

Задание 8,

Фамилия \_\_\_\_\_

1. Выберите верные утверждения:

№	Задание	Ответ
a	Любой случайный оракул стойкий к нахождению коллизий второго рода	
b	Любая стойкая к коллизиям второго рода хэш-функция является стойкой к коллизиям первого рода	
c	Любая стойкая к коллизиям второго рода хэш-функция является стойкой односторонней хэш-функцией	
d	Любой стойкий MAC с фиксированным ключом и сверх-полиномиальной областью определения даёт стойкую к коллизиям хэш-функцию	
e	На любую хэш-функцию на $(M, T)$ возможна теоретическая атака сложностью $O(\sqrt{ T })$	
f	Атака на стойкость хэш-функции в модели случайного оракула даёт атаку в модели односторонней хэш-функции	
g	Атака на стойкость к коллизиям второго рода для некоторой хэш-функции даёт атаку на случайный оракул для данной функции.	
h	Отправка хэш-значения для некоторой величины (выбранной равномерно из множества со сверх-полиномиальной мощностью) по открытому каналу гарантирует, что противник не сможет восстановить данную величину. (используется хэш-функция, стойкая к коллизиям второго рода)	
	<b>Не заполнять!</b>	/ 8

2. Рассмотрим следующие функции сжатия

$$f_1 = AES(y, x) \oplus y$$

$$f_2 = AES(x, x) \oplus y$$

Задача – найти 4 различные пары  $(x_1, y_1), (x_2, y_2), (x_3, y_3), (x_4, y_4)$ :

$$f_1(x_1, y_1) = f_1(x_2, y_2)$$

$$f_2(x_3, y_3) = f_2(x_4, y_4)$$

Необходимо вывести в виде формулы получение этих пар и представить ответ в виде hex-строки.

	Ответ
	Доп. Листы.
<b>Не заполнять!</b>	/4

3. Пусть  $H_1$  и  $H_2$  – стойкие к коллизиям хэш-функции на  $M \rightarrow \{0,1\}^{256}$ . Доказать, что  $H_2(H_1(m))$  – стойкая к коллизиям хэш-функция. Доказать от противного – предположить, что  $H_2(H_1(*))$  не стойкая к коллизиям.

	Ответ
<b>Не заполнять!</b>	/2

4. Пусть  $H: M \rightarrow T$  – стойкая к коллизиям хэш-функция. Какая из описанных хэш-функций является стойкой? Формально докажите или опровергните стойкость.

№	Задание	Ответ
a	$H'(m) = H(m) \oplus H(m \oplus 1^{ m })$	
b	$H'(m) = H(m) \oplus H(m)$	
c	$H'(m) = H(m)    H(m)$	
d	$H'(m) = H(m) \oplus H(0)$	
e	$H'(m) = H(m)    H(0)$	
f	$H'(m) = H(H(H(m)))$	
g	$H'(m) = H(0)$	
h	$H'(m) = \text{HMAC}(m, m)$	
	<b>Не заполнять!</b>	/8

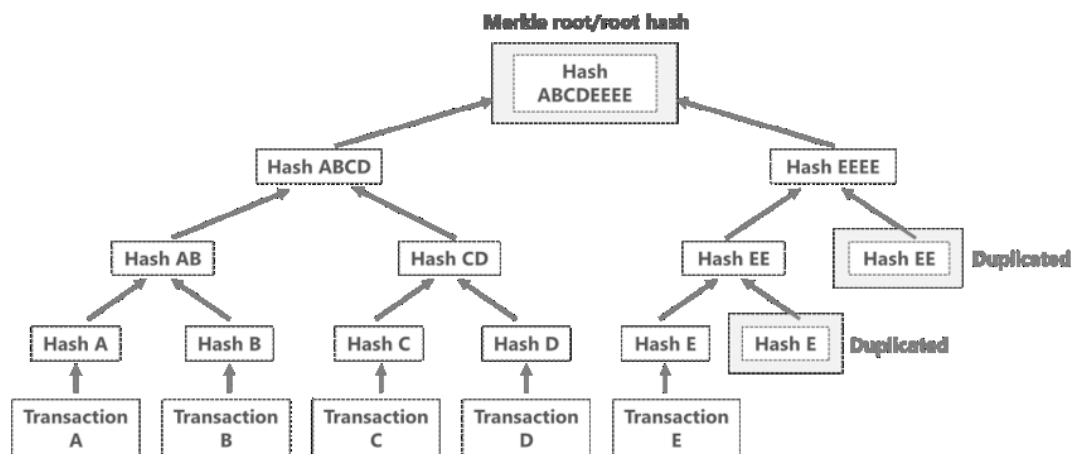
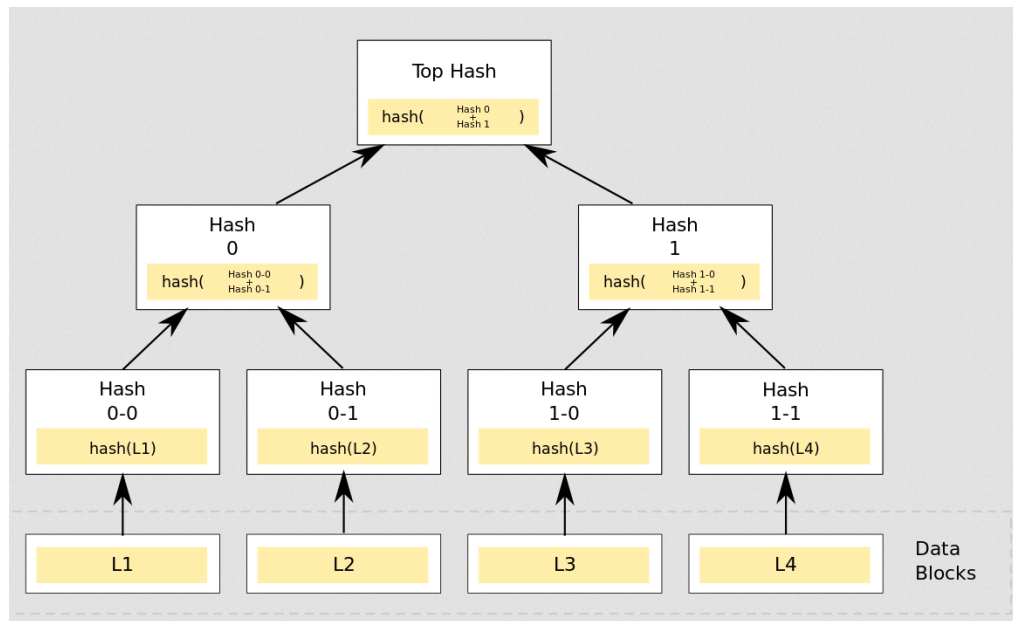
5. Докажите утверждения ниже

Пусть  $H: M \rightarrow T$  – случайный оракул.  $|M| > |T|$ . Какова сложность нахождения тройной коллизии, т.е. трех различных величин  $x, y, z \in M: H(x) = H(y) = H(z)$ ? (ответ + его вывод на доп. Листах)

	Ответ
<b>Не заполнять!</b>	/4

6. Почитать что такое дерево Меркла (Merkle tree), просмотра и осознание картинки на последней странице дз – достаточно. В рамках данного задания считать дерево несбалансированным, т.е. возможны «висячие» узлы со значением  $n'$ , для которых нет пар. В таком случае хэш для родительского узла вычисляется как  $H(n', n')$ . Пусть имеется  $N = 647$  различных файлов. Ответе на вопросы ниже.

№	Задание	Ответ
a	Какова высота дерева меркла для вычисления хэш-значения, обеспечивающего целостность всех файлов?	
b	Какое количество хэшей необходимо пересчитать, при замене одного из файлов?	
c	Какое минимальное количество хэшей необходимо пересчитать при замене 4-х файлов?	
d	Какое максимальное количество хэшей необходимо пересчитать при замене 4-х файлов?	
e	Какое количество хэшей необходимо вычислить при построении дерева?	
f	Сколько узлов хэш значений отвечает за целостность одного файла?	
g	За целостность какого количество файлов отвечает корневой узел?	
h	Предположим необходимо переслать один из файлов. Предполагая, что получатель знает только значение корня дерева (и может проверить только его) Меркла, какое минимальное количество узлов дерева необходимо переслать вместе с файлом, для осуществления проверки файла получателем? (authentication path)	
	<b>Не заполнять!</b>	/ 8



Merkel's Tree



Merkle Tree

