

Задание 9,

Фамилия _____

1. Выберите верные утверждения:

№	Задание	Ответ
a	Любую схему стойкого аутентифицированного шифрования можно использовать в качестве стойкого кода аутентичности	
b	При использовании схемы MAC-then-Encrypt необходимо использовать независимые ключи для MAC и шифрования	
c	При использовании схемы EAX необходимо использовать независимые ключи для MAC и шифрования	
d	ССА стойкость более сильно определение, чем CPA стойкость	
e	Возможно построить ССА стойкий шифр, который не будет CPA стойким	
f	Обеспечение целостности открытых текстов не может быть обеспечена через целостность соответствующих шифртекстов	
g	Схема Encrypt-and-MAC в общем случае является не стойкой	
h	ССА стойкости достаточно для защиты аутентичности от пассивных противников	
i	Целостность шифртекстов более сильное определение, чем целостность открытых текстов, при передаче шифртекстов по каналу связи	
	Не заполнять!	/ 9

2. Пусть $k \in_R K$ – случайная величина, полученная с использованием **неравномерного** распределения, $K = \{0,1\}^{256}$:

$$\forall c \in \{0,1\}^{256}: \Pr[k = c] = \begin{cases} \frac{1}{2^{128}}, & \text{if } MSB_{128}(c) = 0^{128} \\ 0, & \text{else} \end{cases}$$

Иными словами, k выбирается из подмножества векторов в K , для которых первые 128 бит – нулевые.

Пусть $F(k, x)$ – стойкая PRF, с множеством ключей K . Какие из PRF ниже является стойкими PRF (в практическом смысле, минимальный параметр стойкость – 80 бит), но не является стойкими при выборе k с использованием распределения, описанного выше?

№	Задание	Ответ
a	$F'(k, x) = \begin{cases} F(k, x), & \text{if } MSB_{128}(k) \neq 0^{128} \\ 0^{256}, & \text{else} \end{cases}$	
b	$F'(k, x) = \begin{cases} F(k, x), & \text{if } MSB_{128}(k) \neq 1^{128} \\ 0^{256}, & \text{else} \end{cases}$	
c	$F'(k, x) = F(k, x)$	
d	$F'(k, x) = \begin{cases} F(k, x), & \text{if } MSB_{128}(k) \neq 1^{128} \\ 1^{256}, & \text{else} \end{cases}$	
	Не заполнять!	/ 8

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).

№	Задание	Ответ
a	$E'(k, m) = E(k, m)$ $D'(k, c) = \begin{cases} D(k, c), & \text{if } D(k, c) \neq \perp \\ 0^n, & \text{else} \end{cases}$	
b	$E'(k, m) = E(k, m \oplus 1^n)$ $D'(k, c) = \begin{cases} D(k, c) \oplus 1^n, & \text{if } D(k, c) \neq \perp \\ \perp, & \text{else} \end{cases}$	
c	$E'(k, m) = (E(k, m), 0)$ $D'(k, (c, d)) = D(k, c)$	
d	$E'(k, m) = E(k, m) \oplus 1^s$ $D'(k, c) = D(k, c \oplus 1^s)$	
e	$E'(k, m) = E(k, m) E(k, m)$ $D'(k, (c_1, c_2)) = \begin{cases} D(k, c_1), & \text{if } D(k, c_1) = D(k, c_2) \\ \perp, & \text{else} \end{cases}$	
f	$\{c \leftarrow E'(k, m), \text{return } (c, c)\}$ $D'(k, (c_1, c_2)) = \begin{cases} D(k, c_1), & \text{if } D(k, c_1) = D(k, c_2) \\ \perp, & \text{else} \end{cases}$	
Не заполнять!		/12

4. Пусть (E, D) – строго стойкий блочный шифр на $(K, M \times R)$, $1/|R|$ – пренебрежимо малая. Докажите, что шифр ниже стойкий ССА шифр, но не стойкий АЕ шифр (не обеспечивается целостность шифртекстов). Строго стойкий блочных шифр (strongly secure block cipher) – шифр, стойкий против противников, которые могут помимо запросов на зашифрование произвольных блоков запрашивать запросы на расшифрование произвольных блоков блочного шифра в игре на стойкость блочного шифра (PRP).

$$E'(k, m) = \{r \leftarrow^R R, c \leftarrow^R E(k, (m, r)), \text{return } c\}$$

$$D'(k, c) = \{(m, r') \leftarrow D(k, c), \text{return } m\}$$

	Ответ
	Доп. Листы.
Не заполнять!	/2