Можете ли вы предложить что-то еще лучше? Да, поскольку у вас есть секретный декодирующий ключ. Это d, инверсное значение $e \bmod (p-1)(q-1)$. Для его вычисления имеется удобный алгоритм, которым можно воспользоваться, конечно, при условии, что вы знаете два простых числа p и q, которые были использованы для получения N. (Вы ведь знаете их, потому что сами их выбрали, не забыли?)

Назовите кодированное число/сообщение, которое Боб отправил вам назад, Y. Его первоначальное сообщение было

$$Y^d \bmod N.$$

Для определения этого значения нужно всего лишь ввести это в Wolfram Alpha (замените Y, d и N фактическими числами).

Ева знает N, поскольку оно было написано на карточке, которую вы попросили ее передать Бобу. Она знает У, поскольку это число было указано в ответе Боба, отправленном вам. Но она не знает d, и у нее нет возможности его выяснить. Ева сталкивается с алгоритмической трудностью. При умножении двух чисел никаких сложностей ни у кого не возникнет, ведь этому все-таки в школе всех научили. А вот определить множитель, имея огромное число, гораздо сложнее.

? Если вы получили бы стопку монет достоинством в один пенс каждая и высотой с Эмпайр-стейт-билдинг, поместились бы все эти деньги в одном помещении?

Вы решили, что это одна из тех головоломок, задаваемых на собеседованиях, в которых предлагается оценить

какое-то абсурдное количество. Успокойтесь: на самом деле именно в этом вопросе не спрашивается, *сколько именно* пенсов. В нем спрашивается, *поместится ли стопка пенсов* в помещении? Интервьюер хочет получить от вас простой ответ – да или нет (и, разумеется, вы должны его пояснить).

Сказанное должно быть ключом, как ключом является и то, что в вопросе не говорится о размере помещения. Помещение может быть самым разным. Интуитивно можно предположить, что стопка монет не поместится в телефонной будке, но легко уложится в Зале зеркал в Версале.

Ответ является приблизительно следующим: «В Эмпайр-стейт-билдинге примерно сто этажей (если говорить точно, их 102). Его высота по крайней мере в 100 раз выше обычного помещения. Мне придется разделить стопку монет высотой с небоскреб на сто меньших стопок высотой от пола до потолка помещения. Поэтому вопрос становится таким: смогу ли я разместить примерно сотню стопок монет высотой от пола до потолка в помещении? Легко! Это всего лишь решетка монет десять на десять. Если в помещении есть место для сотни монет, лежащих на полу рядом друг с другом, то задача решается. В самой крошечной квартире в Нью-Йорке и даже в старомодной телефонной будке найдется место, чтобы положить рядом друг с другом сто монет.

На ваш ответ повлияет и ваша манера его предоставления. Поэтому цель не только дать правильный ответ, но и показать, что задачу можно решить легко. Великие спортсмены на соревнованиях выступают легко. А в последнее время ожидается, что так же легко результаты будут выдавать и претенденты на получение работы.