Задание 7,

Фамилия ____

1. Выберите верные утверждения:

№	Задание	Ответ
a	Любая стойкая PRF даёт стойкий MAC	
b	Любая стойкая PRF, с сверх полиномиальной областью значений даёт стойкий MAC	
c	Любая стойкая PRP, с сверх полиномиальной областью значений даёт стойкий MAC	
d	Стойкая PRF с сверх полиномиальной областью значений является более сильным определением, чем стойкий MAC	
e	На любой MAC на (K, M, T) возможна теоретическая атака сложностью $O(\|T\|)$	
f	На любой CBC-MAC на (K, M, T) возможна теоретическая атака сложностью $O(\sqrt{\|T\|})$	
g	CMAC требует использования трех независимых случайных ключей	
h	Любое беспрификсное кодирование увеличивает длину сообщения	
i	Стойкий MAC обеспечивает целостность сообщений при передаче	
j	Стойкий MAC обеспечивает аутентичность источника информации (т.е. гарантирует, что только имеющий секретный ключ мог отправить это сообщение)	
k	Добавление длины сообщения в конец сообщения является беспрификсным кодированием	
	Не заполнять!	/ 10

2. Рассмотрим ECBC MAC. Вместо использования нулевого IV будем использовать случайный IV для каждого сообщения и включать его в состав итоговой метки. Т.е. $t = IV||MAC(k, m)$. Данная система не является стойким MAC. Задача – от имени противника получить верный MAC для сообщения 0^n, где n – размер блока PRF. Является ли данный MAC стойкой **беспрификсной** PRF?

	Ответ
Не заполнять!	/4

3. Alice отправляет данные 6 получателям $B_1, . . , B_6$. Задача – обеспечить целостность. Alice использует MAC. Использование одного ключа для всех получателей не обеспечивает целостность, так как если противником является одним из получателей, то он может подделать MAC для любого сообщения и рассылать сообщения от имени Alice. Вместо этого Alice использует 4 секретных ключа $S = \{k_1, \dots, k_4\}$. Alice пересылает по защищенному каналу некое подмножество $S_i \subseteq S$ каждому получателю B_i. Пересылая затем каждое сообщение, она включает также 4 кода аутентичности для каждого сообщения, выработанных на этих ключах. Каждый пользователь B_i считает пакет целостным, если для всех его ключей S_i совпали коды аутентичности (те коды аутентичности, которые не соответствуют ключам пользователя им игнорируются).
   Как Alice должна распределить ключи между пользователями?

	Ответ
Не заполнять!	/4

4. 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. $a[x, \dots, y]$ – взятие подверктора вектора a с индексами от x до y, $a[q \dots]$ – взятие подвектора вектора a начиная с индекса q и до длины вектора a.

№	Задание	Ответ
a	$S'(k, m) = S(k, m\|\|m), V'(k, m, t) = V(k, m\|\|m, t)$	
b	$S'(k, m) = S(k, m)$, $V'(k, m, t,) = [V(k, m, t) = 1 \text{или} \, V(k, m \oplus 1^n, t) = 1]$	
c	$S'(k, m) = S(k, m \oplus 1^n), V'(k, m, t) = (k, m \oplus 1^n, t)$	
d	$S'(k, m) = [t \leftarrow S(k, m), \text{output } (t, t)]$ $V'(k, m, (t_1, t_2)) = \begin{cases} V(k, m, t_1), \text{if } t_1 = t_2 \\ 0, \text{else} \end{cases}$	
e	$S'(k, m) = S(k, m[0, \dots, n-2]\|\|0$ $V'(k, m, t) = V(k, m[0, \dots, n-2]\|\|0, t)$	
f	$S'(k, m) = \big(S(k, m), S(k, 0^n)\big)$ $V'\big(k, m, (t_1, t_2)\big) = [V(k, m, t_1) \text{ и } V(k, 0^n, t_2)]$	
g	$S'(k, m) = S(k, m)\|\|m$ $V'(k, m, t) = [V(k, m, t[0, \dots, 127]) \text{ и } m = t[128 \dots]]$	
h	$S'\big(k, (a_1, a_2)\big) = S(k, a_1)\|\|S(k, a_2)$	
i	$S'\big(k, (a_1, a_2)\big) = S(k, a_1) \oplus S(k, a_2)$	
j	$S'\big((k_1, k_2), (a_1, a_2)\big) = S(k_1, a_1)\|\|S(k_2, a_2)$	
k	$S'\big((k_1, k_2), (a_1, a_2)\big) = S(k_1, a_1) \oplus S(k_2, a_2)$	
	Не заполнять!	/22

5. Докажите утверждения ниже

№	Задание	Ответ
a	Пусть $I_1 = (S_1, V_1), I_2 = (S_2, V_2)$ – MAC. Пусть $I = (S, V)$: $S\big((k_1, k_2), m\big) = \big(S_1(k_1, m), S_2(k_2, m)\big)$, $V\big((k_1, k_2), m, (t_1, t_2)\big) = [V_1(k, m, t_1) = 1 \text{ и } V_2(k, m, t_2) = 1]$. Докажите, что I – стойкий, если хотя бы один из I_1, I_2 – стойкий MAC	(доп листы)
b	Пусть $I_1 = (S_1, V_1), I_2 = (S_2, V_2)$ – **детерминированные** MAC. Пусть $I = (S, V)$: $S\big((k_1, k_2), m\big) = \big(S_1(k_1, m) \oplus S_2(k_2, m)\big)$. Докажите, что I – стойкий, если хотя бы один из I_1, I_2 – стойкий MAC	(доп листы)
	Не заполнять!	/4