

Задача А. Подпись с деревом Мёркла

Имя входного файла:	стандартный ввод
Имя выходного файла:	стандартный вывод
Ограничение по времени:	10 секунд
Ограничение по памяти:	256 мегабайт

В этой задаче Вам надо будет найти подпись произвольного документа в схеме Лампорта-Диффи-Мёркла.

Возьмем дерево из практики 4, и предположим, что его высота всегда равна 8, то есть безопасным образом можно подписать не больше 256 документов. К вашей удаче, подписывающий по ошибке готов подписать 1000 сообщений. Правда, и подписывающий стремится Вас обмануть. Ваша задача заключается в подписи документа, который у Вас просят.

Протокол взаимодействия

Интерактор генерирует 256 секретных ключей, каждый из которых состоит из $2 \cdot 256$ бинарных строк длины 256. Далее он применяет к каждой строчке ключа SHA-256, тем самым получая публичные ключи. На публичных ключах он строит дерево Мёркла, где сообщение в листе представлено как конкатенация строк: $y_{0,0} \parallel y_{0,1} \parallel \dots \parallel y_{0,255} \parallel y_{1,0} \parallel y_{1,1} \parallel \dots \parallel y_{1,255}$, а узлы хешируются по правилам предыдущего занятия.

В первой строке интерактор выводит публичный ключ — хеш корня дерева Мёркла.

Затем происходит не более 1000 раундов, за которые Вы должны решить задачу. В каждом раунде взаимодействия происходит 5 шагов:

1. Интерактор сообщает номер ключа, которым будет подписано сообщение.
2. Вы отвечаете на это хешом документа D в виде бинарной строки длины 256.
3. Интерактор в первой строке возвращает подпись $x_{D_{0,0}} \parallel x_{D_{1,1}} \parallel \dots \parallel x_{D_{255,255}}$ в Base64, полученную из ключа с помощью хеша. Во второй строке интерактор передаёт публичный ключ в Base64: $y_{0,0} \parallel \dots \parallel y_{0,255} \parallel y_{1,0} \parallel \dots \parallel y_{1,255}$. В следующих 8 строках выводится доказательство в дереве Мёркла. Учтите, что с вероятностью $\frac{1}{2}$ при выводе допущена ошибка: либо в подписи, либо в доказательстве. В последней строке содержится бинарная строка длины 256 — хеш документа Q , который Вас просят подписать тем же ключом.
4. В первой строке ВЫ должны вывести “YES”, если предоставленные данные корректны, иначе выведите “NO”. Затем, если Вы можете подписать, то Вы должны вывести “YES” и на следующей строке $x_{Q_{0,0}} \parallel \dots \parallel x_{Q_{255,255}}$ в Base64. Иначе, выведите “NO”.

Пример

стандартный ввод	
ok9AwuJ9/AGRnQoMR1SvRXL3w2D3TsJtB1aGmPYSapU=	161
J8AF2xiyp5rvQ6hDipuc33cZfQM7Cb3wxT0Rz+ouHhtoCQDZEQ...	S3j4CwKqhkI2hf2rVNWOM+BHuBqpknjpTqi1t6F54YlBsLZFdC...
LkndRBhjjd7zcb18/HGMgoxXTMnZ3drvr092p7yP9pY=	Dgc/XJI81YrZSBMdntyfgRwlYP6GGgIwQaUdYb5IVq4=
s2AKreWLXq3A7JwnuLY9xbLcvklx2utJwtXJahmSavc=	PawtdyrZVJwPmqzM+mxX6nIVy6K2qCZaeYUyZBGBBRo=
+PZhKCPNkbpCzDH/qQP6pjHeTH/644v+vTH38dhhePg=	SLWkDFQgHh0pgqQRQ5xYRcArHDBGxD35nJ2eioXMHro=
k7uSAe6/ga35Xhp7myuijH0sKpK+gQLTitp+Gbd3SKo=	dUK7U3R33HkBIcJT0e0Ylx4Gx/zfqIVYjvQo1NS9V0g=
11001010000001101101011101011110001100000011100010...	
209	
...	
стандартный вывод	
000...	
YES	
NO	
11010110101100111001110101100110010000001010101001...	
...	
YES	
J8AF2xiyp5rvQ6hDipuc33cZfQM7Cb3wxT0Rz+ouHhtoCQDZEQ...	