	$G'(k) = G(k)\|\|G(k)$	
b	$G'(k) = G(k) \oplus 1^n$	
c	$G'(k) = rev(G(k))$, $rev(m)$ – смена порядка битов на обратный	
d	$G'(k) = G(k)\|\|0$	
e	$G'(k) = G(0)$	
f	$G'(k, k') = G(k) \vee G(k')$, $\vee$ - побитовый OR	
g	$G'(k, k') = G(k)\|\|G(k')$	
h	$G'(k, k') = G(k) \oplus G(k')$	
i	$G'(k, k') = k\|\|G(k')$	
	Не заполнять!	/18

7. $\mathrm{E} = (E, D)$ –шифр на (K, M, C). Пусть имеется возможность случайно выбирать шифртекст равновероятно из C. Рассмотрим игру: Противник посылает сообщение $m \in M$ претенденту. Претендент вычисляет $b \xleftarrow{R} \{0,1\}, k \xleftarrow{R} K, c_0 \xleftarrow{R} E(k, m), c_1 \xleftarrow{R} C, c \leftarrow c_b$ и отправляет c противнику, который затем вычисляет бит $b' \in \{0,1\}$, являющегося результатом игры. Определим $Adv_{ctDist} = |\Pr[b' = b] - 1\backslash 2|$. Определим E – стойкий шифр с псевдослучайными шифртекстами (pseudo-random ciphertext secure), если для любых противников величина Adv_{ctDist} – пренебрежимо малая.
Формально докажите или опровергните утверждения ниже.

№	Задание	Ответ	
a	Если E – стойкий шифр с псевдослучайными шифртекстами, то он всегда семантически стойкий		
b	Одноразовый блокнот - стойкий шифр с псевдослучайными шифртекстами		
c	Невозможно построить шифр, который будет семантически стойким, но не стойким с псевдослучайными шифртекстами.		
	Не заполнять!	/3	/3

8. Пусть G стойкий PRG на $(S.R)$, $|R| \geq 2|S|$. Показать, что $|S|$ - супер-полиномиальна. Для этого показать наличие противника с преимуществом не менее $1/2$ против G с временем атаки линейным от $|S|$.

	Ответ
Не заполнять!	/4